Sur la conjecture d'André-Oort et courbes modulaires de Drinfeld

Florian Breuer

UNIVERSITÉ PARIS 7 - DENIS DIDEROT

Année: 2002 N° | | | | | | | | | |

THÈSE

Spécialité: Mathématiques

Presentée par

Florian BREUER

pour obtenir le grade de

DOCTEUR en MATHÉMATIQUES

Sur la conjecture d'André-Oort et courbes modulaires de Drinfeld

Soutenu le 8 novembre 2002 devant le jury composé de:

Yves André	
Laurent Denis	
Bas Edixhoven	(président, rapporteur)
Ernst-Ulrich Gekeler	(rapporteur)
Marc Hindry	(directeur de thèse)

BL und OB gewidmet

Remerciements

Tout d'abord je voudrais exprimer ma plus profonde reconnaissance à mon directeur de thèse, Marc Hindry, pour son soutien constant, pour ses conseils chaleureux et pour toutes les mathématiques qu'il m'a apprises. Il a en plus consacré beaucoup d'effort et temps à lire cette thèse de près, et ses nombreuses remarques et conseils ont beaucoup contribué à ce travail.

Je tiens à remercier Hans-Georg Rück, qui le premier m'a parlé de remplacer les courbes elliptiques par les modules de Drinfeld dans la conjecture d'André-Oort en 1999, une suggestion que je n'ai suivie que deux ans plus tard, mais qui a mené à la présente thèse.

Je suis très honoré que Bas Edixhoven et Ernst-Ulrich Gekeler aient accepté d'être rapporteurs, tâche dont ils se sont acquittés avec diligence.

Je suis très reconnaissant aussi à Bas Edixhoven pour ses explications patientes (surtout en dernière minute!), et pour m'avoir communiqué une version préliminaire de [21].

Je remercie Yves André et Laurent Denis d'avoir accepté de faire partie de mon jury.

Je voudrais aussi remercier Henning Stichtenoth pour m'avoir fourni la Proposition 3.1.4, qui m'a permis d'enlever la condition $q \geq 5$ dans mes résultats principaux.

Je profite de l'occasion pour remercier Jean-Pierre Serre pour avoir trouvé une lacune dans une version antérieure des Corollaires A.2.5 et A.2.6.

Pendant les années où j'ai travaillé sur cette thèse j'ai bénéficié de discussions avec Yves André, Barry Green, Gerhard Frey, Joseph Oesterlé, Hans-Georg Rück, Henning Stichtenoth, Brink van der Merwe, Ingo Waschkies, Andrei Yafaev et Jing Yu. Je voudrais prendre cette opportunité pour les remercier tous.

Mes amis et ma famille ont beaucoup apportés à la qualité de ma vie de thésard, et m'ont donné du courage quand j'en avais le plus besoin. En particulier, je veux remercier Carola, Catriona, Christine, Erik, Hannes, Ingo, Ivar, Klaus, Lucie, Magda, Pietro, Uschi et surtout BL et OB, à qui cette thèse est dédiée.

Finalement, cette thèse a été écrite avec le soutien financier d'une *Bourse du Gouvernement Français* (Numéro 1998/2672), et je voudrais remercier le gouvernement Français pour sa générosité.

Sur la conjecture d'André-Oort et courbes modulaires de Drinfeld

On the André-Oort conjecture and Drinfeld modular curves

Florian Breuer

Contents

Introduction en Français

Le but de cette thèse est de formuler et démontrer un analogue de la conjecture d'André-Oort pour un produit de courbes modulaires de Drinfeld.

0.1 La conjecture d'André-Oort

Un énoncé général de cette conjecture est le suivant.

Conjecture 0.1 (André-Oort) *Soit X une variété de Shimura et $Z \subset X$ une sous-variété algébrique géométriquement irréductible. Alors $Z(\mathbb{C})$ contient un sous-ensemble Zariski-dense de points spéciaux si et seulement si Z est une sous-variété de type Hodge.*

Les définitions exactes des variétés de Shimura, des points spéciaux et des sous-variétés de type Hodge nous amèneraient trop loin. On renvoie le lecteur plutôt à [47], aussi qu'à [20, 22, 48, 49, 71].

Intuitivement, par contre, on peut comprendre la conjecture de la manière suivante. Une variété de Shimura est une variété de modules X de certains objets (par exemple des variétés abéliennes, ou, plus généralement, des motifs), munis de certaines structures supplémentaires (par exemple des polarisations, endomorphismes ou structures de niveau). Une sous-variété de type Hodge est alors essentiellement une sous-variété qui est elle-même une variété de Shimura, i.e. un espace de modules de mêmes objets, mais munis des structures supplémentaires plus fortes. Les points spéciaux sont alors les sous-variétés de type Hodge de dimension zéro. On imagine renforcer les structures supplémentaires jusqu'au point où l'espace de modules aura la dimension zéro, mais restera non-vide. Voilà alors nos points spéciaux, qui sont d'ailleurs denses (même dans la topologie complexe) dans X. La conjecture dit que les seules sous-variétés contenant un sous-ensemble Zariski-dense de points spéciaux sont ces sous-variétés Z obtenues en renforçant les structures supplémentaires.

Dans la section suivante on étudiera un cas spécial avec plus de détail - et nos définitions seront totalement rigoureuses.

La conjecture 0.1 a été énoncée pour la première fois, pour le cas $\dim(Z) = 1$, comme problème dans le livre d'Yves André [1], qui est apparu en 1989. Plus tard, Frans Oort a énoncé la Conjecture 0.1 pour le cas où $X = \mathcal{A}_{g,1}$ est la variété de modules de variétés abéliennes principalement polarisées de dimension g (voir [47, 53, 54]). Dans ce cas les points spéciaux correspondent aux variétés abéliennes à muliplication complexe (CM), et ils s'appellent points CM.

La conjecture précédente a une forte similarité avec la conjecture de Manin-Mumford, qui a été démontré par Michel Raynaud en 1983 [56, 57]:

Théorème 0.2 (Raynaud) *Soit A une variété abélienne, et $V \subset A$ une sous-variété algébrique géométriquement irréductible. Alors $V(\mathbb{C})$ contient un sous-ensemble Zariski-dense de points de torsion (de A) si et seulement si $V = t + B$, où $t \in A_{tors}(\mathbb{C})$ et $B \subset A$ est une sous-variété abélienne.*

L'analogie est donnée par

André-Oort	Manin-Mumford
variétés de Shimura	variétés abéliennes
points spéciaux	points de torsion
sous-variétés de type Hodge	translatés de sous-variétés abéliennes par des points de torsion

En fait, c'est cette analogie qui a partiellement suggéré la Conjecture 0.1. André [2] a formulé une conjecture très générale qui implique à la fois ces deux conjectures.

Les cas suivants de la Conjecture 0.1 ont déjà été démontrés.

Moonen, 1994, [47, 48, 49] Supposons que $X = \mathcal{A}_{g,1,m}$ soit la variété de modules de variétés abéliennes principalement polarisées de dimension g munies des structures de niveau-m complètes. Soit $Z \subset X$ une sous-variété algébrique géométriquement irréductible contenant un sous-ensemble Zariski-dense S de points CM satisfaisant la propriété suivante: Il existe un nombre premier p tel que chaque point de S soit le relevé canonique de Serre-Tate de sa réduction modulo une place au-dessus de p. Alors Z est de type Hodge.

Edixhoven, 1995, [19] X est le produit de deux courbes modulaires elliptiques[1], supposant que l'Hypothèse de Riemann Généralisée (GRH) soit vraie pour les corps quadratiques imaginaires.

André, 1995, [2] X est le produit de deux courbes modulaires elliptiques (i.e. comme avant, mais sans supposer GRH).

Yafaev, 1999, [72] X est le produit de deux courbes de Shimura associées aux algèbres de quaternions sur $\mathbb{Q}$, supposant GRH pour les corps quadratiques imaginaires.

Edixhoven, 1999, [20, 21] X est une surface modulaire de Hilbert, ou X est le produit de n courbes modulaires elliptiques. Pour les deux résultats il faut supposer GRH.

[1] on utilise le mot "elliptique" pour souligner la distinction avec les courbes modulaires de Drinfeld

Belhaj-Dahmane, 2001, [6] Soit $X \subset \mathcal{A}_{g,1}$ la courbe correspondant aux Jacobiennes des courbes de la forme $y^n = x(x-1)(x-\lambda)$ quand $\lambda \in \mathbb{C}$ varie. Alors, X n'est pas de type Hodge, et (sous quelques restrictions techniques) il n'y a qu'un nombre fini des ces Jacobiennes (pour un n fixé) qui ont des multiplications complexes.

Edixhoven et Yafaev, 2001, [22] Soit X une variété de Shimura et $Z \subset X$ une courbe. Alors Z est de type Hodge si elle contient un sous-ensemble infini de points spéciaux qui sont tous dans la même orbite de Hecke.

Il y a au moins deux applications de ces résultats connus. Premièrement, le résultat d'Edixhoven et Yafaev permet de réparer une lacune dans un résultat de Wolfart [70] sur l'algébricité des valeurs de fonctions hypergéometriques en des nombres algébriques, voir [6, 13, 22, 71].

Comme deuxième application, Cornut [16] a utilisé le résultat de Moonen (il aurait pu aussi utiliser le résultat d'Edixhoven sur le produit de n courbes modulaires) pour démontrer plus facilement une conjecture de Mazur sur les points de Heegner supérieurs [45], après avoir déjà démontré cette conjecture à partir de méthodes plus profondes [15]. On peut espérer démontrer des résultats analogues sur les points de Heegner sur les courbes elliptiques "modulaires" sur les corps de fonctions, en combinant les résultats de cette thèse avec les méthodes de Cornut. Ceci fait l'objet des travaux en cours, qui ne sont malheureusement pas prêts à temps pour être inclus ici.

0.2 Le cas des courbes modulaires elliptiques

Dans cette thèse on s'intéresse au cas spécial suivant. On regarde l'espace affine $\mathbb{A}^n$ comme espace de modules de n-uples de courbes elliptiques, où un n-uple $(E_1, \ldots, E_n)$ correspond au point $(j(E_1), \ldots, j(E_n)) \in \mathbb{A}^n(\mathbb{C})$, et $j(E)$ dénote l'invariant-j de la courbe elliptique complexe E. Alors $\mathbb{A}^n$ est une variété de Shimura[2], et les points spéciaux sont les *points CM*, donc les points $(x_1, \ldots, x_n)$, où chaque x_i est l'invariant-j d'une courbe elliptique à multiplication complexe. Maintenant la Conjecture 0.1 dit qu'une sous-variété algébrique irréductible $X \subset \mathbb{A}^n$ contient un sous-ensemble Zariski-dense de points CM si et seulement si X est une sous-variété de type Hodge, qu'on appelle une sous-variété *modulaire*. Mais qu'est ce que ça signifie ici?

On se restreint d'abord au cas $n = 2$. Alors $\mathbb{A}^2$, le plan affine, paramétrise les classes d'isomorphie de couples de courbes elliptiques. La seule sous-variété modulaire $X \subset \mathbb{A}^2$ de dimension 2 est $\mathbb{A}^2$ elle-même, pendant que celles de dimension 0 sont les points CM. Alors il reste à caractériser les sous-variétés modulaires de dimension 1 - les *courbes modulaires*. Soit $N \in \mathbb{N}$ et notons $Y_0(N)$ la courbe modulaire paramétrisant les couples (E_1, E_2, f) de courbes elliptiques liées par une isogénie $f : E_1 \to E_2$ cyclique de degré N (i.e. $\ker(f) \cong \mathbb{Z}/N\mathbb{Z}$). Alors on peut envoyer $Y_0(N)$ dans $\mathbb{A}^2$ en envoyant (E_1, E_2, f) sur le point $(j(E_1), j(E_2))$. L'image, qu'on note $Y_0'(N)$, est une courbe algébrique

[2] on pourrait également considérer $\mathbb{A}^n/S_n$, l'espace de produits de n courbes elliptiques. On peut plonger $\mathbb{A}^n/S_n$ dans $\mathcal{A}_{n,1}$.

irréductible définie sur $\mathbb{Q}$. C'est un modèle birationnel de $Y_0(N)$, mais n'est pas lisse en générale. Maintenant il est facile à voir que $Y_0'(N)(\mathbb{C})$ contient un nombre infini de points CM: Il existe un nombre infini de $x_1 \in \mathbb{C}$ correspondant aux courbes elliptiques CM, et pour chaqun il existe au moins un $x_2 \in \mathbb{C}$ tel que $(x_1, x_2) \in Y_0'(N)(\mathbb{C})$. Maintenant x_2 est isogène à x_1 (ceci est notre façon de dire que x_2 est l'invariant-j d'une courbe elliptique qui est isogène à une autre courbe elliptique d'invariant-j égale à x_1 - on utilise cet abus de terminologie souvent dans cette thèse), donc x_2 est CM aussi. Alors on a un nombre infini (même dense dans la topologie complexe) de points CM $(x_1, x_2) \in Y_0'(N)(\mathbb{C})$. Les courbes $Y_0'(N)$ sont des exemples de courbes modulaires dans $\mathbb{A}^2$. Il n'y a que deux autres candidates évidentes - des droites horizontales et verticales: $V_x = \{x\} \times \mathbb{A}^1$ et $H_y = \mathbb{A}^1 \times \{y\}$, où x et y sont des points CM dans $\mathbb{A}^1(\mathbb{C})$. Alors on a

Théorème 0.3 (André, Edixhoven) *Les courbes de la forme V_x, H_y et $Y_0'(N)$ sont les seules courbes irréductibles dans $\mathbb{A}^2$ contenant un nombre infini de points CM.*

Ce théorème, qui a été démontré d'abord par Edixhoven [19] sous GRH, et puis par André [2] sans hypothèse parasite, règle la Conjecture 0.1 pour $\mathbb{A}^2$.

On continue maintenant avec le cas plus général $\mathbb{A}^n$. Les courbes modulaires dans $\mathbb{A}^n$ sont définies de façon suivante. Rapellons-nous que $\mathrm{GL}_2^+(\mathbb{R})$ agit sur le demi-plan de Poincaré $\mathfrak{H}$ par transformations linéaires fractionelles, et que les points $\tau \in \mathfrak{H}$ déterminent chacun une courbe elliptique $E_\tau \cong \mathbb{C}/(\tau\mathbb{Z} \oplus \mathbb{Z})$ d'invariant $j(\tau)$.

Soit $(\sigma_1, \ldots, \sigma_n) \in \mathrm{GL}_2^+(\mathbb{Q})^n$, et regardons l'application

$$\begin{array}{ccc} \mathfrak{H} & \longrightarrow & \mathbb{A}^n(\mathbb{C}) \\ \tau & \longmapsto & (j(\sigma_1(\tau)), \ldots, j(\sigma_n(\tau))). \end{array}$$

L'image est contenue dans une courbe algébrique irréductible Y dans $\mathbb{A}^n$, et $Y(\mathbb{C})$ contient un nombre infini de points CM, encore parce que les coordonnées des points de Y sont liées par des isogénies. On appelle des courbes construites ainsi des *courbes modulaires* dans $\mathbb{A}^n$. Pour les détails, voir §B.4. Alors on peut déduire du Théorème 0.3 le résultat suivant (Théorème B.4).

Théorème 0.4 *Soit Y une courbe algébrique irréductible dans $\mathbb{A}^n$ telle que aucune des projections standard $Y \to \mathbb{A}^1$ ne soient constante. Alors Y est une courbe modulaire de la forme décrite plus haut si et seulement si $Y(\mathbb{C})$ contient un nombre infini de points CM.*

Mais on n'a pas encore traité la Conjecture 0.1, il nous manque encore les sous-variétés modulaires de dimensions supérieures. On définit les *sous-variétés modulaires* de $\mathbb{A}^n$ comme des produits (à permutations des coordonnées près) de

- points CM dans $\mathbb{A}^1$
- copies de $\mathbb{A}^1$, et

- courbes modulaires dans $\mathbb{A}^m$, pour $m \leq n$.

Encore une fois, les points CM sont denses (dans la topologie complexe) dans ces variétés modulaires. La Conjecture 0.1 implique la réciproque.

Conjecture 0.5 *Soit $Y \subset \mathbb{A}^n$ une variété algébrique irréductible. Alors $Y(\mathbb{C})$ contient un ensemble Zariski-dense de points CM si et seulement si Y est une variété modulaire.*

Edixhoven [21] a démontré que la Conjecture 0.5 est vraie sous GRH pour les corps quadratiques imaginaires.

Il semble qu'on pourrait encore généraliser la Conjecture 0.5 en remplaçant $\mathbb{A}^n$ par le produit de n courbes modulaires. Soit $\Gamma_i \subset \mathrm{SL}_2(\mathbb{Z})$ un sous-groupe de congruence et soit $Y_i = \Gamma_i \backslash \mathfrak{H}$ la courbe modulaire associée, pour $i = 1, \ldots, n$. Alors Y_i n'est autre que "$\mathbb{A}^1$ avec une certaine structure de niveau ajoutée", et on peut remplaçer $\mathbb{A}^n = \prod_{i=1}^n \mathbb{A}^1$ par $X = \prod_{i=1}^n Y_i$ et demander, quelles sont les sous-variétés algébriques $Z \subset X$ contenant des sous-ensembles Zariski-denses de points CM? La réponse (sous GRH) est encore: les sous-variétés modulaires, i.e. produits de:

- points CM,
- copies de Y_i, et
- correspondances de Hecke sur des sous-produits $\prod_{i \in S} Y_i$ pour $S \subset \{1, \ldots, n\}$.

Mais puisque les structures de niveau ne jouent aucun rôle dans la définition de sous-variétés modulaires et de points CM, on voit que cette situation est trivialement équivalente à la Conjecture 0.5.

Le but de cette thèse est de formuler et démontrer un analogue en caractéristique p de la Conjecture 0.5, où on remplace les courbes elliptiques par des modules de Drinfeld de rang 2.

Comme GRH est déjà connue en caractéristique p (le Théorème de Hasse-Weil), on peut s'attendre à ce que l'approche d'Edixhoven fonctionne. Et elle marche, bien qu'il faille changer beaucoup de détails, ce qui reflète les différences entre l'analyse et la topologie dans la caractéristique 0 et la caractéristique p.

0.3 l'Approche d'Edixhoven

La démonstration d'André [3] du Théorème 0.3 utilise un résultat diophantien dû à David Masser, et n'a pas besoin de GRH. Il devrait être possible d'adapter sa démonstration à la caractéristique p, mais il faut d'abord adapter ce résultat de Masser. Toutefois, l'approche d'Edixhoven a l'avantage de sembler plus convenable à généraliser (au cas d'un produit de plusieurs courbes modulaires ou plus généralement au cas des variétés de Shimura), et, puisque GRH ne pose plus de problème en caractéristique p, c'est cette approche qu'on va suivre ici.

Maintenant, on va donner une esquisse de cette approche. Elle repose sur une caractérisation des courbes modulaires en terme de certains opérateurs de Hecke. Soit $n \in \mathbb{N}$ sans facteur carré, et notons T_n l'opérateur de Hecke qui

envoie les sous-ensembles de $\mathbb{A}^2$ vers les sous-ensembles de $\mathbb{A}^2$, définie par son action sur les points:

$$T_n : (x_1, x_2) \mapsto \{(y_1, y_2) \mid \begin{array}{l}\text{il existent des isogénies cycliques} \\ x_1 \to y_1 \text{ et } x_2 \to y_2 \text{ de degré } n.\}\end{array}$$

Alors Edixhoven a montré [19]

Théorème 0.6 (Edixhoven) *Soit $Y \subset \mathbb{A}^2$ une courbe algébrique irréductible, et supposons que les deux projections $p_i : Y \to \mathbb{A}^1$ soient dominantes de degré d_i, pour $i = 1, 2$. Supposons que $Y \subset T_n(Y)$ pour un $n \in \mathbb{N}$ sans facteur carré, composé de nombres premiers $p \geq \max(13, d_1)$. Alors Y est une courbe modulaire $Y_0'(N)$ pour un certain $N \in \mathbb{N}$.*

La démonstration du Théorème 0.6 est de nature topologique, et n'utilise pas GRH. Pour l'appliquer, il faut rappeler quelques propriétés des points CM.

Soit E une courbe elliptique CM, avec $\mathcal{O} = \mathrm{End}(E)$ un ordre dans le corps quadratique imaginaire K, et soit p un nombre premier décomposé dans K, et qui ne divise pas le conducteur de $\mathcal{O}$. Dans ce cas, on dit que p est décomposé dans $\mathcal{O}$, et on peut écrire $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$ où $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Soit $\sigma = (\mathfrak{p}_1, K(j(E))/K))$ le Frobenius associé à $\mathfrak{p}_1$. Alors il résulte de la théorie CM (voir [41, Theorem 10.5]) que E et E^σ sont liées par une isogénie cyclique de degré p.

Soit $Y \subset \mathbb{A}^2$ une courbe algébrique irréductible contenant un nombre infini de points CM, et supposons pour simplicité que Y soit définie sur $\mathbb{Q}$. Maintenant, soit $(x_1, x_2) \in Y(\overline{\mathbb{Q}})$ un point CM, soit $\mathcal{O}_i = \mathrm{End}(x_i)$ un ordre dans le corps quadratique imaginaire K_i, pour $i = 1, 2$, et posons $K = K_1K_2$. Soit p un nombre premier qui se décompose dans $\mathcal{O}_1$ et dans $\mathcal{O}_2$. Choisissons un premier $\mathfrak{P}$ de $K(x_1, x_2)$ au-dessus de p, et notons par $\sigma \in \mathrm{Gal}(K(x_1, x_2)/\mathbb{Q})$ le Frobenius de $\mathfrak{P}$. Alors x_i est lié à x_i^σ par une isogénie cyclique de degré p, pour $i = 1, 2$, donc

$$(x_1, x_2) \in Y \cap T_p(Y^\sigma) = Y \cap T_p(Y). \tag{1}$$

En plus, toute l'orbite de Galois de (x_1, x_2) est contenue dans cette intersection. Or, l'indice de cette intersection est $2d_1d_2(p+1)^2$. Donc, si l'orbite de Galois de (x_1, x_2) est suffisamment grande, alors l'intersection est impropre, $Y \subset T_p(Y)$, et on peut appliquer le Théorème 0.6.

Comme $\mathrm{Gal}(K(x_i)/K) \cong \mathrm{Pic}(\mathcal{O}_i)$, on voit que l'orbite de Galois croît en fonction du nombre de classes de $\mathcal{O}_i$. Puis on utilise le Théorème de Siegel sur le nombre de classes d'un corps quadratique imaginaire, ainsi qu'une version très forte du Théorème de Čebotarev (c'est là qu'on utilise GRH), pour montrer que, si le discriminant de $\mathcal{O}_i$ est suffisamment grand (ce qui équivaut à ce que la hauteur de x_i soit suffisamment grande, voir Appendice B), alors il existe un nombre premier p décomposé dans $\mathcal{O}_1$ et dans $\mathcal{O}_2$ mais qui est encore assez petit par rapport au nombre de classes de $\mathcal{O}_i$ pour que l'intersection (1) soit impropre. Alors le Théorème 0.3 s'ensuit.

On a encore plus. Notre résultat est effectif (puisque le Théorème de Siegel est effectif sous GRH): On peut borner la hauteur des points CM sur les courbes non modulaires $Y \subset \mathbb{A}^2$ en termes du degré de Y et du degré du corps de définition de Y. Voir l'appendice B pour plus de détails.

Ceci permet de résoudre la Conjecture 0.5 pour $\mathbb{A}^2$ (sous GRH). Quand on étend cette approche au cas de $\mathbb{A}^n$ pour $n \geq 2$ on a besoin d'un peu de géométrie algébrique compliquée mais élémentaire, mais l'idée de base reste la même. On montre d'abord qu'une variété algébrique $Z \subset \mathbb{A}^n$ est modulaire si elle est stabilisée par un opérateur de Hecke convenable. Puis, étant donné une variété algébrique $Y \subset \mathbb{A}^n$ contenant un sous-ensemble Zariski-dense de points CM, on applique ce résultat pour couvrir Y par une famille Zariski-dense de sous-courbes modulaires. Puis on montre que Y est modulaire. Cette approche a été trouvée par Edixhoven [21], sous GRH.

Enfin, on remarque que l'approche esquissée au-dessus est très similaire à la démonstration de Marc Hindry de la Conjecture de Manin-Mumford, voir [35] et [36].

0.4 Esquisse de cette thèse

On considère maintenant un analogue de la Conjecture 0.5 en caractéristique p. Soit p un nombre premier impair (tous ce qu'on fait ici devrait rester valable pour $p = 2$ aussi, mais il faudra changer beaucoup de petits détails), et soit q une puissance de p. Soit $A = \mathbb{F}_q[T]$ et $k = \mathbb{F}_q(T)$, et notons par ∞ la place de k avec uniformisante $1/T$. Soit $k_\infty = \mathbb{F}_q((1/T))$ le complété de k à ∞ et soit $\mathbf{C} = \hat{\bar{k}}_\infty$ le complété de la clôture algébrique de k_∞, qui est encore algébriquement clos. On remarque que A, k, k_∞ et $\mathbf{C}$ jouent les rôles de $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, respectivement.

On regarde $\mathbb{A}^n$ comme espace de modules de n-uples de A-modules de Drinfeld de rang 2 sur $\mathbf{C}$ (voir le Chapitre 1 pour une introduction aux modules de Drinfeld et aux variétés modulaires), où le n-uple $(\phi^1, \ldots, \phi^n)$ correspond au point $(j(\phi^1), \ldots, j(\phi^n)) \in \mathbb{A}^n(\mathbf{C})$. Alors un point $(x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbf{C})$ est un *point CM* si les modules de Drinfeld correspondants sont tous à multiplication complexe. On définit les sous-variétés modulaires de $\mathbb{A}^n$ de la même façon que dans le cas classique, ce sont les sous-variétés déterminées par des conditions d'isogénie imposées entre les coordonées.

Les résultats principaux de cette thèse sont

Théorème 0.7 *Soit q impair. Soient d et m des entiers positifs donnés, et soit g un entier non negatif donné. Alors il existe une constante effectivement calculable $B = B(d, m, g)$ vérifiant la propriété suivante. Soit Y une courbe algébrique irréductible dans $\mathbb{A}^2$ de degré d, définie sur une extension finie F de k de degré $[F : k] = m$ et de genre $g(F) = g$. Alors Y est une courbe modulaire $Y_0'(N)$ pour un certain $N \in A$ si et seulement si $Y(\mathbf{C})$ contient un point CM de hauteur supérieure à B.*

Théorème 0.8 *Soit q impair. Soit $Y \subset \mathbb{A}^n$ une variété algébrique irréductible. Alors $Y(\mathbf{C})$ contient un sous-ensemble Zariski-dense S de points CM si et seulement si Y est une variété modulaire.*

Ces théorèmes sont des analogues du Théorème 0.3 et de la Conjecture 0.5, respectivement.

Maintenant, on présente un résumé des chapitres.

Chapitre 1 : "Preliminaries". On présente une introduction générale sur les modules de Drinfeld dans §1.1, comme on peut le trouver dans la littérature. Dans §1.2 on présente la théorie de modules de Drinfeld de rang 2 à multiplication complexe. On commence par quelque propriétés générales des corps de fonctions quadratiques "imaginaires", puis on continue avec la théorie de corps de classes pour les corps de fonctions introduisant les "corps de classes d'anneaux", et on énonce le Théorème de Čebotarev pour les corps de fonctions. Puis on peut énoncer le Main Theorem de la multiplication complexe de modules de Drinfeld. Dans §1.3 on commence par décrire le demi-plan de Drinfeld et l'action de $\mathrm{PGL}_2(k_\infty)$, et puis on construit des courbes modulaires de Drinfeld et des variétés modulaires dans $\mathbb{A}^n$. Les résultats dans ce chapitre sont bien connus, sauf peut-être quelques définitions et résultats dans §1.3, et même eux devraient être connus par les experts.

Chapitre 2 : "Hecke operators". Dans ce chapitre on développe la plupart du formalisme géométrique dont on a besoin pour prouver nos résultats principaux. Après avoir traité les notions de base des opérateurs de Hecke et des orbites de Hecke dans §2.1, on regarde brièvement les points stabilisés par des opérateurs de Hecke dans §2.2. Puis on montre un résultat fondamental sur la surjectivité des projections entre opérateurs de Hecke (Theorem 2.1) dans §2.3. Puis on prouve un analogue du Théorème 0.6 dans §2.4 (Theorem 2.2), où on applique des méthodes de la topologie et de la théorie des groupes. Finalement, dans §2.5, on étend ce résultat au cas des sous-variétés de dimension supérieure stabilisées par des opérateurs de Hecke (Theorem 2.3). Les résultats dans ce chapitre sont nouveaux, mais il existe déjà des analogues en caractéristique 0, dont quelques uns sont parus dans la littérature, et dont la plupart devrait être connus par certains experts.

Chapitre 3 : "Heights of CM points". C'est dans ce chapitre qu'on démontre nos résultats principaux. On commence par rapeler quelques notions de bases sur les fonctions zêta et on déduit une borne inférieure du nombre de classes d'un corps de fonctions quadratique dans §3.1. Dans §3.2 on déduit quelques approximations analytiques des invariants-j CM (Theorem 3.3). Dans §3.3 on définit la notion de la *hauteur CM* d'un point CM dans $\mathbb{A}^n$, et on relie cette hauteur CM à la hauteur usuelle arithmétique (Proposition 3.3.4), utilisant les approximations analytiques obtenues dans la section précédente. Puis, en utilisant la hauteur CM, les propriétés arithmétiques des points CM, le Théorème de Čebotarev et notre minoration du nombre des classes, on démontre le Théorème 0.7 (Theorem 3.4) dans §3.4. De façon similaire, on démontre le Théorème 0.8 (Theorem 3.5) dans §3.5. On termine le chapitre avec quelques commentaires dans §3.6. Encore, les résultats dans ce chapitre sont nouveaux, mais il existe des analogues en caractéristique 0 dans [21].

Appendice A : "Some results from group theory". Dans cet appendice on recueille quelques résultats de la théorie des groupes dont on a besoin dans

le Chapitre 2. La plupart de ces résultats sont démontrés ici, à cause du manque de références adéquates.

Appendice B : "Heights of CM points on complex affine curves". Cet appendice est paru comme article dans *The Ramanujan Journal* [8]. Il s'agit du cas de caractéristique 0. On introduit la notion de *hauteur CM* pour les courbes elliptiques CM, et on montre comment les résultats d'Edixhoven [19] peuvent être rendus effectifs (sous GRH). On décrit aussi les courbes modulaires dans $\mathbb{A}^n$, et on déduit le Théorème 0.4 du Théorème 0.3.

Appendice C : "Distinguished liftings and the André-Oort conjecture". Cet appendice est un article à paraître dans *Quaestiones Math.* [9]. On étudie un certain problème de relèvement, où on veut relever une variété algébrique affine d'un corps fini à un corps de nombres, soumis à certaines conditions, qui reposent sur l'interprétation de l'espace $\mathbb{A}^n$ comme espace de modules de n-tuples de courbes elliptiques. Ce problème est une variante proche de la Conjecture 0.5, et on applique quelques résultats connus sur la Conjecture d'André-Oort à ce problème de relèvement. On démontre aussi quelques cas très spéciaux de la Conjecture 0.5, qui se rapportent à ce problème de relèvement.

Introduction in English

The aim of this thesis is to formulate and prove an analogue of the André-Oort conjecture for the product of Drinfeld modular curves.

0.5 The André-Oort conjecture

A general statement of the André-Oort conjecture is the following.

Conjecture 0.1 (André-Oort) *Let X be a Shimura variety and $Z \subset X$ a geometrically irreducible algebraic subvariety. Then $Z(\mathbb{C})$ contains a Zariski-dense subset of special points if and only if Z is of Hodge type.*

The exact definitions of Shimura varieties, special points and subvarieties of Hodge type would take us too far afield. Instead, we refer the reader to [47], as well as to [20, 22, 48, 49, 71].

Intuitively, however, the conjecture can be understood as follows. A Shimura variety is a moduli space X of certain objects (usually abelian varieties, or, more generally, motives) equipped with some extra structure (such as polarizations, endomorphisms and level structures). A subvariety of Hodge type is essentially a subvariety which is a Shimura variety in its own right, i.e. a moduli space of the same objects, but with more stringent requirements on the extra structure. Special points are just zero-dimensional subvarieties of Hodge type. Think of strengthening the requirements on the extra structure so far that the resulting moduli space has dimension zero, but is not empty. The resulting points, which are dense (in the complex topology) in X, are then the special points. The conjecture states that the only subvarieties Z containing a (Zariski) dense set of special points are precisely those obtained as moduli spaces with stronger conditions on the extra structure.

In the next section we will study a special case in more detail - and our definitions will be fully rigorous.

Conjecture 0.1 was first stated, for the case $\dim(Z) = 1$, as a problem in Yves André's book [1], which appeared in 1989. Later, Frans Oort stated Conjecture 0.1 for the case where $X = \mathcal{A}_{g,1}$ is the moduli space of principally polarized abelian varieties of dimension g (see [47, 53, 54]). In this case the special points correspond precisely to the abelian varieties with complex multiplication (CM), and they are called CM points.

The above conjecture exhibits striking similarities with the Manin-Mumford conjecture, which was proved by Michel Raynaud in 1983 [56, 57]:

Theorem 0.2 (Raynaud) *Let A be an abelian variety, and $V \subset A$ a geometrically irreducible algebraic subvariety. Then $V(\mathbb{C})$ contains a Zariski-dense subset of torsion points (of A) if and only if $V = t + B$, where $t \in A_{tors}(\mathbb{C})$ and $B \subset A$ is an abelian subvariety.*

The analogy is given by

André-Oort	Manin-Mumford
Shimura varieties	abelian varieties
special points	torsion points
subvarieties of Hodge type	translates of abelian subvarieties by torsion points

It is in fact this analogy that in part suggested Conjecture 0.1 in the first place. André [2] has formulated a very general conjecture that implies both conjectures.

The following special cases of Conjecture 0.1 have already been proved.

Moonen, 1994, [47, 48, 49] Suppose $X = \mathcal{A}_{g,1,m}$ is the moduli space of principally polarized abelian varieties with full level-m structure. Let $Z \subset X$ be an irreducible algebraic subvariety containing a Zariski-dense subset S of CM points with the following property: There exists a rational prime p such that every point of S is the Serre-Tate canonical lift of its reduction modulo a place above p. Then Z is of Hodge type.

Edixhoven, 1995, [19] X is the product of two elliptic[3] modular curves, assuming that the Generalized Riemann Hypothesis (GRH) holds for imaginary quadratic fields.

André, 1995, [2] X is the product of two elliptic modular curves (i.e. as above, but without assuming GRH).

Yafaev, 1999, [72] X is the product of two Shimura curves associated to quaternion algebras over $\mathbb{Q}$, assuming GRH holds for imaginary quadratic fields.

Edixhoven, 1999, [20, 21] X is a Hilbert modular surface, or X is the product of n elliptic modular curves. For both results one needs to assume GRH.

Belhaj-Dahmane, 2001, [6] Suppose $X \subset \mathcal{A}_{g,1}$ is the curve corresponding to the Jacobians of curves of the form $y^n = x(x-1)(x-\lambda)$ as $\lambda \in \mathbb{C}$ varies. Then X is not of Hodge type, and (under some technical restrictions) only finitely many of these Jacobians (for n fixed) have complex multiplication.

Edixhoven and Yafaev, 2001, [22] Let X be a Shimura variety and $Z \subset X$ a curve. Then Z is of Hodge type if it contains an infinite set S of special points, all of which lie in the same Hecke orbit.

[3] we use the term "elliptic" modular curves to emphasise the distinction with Drinfeld modular curves

The above known cases have at least two applications. Firstly, the result of Edixhoven and Yafaev provides the final ingredient to fix a gap in a result of Wolfart [70] on the algabraicity of values of hypergeometric functions at algebraic numbers, see [6, 13, 22, 71].

As a second application, Cornut [16] used Moonen's result (he could also have used Edixhoven's result on products of modular curves) to derive a simpler proof of Mazur's conjecture on higher Heegener points [45], after already having proved that conjecture using more difficult techniques [15]. One may hope to gain similar insight on Heegner points on "modular" elliptic curves over rational function fields, combining the results of this thesis with Cornut's methods. That is the object of work in progress, which was unfortunately not completed in time to be included here.

0.6 The case of elliptic modular curves

In this thesis we are interested in the following special case. We may view affine n-space $\mathbb{A}^n$ as the moduli space of n-tuples of elliptic curves, where a tuple $(E_1, \ldots, E_n)$ corresponds to the point $(j(E_1), \ldots, j(E_n)) \in \mathbb{A}^n(\mathbb{C})$, and $j(E)$ denotes the j-invariant of the (complex) elliptic curve E. Then $\mathbb{A}^n$ is a Shimura variety[4], and the special points are the *CM points*, i.e. points of the form $(x_1, \ldots, x_n)$, where each x_i is the j-invariant of an elliptic curve with complex multiplication. Now Conjecture 0.1 states that an irreducible algebraic variety $X \subset \mathbb{A}^n$ contains a Zarisksi-dense subset of CM points if and only if X is a subvariety of Hodge type, which we will call a *modular* subvariety. But what does that mean in this situation?

We first consider the case $n = 2$. Then $\mathbb{A}^2$, the affine plane, parametrizes isomorphism classes of ordered pairs of elliptic curves. The only modular subvariety $X \subset \mathbb{A}^2$ of dimension 2 is $\mathbb{A}^2$ itself, whereas those of dimension 0 are the CM points. So it remains to classify the modular subvarieties of dimension 1 - the *modular curves*. Let $N \in \mathbb{N}$ and denote by $Y_0(N)$ the modular curve parametrising pairs (E_1, E_2, f) of elliptic curves linked by a cyclic isogeny $f : E_1 \to E_2$ of degree N. This just means that $\ker(f) \cong \mathbb{Z}/N\mathbb{Z}$. Then we may map $Y_0(N)$ into $\mathbb{A}^2$ by sending (E_1, E_2, f) to the point $(j(E_1), j(E_2))$. The image, which we denote by $Y_0'(N)$, is an irreducible algebraic curve defined over $\mathbb{Q}$. It is a birational model of $Y_0(N)$, but is not smooth in general. Now it is easy to see that $Y_0'(N)(\mathbb{C})$ contains infinitely many CM points: there are infinitely many $x_1 \in \mathbb{C}$ corresponding to CM elliptic curves, and for each of them we have at least one $x_2 \in \mathbb{C}$ such that $(x_1, x_2) \in Y_0'(N)(\mathbb{C})$. Now x_2 is isogenous to x_1 (this is our short-hand way of saying that x_2 is the j-invariant of an elliptic curve isogenous to an elliptic curve with j-invariant x_1 - we will use this slight abuse of terminology throughout this thesis), hence each x_2 is also CM. So we have infinitely many CM points $(x_1, x_2) \in Y_0'(N)(\mathbb{C})$, in fact, these points are even dense in the complex topology. So the curves $Y_0'(N)$ are examples of modular curves in $\mathbb{A}^2$. The only other obvious candidates are horizontal and

[4] equivalently, we could consider $\mathbb{A}^n/S_n$, the space of products of n elliptic curves. We can embed $\mathbb{A}^n/S_n$ into $\mathcal{A}_{n,1}$.

vertical lines: $V_x = \{x\} \times \mathbb{A}^1$ and $H_y = \mathbb{A}^1 \times \{y\}$, where x and y are CM points in $\mathbb{A}^1(\mathbb{C})$. Then we have

Theorem 0.3 (André, Edixhoven) *The curves of the form V_x, H_y and $Y_0'(N)$ are the only irreducible curves in $\mathbb{A}^2$ containing infinitely many CM points.*

This theorem, first proved by Edixhoven [19] under assumption of GRH, and then unconditionally by André [2], settles Conjecture 0.1 for $\mathbb{A}^2$.

We now move on to the more general case $\mathbb{A}^n$. The modular curves in $\mathbb{A}^n$ are given as follows. Recall that $\mathrm{GL}_2^+(\mathbb{R})$ acts on the Poincaré upper half-plane $\mathfrak{H}$ by fractional linear transformations, and that the points $\tau \in \mathfrak{H}$ each determine an elliptic curve $E_\tau \cong \mathbb{C}/(\tau\mathbb{Z} \oplus \mathbb{Z})$ with j-invariant $j(\tau)$. Let $(\sigma_1, \ldots, \sigma_n) \in \mathrm{GL}_2^+(\mathbb{Q})^n$, and consider the map

$$\begin{array}{ccc} \mathfrak{H} & \longrightarrow & \mathbb{A}^n(\mathbb{C}) \\ \tau & \longmapsto & (j(\sigma_1(\tau)), \ldots, j(\sigma_n(\tau))). \end{array}$$

The image lies on an irreducible algebraic curve Y in $\mathbb{A}^n$, and $Y(\mathbb{C})$ contains infinitely many CM points, again because the various coordinates of points on Y are isogenous to each other. The curves thus constructed are called *modular curves* in $\mathbb{A}^n$. For details of this construction, see §B.4. Then one may deduce from Theorem 0.3 the following result (Theorem B.4).

Theorem 0.4 *Let Y be an irreducible algebraic curve in $\mathbb{A}^n$ such that none of the standard projections $Y \to \mathbb{A}^1$ are constant. Then Y is a modular curve of the form described above if and only if $Y(\mathbb{C})$ contains infinitely many CM points.*

But that is not enough to settle Conjecture 0.1, as we have not yet treated subvarieties of higher dimension. We define the *modular varieties* in $\mathbb{A}^n$ to be products (up to a permutation of coordinates) of

- CM points in $\mathbb{A}^1$
- copies of $\mathbb{A}^1$, and
- modular curves in $\mathbb{A}^m$, for $m \leq n$.

Again, the CM points are dense (in the complex topology) on these modular varieties. Conjecture 0.1 claims the converse.

Conjecture 0.5 *Let $Y \subset \mathbb{A}^n$ be an irreducible algebraic variety. Then $Y(\mathbb{C})$ contains a Zariski-dense subset of CM points if and only if Y is a modular variety.*

Edixhoven [21] has proved that Conjecture 0.5 is true if GRH holds for imaginary quadratic fields.

We mention in passing that one can seemingly generalize Conjecture 0.5 by replacing $\mathbb{A}^n$ with the product of n modular curves. Let $\Gamma_i \subset \mathrm{SL}_2(\mathbb{Z})$ be congruence subgroups and $Y_i = \Gamma_i \backslash \mathfrak{H}$ the modular curves associated to the Γ_i, for $i = 1, \ldots, n$. Then Y_i is just "$\mathbb{A}^1$ with some level structure added",

and we may replace $\mathbb{A}^n = \prod_{i=1}^n \mathbb{A}^1$ by $X = \prod_{i=1}^n Y_i$ and ask, which algebraic subvarieties $Z \subset X$ contain Zariski-dense subsets of CM points? The answer (under GRH) is again modular subvarieties, i.e. products of:

- CM points,
- whole factors Y_i, and
- Hecke correspondences on subproducts $\prod_{i \in S} Y_i$ for $S \subset \{1, \ldots, n\}$.

But as the level structures play absolutely no role in the definition of modular subvarieties and CM points, we see that this situation is trivially equivalent to Conjecture 0.5.

The aim of this thesis is to state and prove a characteristic p analogue of Conjecture 0.5, where elliptic curves are replaced by rank 2 Drinfeld modules.

As GRH is already known to hold in characteristic p (the Hasse-Weil theorem), Edixhoven's approach is expected to work. And it does, although some details had to be changed, reflecting differences between the analysis and topology in characteristic 0 and in characteristic p.

0.7 Edixhoven's approach

André's proof [3] of Theorem 0.3 uses a transcendence result of David Masser, and has the advantage that it does not need GRH. It should also be possible to adapt this proof to characteristic p, but one must first adapt Masser's result. However, Edixhoven's proof has the advantage that it seems to generalize (to products of several modular curves, or to more general Shimura varieties) more readily. And as GRH is no problem in characteristic p, it is the approach we follow here.

We now present a brief outline of Edixhoven's approach. It is based on a characterization of modular curves in terms of certain Hecke operators. Let $n \in \mathbb{N}$ be square-free and denote by T_n the Hecke operator which sends subsets of $\mathbb{A}^2$ to subsets of $\mathbb{A}^2$, generated by its action on single points:

$$T_n : (x_1, x_2) \mapsto \{(y_1, y_2) \mid \begin{array}{l} \text{there exist cyclic isogenies} \\ x_1 \to y_1 \text{ and } x_2 \to y_2 \text{ of degree } n.\} \end{array}$$

Then Edixhoven has proved [19]

Theorem 0.6 (Edixhoven) *Let $Y \subset \mathbb{A}^2$ be an irreducible algebraic curve, and suppose the two projections $p_i : Y \to \mathbb{A}^1$ are dominant and have degrees d_i, for $i = 1, 2$. Suppose that $Y \subset T_n(Y)$ for some square-free n composed of primes $p \geq \max(13, d_1)$. Then Y is a modular curve $Y_0'(N)$ for some $N \in \mathbb{N}$.*

The proof of Theorem 0.6 is topological in nature, and does not require GRH. To apply it we must recall some properties of CM points.

Let E be a CM elliptic curve, with $\mathcal{O} = \mathrm{End}(E)$ an order in the imaginary quadratic field K, and let p be a rational prime which splits in K and does not

divide the conductor of $\mathcal{O}$. In this case we say that p splits in $\mathcal{O}$, and we may write $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Let $\sigma = (\mathfrak{p}_1, K(j(E))/K))$ be the Frobenius element associated to $\mathfrak{p}_1$. Then it follows from the Main Theorem of complex multiplication (see [41, Theorem 10.5]) that E and E^σ are linked by a cyclic isogeny of degree p.

Let $Y \subset \mathbb{A}^2$ be an irreducible algebraic curve containing infinitely many CM points, and suppose for simplicity that Y is defined over $\mathbb{Q}$. Now let $(x_1, x_2) \in Y(\overline{\mathbb{Q}})$ be a CM point, let $\mathcal{O}_i = \mathrm{End}(x_i)$ be an order in the imaginary quadratic field K_i, for $i = 1, 2$, and set $K = K_1K_2$. Let p be a prime that splits completely in $\mathcal{O}_1$ and in $\mathcal{O}_2$. Now pick a prime $\mathfrak{P}$ of $K(x_1, x_2)$ lying over p, and let $\sigma \in \mathrm{Gal}(K(x_1, x_2)/\mathbb{Q})$ denote the Frobenius element associated to $\mathfrak{P}$. Then we find that x_i is linked to x_i^σ via a cyclic isogeny of degree p, for $i = 1, 2$, so

$$(x_1, x_2) \in Y \cap T_p(Y^\sigma) = Y \cap T_p(Y). \tag{1}$$

Moreover, the whole Galois orbit of (x_1, x_2) lies in this intersection. On the other hand, the intersection index is given by $2d_1d_2(p+1)^2$. So if the Galois orbit of (x_1, x_2) is sufficiently large, then the intersection is improper, $Y \subset T_p(Y)$, and we can apply Theorem 0.6.

As $\mathrm{Gal}(K(x_i)/K) \cong \mathrm{Pic}(\mathcal{O}_i)$, we see that the Galois orbit grows with the class number of $\mathcal{O}_i$. One now uses Siegel's Theorem on the class number of imaginary quadratic fields, together with a strong version of the Čebotarev theorem (which needs GRH) to show that, if the discriminant of $\mathcal{O}_i$ is sufficiently large (which is equivalent to x_i having a large arithmetic height, see Appendix B) then there exists a prime p which splits in $\mathcal{O}_1$ and $\mathcal{O}_2$, and is yet sufficiently small compared to the class number of $\mathcal{O}_i$ that the intersection (1) is improper. Theorem 0.3 follows.

We have even more. The above theorem is effective (as Siegel's theorem is effective under GRH): we may bound the heights of CM points on non-modular curves $Y \subset \mathbb{A}^2$ in terms of the degree of Y and the degree of the field of definition of Y. See Appendix B for the details.

That solves Conjecture 0.5 for $\mathbb{A}^2$ (assuming GRH). When one extends the above approach to attack the case of $\mathbb{A}^n$ for $n \geq 2$ a lot of messy (but elementary) algebraic geometry enters the picture, but the basic idea is still the same. One first shows that a variety $Z \subset \mathbb{A}^n$ is modular if it is fixed by a suitable Hecke operator. Then, given a variety $Y \subset \mathbb{A}^n$ containing a Zariski-dense set of CM points, one applies this result to cover Y with a Zariski-dense family of modular subcurves. One then concludes that Y is itself a modular variety. This approach was found by Edixhoven [21], and needs GRH.

As a closing remark, we point that the approach outlined above is very similar to Hindry's proof of the Manin-Mumford conjecture, see [35] and [36].

0.8 Outline of this thesis

We now consider an analogue of Conjecture 0.5 in characteristic p. Let p be an odd prime (everything we do should also be possible for $p = 2$, but many details would have to be modified), and let q be a power of p. Let $A = \mathbb{F}_q[T]$

and $k = \mathbb{F}_q(T)$, and denote by ∞ the place of k with uniformizer $1/T$. Let $k_\infty = \mathbb{F}_q((1/T))$ be the completion of k with respect to the place ∞ and $\mathbf{C} = \hat{\bar{k}}_\infty$ be the completion of the algebraic closure of k_∞. Then $\mathbf{C}$ is again algebraically closed. We point out that A, k, k_∞ and $\mathbf{C}$ play the roles of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, respectively.

We now view $\mathbb{A}^n$ as the moduli space of n-tuples of rank 2 Drinfeld A-modules over $\mathbf{C}$ (see Chapter 1 for an introduction to Drinfeld modules and modular varieties), where the tuple $(\phi^1, \ldots, \phi^n)$ corresponds to the point $(j(\phi^1), \ldots, j(\phi^n)) \in \mathbb{A}^n(\mathbf{C})$. Then a point $(x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbf{C})$ is called a *CM point* if the corresponding Drinfeld modules all have complex multiplication. One defines the modular subvarieties of $\mathbb{A}^n$ in exactly the same way as in the classical case, they are the varieties determined by isogeny conditions between the coordinates.

The principal results of this thesis are

Theorem 0.7 *Assume that q is odd. Let d and m be given positive integers, and g a given non-negative integer. Then there exists an effectively computable constant $B = B(d, m, g)$ such that the following holds. Let Y be an irreducible algebraic curve in $\mathbb{A}^2$ of degree d, defined over a finite extension F of k of degree $[F : k] = m$ and genus $g(F) = g$. Then Y is a modular curve $Y_0'(N)$ for some $N \in A$ if and only if $Y(\mathbf{C})$ contains a CM point of arithmetic height at least B.*

and

Theorem 0.8 *Suppose that q is odd. Let $Y \subset \mathbb{A}^n$ be an irreducible algebraic variety. Then $Y(\mathbf{C})$ contains a Zariski-dense subset S of CM points if and only if Y is a modular variety.*

They are analogues of Theorem 0.3 and Conjecture 0.5, respectively.

We now give a summary of the individual chapters.

Chapter 1 : Preliminaries. We provide a basic introduction to Drinfeld modules in §1.1, as can be found in any number of papers in the literature. In §1.2 we describe the theory of rank 2 Drinfeld modules with complex multiplication. We first present some general properties of "imaginary" quadratic function fields, and then move on to treat class field theory for function fields, introducing ring class fields, and state the Čebotarev Theorem for function fields. Then we go on to state the Main Theorem of complex multiplication for Drinfeld modules. In §1.3 we begin by introducing the Drinfeld upper half-plane and its $\mathrm{PGL}_2(k_\infty)$-action. We then take quotients for subgroups of this action to construct various Drinfeld modular curves. Finally we construct Drinfeld modular curves and modular varieties in $\mathbb{A}^n$. The results of this chapter are well-known, except possibly for some definitions and results in §1.3, and even these should already be known to some experts.

Chapter 2 : Hecke operators. In this chapter we develop most of the geometric machinery that we will need to prove our main results. After providing the basic definitions and properties of Hecke operators and Hecke

orbits in §2.1, we briefly consider the stable points of Hecke operators in §2.2. Then we prove a fundamental result on the surjectivity of projections between Hecke operators (Theorem 2.1) in §2.3. We next prove an analogue of Theorem 0.6 in §2.4 (Theorem 2.2), where we apply topological and group-theoretic methods. Lastly, in §2.5, we extend this result to higher-dimensional subvarieties stabilized by Hecke operators (Theorem 2.3). The results in this chapter are basically new, but have close analogues in characteristic 0, some of which have appeared in the literature, and most of which should be known to some experts.

Chapter 3 : Heights of CM points. In this chapter we will prove the main results mentioned above. We begin by recalling some basic properties of zeta functions and derive a lower bound on the class numbers of quadratic function fields in §3.1. In §3.2 we derive some analytic estimates of CM j-invariants (Theorem 3.3). In §3.3 we define the *CM height* of a CM point in $\mathbb{A}^n$, and relate this height with the usual arithmetic height (Proposition 3.3.4), using the estimates obtained in the previous section. Then, using the CM height together with arithmetic properties of CM points, the Čebotarev theorem and our lower bounds of class numbers, we prove Theorem 0.7 (Theorem 3.4) in §3.4. Similarly, we prove Theorem 0.8 (Theorem 3.5) in §3.5. We close the chapter with some concluding comments in §3.6. Again, the main results in this chapter are new, but have characteristic 0 analogues which have essentially appeared in [21].

Appendix A : Some results from group theory. This appendix gathers together an assortment of results from group theory which are needed in Chapter 2. Most of these results are proved here for lack of suitable references.

Appendix B : Heights of CM points on complex affine curves. This appendix appeared as an article in *The Ramanujan Journal* [8]. It is concerned with the characteristic zero case. We introduce the notion of *CM heights* for elliptic curves with complex multiplication, and show how Edixhoven's results [19] can be made effective (under GRH). We also describe affine models of modular curves in $\mathbb{A}^n$, and derive Theorem 0.4 from Theorem 0.3.

Appendix C : Distinguished liftings and the André-Oort conjecture. This appendix is due to appear as an article in *Quaestiones Math.* [9]. We study a certain lifting problem, where one wants to lift affine varieties from finite fields to number fields, subject to certain conditions, which rely on interpreting the ambient space $\mathbb{A}^n$ as the moduli space of n-tuples of elliptic curves. The problem is a close variant of Conjecture 0.5, and we apply some known cases of the André-Oort conjecture to these lifting problems. We also prove some very special cases of Conjecture 0.5, which pertain specifically to the lifting problem.

0.9 Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor, Marc Hindry, for his constant support, his cheerful advise and for all the mathematics that I have learnt from him. In addition, he has invested much time and effort into a careful reading of this thesis, and his numerous comments and insights have contributed significantly to this work.

I would like to thank Hans-Georg Rück who first suggested to me that one might replace elliptic curves by Drinfeld modules in the André-Oort conjecture in 1999. I only acted on this idea two years later, but it has lead to this thesis.

I am much honoured that Bas Edixhoven and Ernst-Ulrich Gekeler have agreed to referee this thesis, and I would like to thank them for their effort and for serving on my jury.

I am also very grateful to Bas Edixhoven for his many patient explanations (especially in the last minute, when all seemed lost!), and for making a preliminary version of [21] available to me.

I would like to thank Yves Andre and Laurent Denis for accepting to be part of my jury.

I would also like to thank Henning Stichtenoth for providing me with Proposition 3.1.4, which allowed me to drop the condition $q \geq 5$ in my main results.

I take this opportunity to thank Jean-Pierre Serre, too, for pointing out an error in an earlier version of Corollaries A.2.5 and A.2.6.

During the years I spent working on this thesis, I have benefited from discussions with Yves André, Barry Green, Gerhard Frey, Joseph Oesterlé, Hans-Georg Rück, Henning Stichtenoth, Brink van der Merwe, Ingo Waschkies, Andrei Yafaev and Jing Yu. I would like to take this opportunity to thank them all.

My friends and family have made my graduate life much more bearable, and lent me courage when I most needed it. I would like to thank in particular Carola, Catriona, Christine, Erik, Hannes, Ingo, Ivar, Klaus, Lucie, Magda, Pietro, Uschi and most of all BL and OB, to whom this thesis is dedicated.

Lastly, this thesis was written with the financial support of a *Bourse du Gouvernement Français* (Number 1998/2672), and I would like to thank the French government for their generosity.

0.10 Notation and conventions

Throughout this thesis, we adhere to the following conventions.

A ring always has an identity, and is commutative unless stated otherwise. A field is always commutative.

The algebraic closure of a field F is denoted by $\overline{F}$. The separable closure is denoted by F^{sep}.

A variety X over a field F is a closed algebraic set in the sense of [32, Chapter 1], defined by polynomial equations with coefficients in F. We do not assume it to be irreducible. X is called F-irreducible, if it is irreducible over F (i.e. it cannot be written as a finite union of proper subvarieties defined over F), but not necessarily irreducible over $\overline{F}$. If X is $\overline{F}$-irreducible, then we say it is absolutely or geometrically irreducible.

For a ring R, we use the following definitions of linear groups over R. $\mathrm{GL}_2(R)$ and $\mathrm{SL}_2(R)$ are the groups of 2×2 matrices over R, whose determinants are units and the identity, respectively. We denote by $Z(R)$ (or sometimes $Z(R^*)$) the group of scalar matrices $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$, for $x \in R^*$. We define the projective linear groups by

$$\begin{aligned} \mathrm{PGL}_2(R) &= \mathrm{GL}_2(R)/Z(R) \\ \mathrm{PSL}_2(R) &= \mathrm{SL}_2(R)/(\mathrm{SL}_2(R) \cap Z(R)) \cong \mathrm{SL}_2(R)/\{x \in R^* \mid x^2 = 1\}. \end{aligned}$$

All logarithms are taken to the base q.

The following notation, sorted in order of appearance, will be used. Some notation that is only used briefly (for example in a single proof) has not been listed.

Chapter 1 : Preliminaries

- $\mathbb{F}_q$: the finite field with q elements, where q is a power of the odd prime p.
- $\mathcal{X}$: a smooth, geometrically irreducible projective algebraic curve over $\mathbb{F}_q$.
- $\mathcal{K} = \mathbb{F}_q(\mathcal{X})$: the field of rational functions on $\mathcal{X}$.
- $\infty \in \mathcal{X}(\overline{\mathbb{F}}_q)$: a chosen closed point of $\mathcal{X}$, of degree d_∞.
- $\mathcal{A} = \Gamma(\mathcal{X} \smallsetminus \infty, \mathcal{O}_\mathcal{X})$: the ring of functions regular away from ∞.
- v_∞ : the valuation of $\mathcal{K}$ associated to ∞.
- $\deg(\cdot) = -d_\infty v_\infty(\cdot)$
- $|\cdot|_\infty = q^{\deg(\cdot)}$: the normalized absolute value associated to ∞.
- $\mathcal{K}_\infty$: the completion of $\mathcal{K}$ at ∞.
- $\mathbf{C}_\infty = \hat{\bar{\mathcal{K}}}_\infty$: the completion of the algebraic closure of $\mathcal{K}_\infty$.

- $\mathrm{Pic}(\mathcal{A})$: the class group of $\mathcal{A}$.
- $\mathbb{G}_{a,L}$: the additive group scheme over a field L.
- $\rho : \mathcal{A} \to L$: the structure morphism of the $\mathcal{A}$-field L.

§1.1 : Drinfeld modules

- $L\{\tau\}$: the ring of twisted polynomials in τ with coefficients in L.
- $\mathrm{Drin}^r_{\mathcal{A}}(L)$: the category of rank r Drinfeld $\mathcal{A}$-modules over L.
- $\hat{f}$: the dual of the isogeny f of Drinfeld modules.
- $\phi[\mathfrak{a}]$: the $\mathfrak{a}$-division points of the Drinfeld module ϕ, where $\mathfrak{a}$ is an ideal in $\mathcal{A}$.
- ϕ/C : the quotient of the Drinfeld module ϕ by the finite A-module C.
- $M^r_{\mathcal{A}}(L)$: the set of isomorphism classes (moduli space) of rank r Drinfeld $\mathcal{A}$-modules over L. Also denoted by $M^r(L)$ when $\mathcal{A} = A = \mathbb{F}_q[T]$.
- $e_\Lambda(z)$: the exponential function associated to the lattice Λ.
- ϕ^Λ : the Drinfeld module associated to the lattice Λ.
- $k = \mathbb{F}_q(T) = \mathbb{F}_q(\mathbb{P}^1)$: the field of rational functions over $\mathbb{F}_q$ in the variable T.
- $A = \mathbb{F}_q[T]$: the ring of polynomials in T over $\mathbb{F}_q$.
- $|\cdot|$: the absolute value associated to the place $\infty = (1/T)$ of k.
- $k_\infty = \mathbb{F}_q((1/T))$: the completion of k at the place $\infty = (1/T)$.
- $\mathbf{C} = \hat{\bar{k}}_\infty$: the completion of the algebraic closure of k_∞.
- $j(\phi)$: the j-invariant of the rank 2 Drinfeld A-module ϕ.

§1.2 : Complex multiplication

- K will usually denote an imaginary quadratic function field.
- $\mathcal{O}_K$: the integral closure of $A = \mathbb{F}_q[T]$ in K.
- $\mathcal{O} = A + f\mathcal{O}_K$: an order of conductor f in K.
- $I_f(\mathcal{O})$: the monoid of $\mathcal{O}$-ideals relatively prime to $f \in A$.
- $P_f(\mathcal{O})$: the monoid of principal ideals in $I_f(\mathcal{O})$.
- $\mathrm{Pic}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$: the class group of $\mathcal{O}$.
- $P_{A,f}$: the monoid of principal ideals $\langle\alpha\rangle$ with $\alpha \equiv a \bmod f$, where $a \in A$ and $(a, f) = 1$.

- $\mathbb{P}_K$: the set of places of a (not necessarily quadratic) field K.
- $\mathcal{O}_P$: the valuation ring in K associated to the place $P \in \mathbb{P}_K$.
- $U_P = \mathcal{O}_P^*$: the unit group of $\mathcal{O}_P$.
- $U_P^n = 1 + \mathfrak{p}^n$: the nth unit group of $\mathcal{O}_P$, where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_P$.
- K_P : the completion of K at the place $P \in \mathbb{P}_K$.
- $\tilde{K}_P$: the residue field of K at the place $P \in \mathbb{P}_K$.
- $|P| = \#\tilde{K}_P$: the norm of the place $P \in \mathbb{P}_K$.
- J_K : the group of idèles of K.
- $C_K = J_K/K^*$: the idèle class group of K.
- $N_{L/K}$: the norm map for the extension L/K. It can act on the field L, the idèle group J_L or on the idèle class group C_L.
- J_K^S : the subgroup of idèles (a_P) satisfying $a_P = 1$ for $P \in S$, where $S \subset \mathbb{P}_K$ is a finite set of places.
- $D_{Q|P}(L/K) \subset \mathrm{Gal}(L/K)$: the decomposition group associated to the place Q over P.
- $\sigma_Q \in D_{Q|P}(L/K)$: the Frobenius element.
- $(\star, L/K)$: the Artin map. It may map J_K, J_K^S, C_K, $I(\mathcal{O}_K)$, $\mathrm{Pic}(\mathcal{O}_K)$ or $\mathrm{Pic}(\mathcal{O})$ to $\mathrm{Gal}(L/K)$, where L/K is an abelian extension.
- $K_{\mathcal{O}} = K[f]$: the ring class field of the order $\mathcal{O}$ of conductor f in K.

§1.3 : Drinfeld modular curves

- $\Omega = \mathbb{P}^1(\mathbf{C}) \smallsetminus \mathbb{P}^1(k_\infty)$: the Drinfeld upper half-plane.
- $Z(R) \cong R^*$: the subgroup of scalar matrices in $\mathrm{GL}_2(R)$, where R is any ring.
- $\mathrm{Stab}_G(z)$: the stabilizer of an element z under the action of the group G.
- $\Lambda_z = \langle z, 1\rangle$: the lattice associated to $z \in \Omega$.
- $\phi^z = \phi^{\Lambda_z}$: the Drinfeld module associated to the lattice Λ_z.
- $Y(1) = \mathrm{PGL}_2(A)\backslash\Omega \cong \mathbb{A}^1$: the simplest Drinfeld modular curve.
- $Y_\Gamma = \Gamma\backslash\Omega$: the (affine) Drinfeld modular curve associated to the congruence subgroup $\Gamma \subset \mathrm{PGL}_2(A)$.
- $\Gamma(N), \Gamma_0(N)$ and $\Gamma_2(N)$: certain congruence subgroups of $\mathrm{PGL}_2(A)$, see §§1.3.2 and 1.3.3.

- $Y(N), Y_0(N)$ and $Y_2(N)$: the Drinfeld modular curves associated to $\Gamma(N), \Gamma_0(N)$ and $\Gamma_2(N)$, respectively.
- $G(N) = \{\alpha \in \mathrm{GL}_2(A/NA) \mid \det(\alpha) \in \mathbb{F}_q^*\}$.
- $Y_0'(N) \subset \mathbb{A}^2$ and $Y_\Gamma' \subset \mathbb{A}^n$: affine models of $Y_0(N)$ and Y_Γ.
- $\Phi_N(t_1, t_2) \in A[t_1, t_2]$: the modular polynomial defining $Y_0'(N)$.
- $C[N]$: the A-submodule of N-division elements of the cyclic A-module C, for $N \in A$.
- $p_i : \mathbb{A}^n \to \mathbb{A}^1$: projection onto the ith coordinate.
- $p_{i,j} : \mathbb{A}^n \to \mathbb{A}^2$: projection onto the ith and jth coordinates.
- $\beta_d : Y_0(NM) \to Y_0(N)$: the dth degeneracy map, where $d|M$.
- $T_{\mathbb{A}^1,M}$: the Mth Hecke operator on $\mathbb{A}^1$.
- S_n : the group of permutations on n letters. $\pi \in S_n$ also defines an automorphism of $\mathbb{A}^n$, called a permutation of coordinates (which acts as the name suggests).
- $p_I : \mathbb{A}^n \to \mathbb{A}^I$: the projection onto the coordinates in $I \subset \{1, \ldots, n\}$.

Chapter 2 : Hecke Operators

§2.1 : Basic definitions

- $\mathfrak{m} \in A$ is monic and square-free.
- $T_\mathfrak{m} = T_{\mathbb{A}^n,\mathfrak{m}}$: the $\mathfrak{m}$th Hecke operator on $\mathbb{A}^n$.
- $T_{X,\mathfrak{m}}$: the Hecke operator $T_\mathfrak{m}$ restricted to X, when $T_\mathfrak{m}$ stabilizes X.
- $\psi(\mathfrak{m}) = |\mathfrak{m}| \prod_{\mathfrak{p}|\mathfrak{m}} (1 + |\mathfrak{p}|^{-1})$: the degree of the modular polynomial $\Phi_\mathfrak{m}(t_1, t_2)$ in the variables t_1 and t_2.
- $T_{X,\mathfrak{m}}^\infty(S)$: the Hecke orbit of a set $S \subset X$.
- $\deg(X)$: the degree of the variety X.

§2.4 : Curves stabilized by Hecke operators

- $Y \subset \mathbb{A}^2$: a geometrically irreducible algebraic curve (which we want to prove modular).
- $G = \mathrm{PGL}_2(k_\infty)^2$: which acts on Ω^2.
- $S = \mathrm{PSL}_2(k_\infty)^2$, $\Gamma = \mathrm{PGL}_2(A)^2$, $\Sigma = \mathrm{PSL}_2(A)^2$.
- $\pi = (j \times j) : \Omega^2 \to \mathbb{A}^2$: the quotient by the action of Γ.

- X : an irreducible component of the rigid analytic variety $\pi^{-1}(Y) \subset \Omega^2$.
- $H \cdot Z$: the H-orbit of a set Z, where H is a group.
- $G_X = \mathrm{Stab}_G(X)$: the stabilizer of X under the action of G on Ω^2.
- $S_X = G_X \cap S$, $\Gamma_X = G_X \cap \Gamma$, $\Sigma_X = G_X \cap \Sigma$.
- p_i : projection onto the ith factor of a space, e.g. $p_1 : \Omega^2 \to \Omega$.
- pr_i : projection onto the ith factor if a group, e.g. $pr_1 : G \to \mathrm{PGL}_2(k_\infty)$.
- $\Delta_{\mathfrak{m}}$: the set of 2×2 matrices over A with determinant in $\mathbb{F}_q^* \mathfrak{m}$.
- $\Delta_{\mathfrak{m}}^*$: those matrices of $\Delta_{\mathfrak{m}}$ for which the four entries are relatively prime.
- $t_i \in \Delta_{\mathfrak{m}}^*$: right coset representatives of $\Delta_{\mathfrak{m}}^* / \mathrm{GL}_2(A)$.
- $t_{ij} = (t_i, t_j)$.
- $H_1 = pr_1(G_X)$, $H_2 = pr_2(G_X)$.

Chapter 3 : Heights of CM Points

§3.1 : Class numbers

- $\deg(P) = [\tilde{F}_P : \mathbb{F}_q]$: the degree of the place $P \in \mathbb{P}_F$.
- $\mathrm{Div}(F)$: the divisor group of F.
- A_n : the number of effective divisors of degree n.
- $Z(t)$: the Zeta function of the function field F (it is a rational function).
- $L(t)$: the numerator of $Z(t)$.
- $\chi(\mathfrak{p})$: the Kronecker symbol. It is 1 if $\mathfrak{p}$ splits, -1 if $\mathfrak{p}$ is inert and 0 if $\mathfrak{p}$ is ramified in the quadratic extension K/k.

§3.2 : Estimating the j-invariant

- $\bar{\pi} \in \mathbf{C}$: a transcendental constant which plays the role of $\pi = 3.14159\ldots \in \mathbb{C}$.
- $e_A(z)$: the Carlitz exponential - the exponental function associated to the lattice A in $\mathbf{C}$.
- $t(z) = (\bar{\pi} e_A(z))^{-1}$: the uniformizer for Drinfeld modular functions.
- $|z|_A = \inf_{a \in A} |z - a|$
- $|z|_i = \inf_{x \in k_\infty} |z - x|$: the imaginary modulus.
- $\zeta \in \mathbf{C}$: generic error term satisfying $|\zeta| < 1$.
- $\mathcal{D}$: the quadratic fundamental domain, and $\mathcal{D}_K = \mathcal{D} \cap K$.

§3.3 : CM heights

- $H_{CM}(x) = H_{CM}(\phi)$: the CM height of the CM Drinfeld module ϕ with j-invariant $x \in \mathbf{C}$.
- $h(x)$: the (logarithmic) arithmetic height of a point $x \in \mathbb{P}^n(\bar{k})$.

Chapter 1

Preliminaries

The aim of this chapter is to fix notation and give an outline of a number of more or less well-known results on Drinfeld modules and Drinfeld modular curves.

Drinfeld modules were introduced by Vladimir Drinfeld [18] in 1974 (he called them "elliptic modules" due to their similarity with elliptic curves), for use in his proof of the two-dimensional Langlands correspondence for function fields.

Let $\mathcal{X}$ be a smooth, geometrically irreducible projective algebraic curve over $\mathbb{F}_q$. We choose a closed point $\infty \in \mathcal{X}(\overline{\mathbb{F}}_q)$ of degree d_∞ over $\mathbb{F}_q$. Let $\mathcal{A} = \Gamma(\mathcal{X} \smallsetminus \infty, \mathcal{O}_\mathcal{X})$ be the ring of functions on $\mathcal{X}$ regular away from ∞, and $\mathcal{K} = \mathbb{F}_q(\mathcal{X}) = \mathrm{Frac}(\mathcal{A})$ its field of fractions. Then $\mathcal{K}$ is an algebraic function field over $\mathbb{F}_q$, and $\mathcal{A}$ is a Dedekind domain with finite class number $\#\mathrm{Pic}(\mathcal{A}) = d_\infty h_\mathcal{K}$, where $h_\mathcal{K}$ is the class number of $\mathcal{K}$.

The point ∞ defines a valuation v_∞ on $\mathcal{K}$, and we denote by $\mathcal{K}_\infty$ the completion of $\mathcal{K}$ with respect to v_∞, and by $\mathbf{C}_\infty = \widehat{\overline{\mathcal{K}}}_\infty$ the completion of the algebraic closure of $\mathcal{K}_\infty$, which is again algebraically closed. For every $x \in \mathcal{K}$ we set $\deg(x) = -d_\infty v_\infty(x)$. Then v_∞ defines an absolute value on $\mathcal{K}$ by $|x|_\infty = q^{\deg(x)}$ which extends to $\mathcal{K}_\infty$ and $\mathbf{C}_\infty$. For $a \in \mathcal{A}$ we have $|a|_\infty = q^{\deg(a)} = \#(A/aA)$.

We notice that we have some strong analogies with number fields. Here $\mathcal{A}, \mathcal{K}, \mathcal{K}_\infty$ and $\mathbf{C}_\infty$ play the roles of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, respectively. The place ∞ plays the role of the Archimedean place of $\mathbb{Q}$ (but ∞ is non-Archimedean).

The principal aim of this thesis is to translate the results mentioned in the Introduction into characteristic p. The underlying philosophy of this translation is

Replace $\mathbb{Z}$ by $\mathcal{A}$ almost everywhere.

For example, abelian groups, which are $\mathbb{Z}$-modules, will be replaced by $\mathcal{A}$-modules. Thus elliptic curves, which can be viewed as $\mathbb{Z}$-module structures on a torus will be replaced by Drinfeld modules, which are essentially $\mathcal{A}$-module structures on the additive group $\mathbb{G}_a$.

At first sight $\mathbb{G}_a$ might not look like the right substitute for a torus, but in fact $\mathbb{G}_a$ has a richer structure in characteristic p than in characteristic 0. Specifically, $\mathbb{G}_a$ has infinitely many new $\mathbb{F}_q$-linear endomorphisms, generated by the qth-power Frobenius map, $\tau_q : x \mapsto x^q$.

Before we give the full definition of a Drinfeld module in §1.1 below, there is another use of $\mathbb{Z}$ in the classical theory which we will translate, namely the very notion of "characteristic" itself. Classically, any field L is equipped with a canonical map $\rho : \mathbb{Z} \to L$, and the characteristic of L is defined as (the generator of) the kernel, which is a prime ideal of $\mathbb{Z}$, hence either (0) or $p\mathbb{Z}$ for some prime number p. If we replace $\mathbb{Z}$ by $\mathcal{A}$ in this setting we get the notion of an *$\mathcal{A}$-field*.

Definition 1.0.1 *An* $\mathcal{A}$-field *is a pair* (ρ, L)*, where* L *is a field and* $\rho : \mathcal{A} \to L$ *a non-zero ring homomorphism. The* $\mathcal{A}$-characteristic *of* (ρ, L) *is defined to be the prime ideal* $P = \ker \rho$*. If* $P = (0)$*, i.e. if* ρ *is an embedding of* $\mathcal{A}$ *in* L*, then we also say* (ρ, L) *has* generic characteristic*. Otherwise* (ρ, L) *has* finite characteristic*.*

We will write L instead of (ρ, L) when ρ is understood. Note that, firstly, not every field is equipped with a non-zero morphism $\rho : \mathcal{A} \to L$ - it must at least have characteristic p in the classical sense. Secondly, the $\mathcal{A}$-characteristic of a given field L depends on ρ. For example $\mathcal{K}$ has generic characteristic when equipped with $\rho_1 : \mathcal{A} \hookrightarrow \mathcal{K}$, the usual inclusion, but finite characteristic when equipped with $\rho_2 : \mathcal{A} \to \mathbb{F}_q \subset \mathcal{K}$.

1.1 Drinfeld Modules

Our standard references for the results in this section are [31, Chapter 4] and [34].

1.1.1 The objects

Let L be an $\mathcal{A}$-field. Consider the non-commutative ring $L\{\tau\}$ of polynomials in the variable τ, with coefficients in L and subject to the commutation relation

$$\tau a = a^q \tau, \ \forall a \in L. \tag{1.1}$$

$L\{\tau\}$ is called the ring of *twisted polynomials* in τ over L. It is isomorphic to the ring of polynomials of the form $f(X) = \sum_{i=0}^{d} a_i X^{q^i} \in L[X]$, where addition is defined as usual and multiplication is defined by composition of polynomials.

The ring $L\{\tau\}$ is a left principal ideal ring, see [31, Chapter 1].

Let $\mathbb{G}_{a,L}$ denote the additive group-scheme over L. The importance of $L\{\tau\}$ is the fact that the ring of $\mathbb{F}_q$-linear endomorphisms of $\mathbb{G}_{a,L}$ is given by

$$\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,L}) = L\{\tau\},$$

where $\tau : x \mapsto x^q$ denotes the qth-power Frobenius.

There is an obvious homomorphism from $\mathcal{A}$ to the ring $L\{\tau\}$, as L is an $\mathcal{A}$-field. A Drinfeld-module is another, non-trivial such homomorphism:

Definition 1.1.1 *A* Drinfeld $\mathcal{A}$-module *over* L *is a ring homomorphism*

$$\begin{array}{rcl} \phi : \mathcal{A} & \longrightarrow & End_{\mathbb{F}_q}(\mathbb{G}_{a,L}) = L\{\tau\} \\ a & \longmapsto & \phi_a \end{array}$$

Satisfying the two conditions

1. **(Non-triviality)** $\phi(\mathcal{A}) \not\subset L$, *and*
2. **(Normalization)** *The constant term of* ϕ_a *is* $\rho(a)$.

We will usually omit the $\mathcal{A}$ from the terminology when there is no risk of confusion. One can view Drinfeld modules purely in terms of non-commutative algebra. One can show the following.

Proposition 1.1.2 *Let* $\phi : \mathcal{A} \longrightarrow L\{\tau\}$ *be a Drinfeld module.*

1. ϕ *is a monomorphism.*
2. *There exists a positive integer* r*, called the* rank *of* ϕ*, such that*

$$\phi_a = \sum_{i=0}^{N} a_i \tau^i, \quad \text{where } a_0 = \rho(a),\ a_N \neq 0 \text{ and } N = r\deg(a) \text{ for all } a \in \mathcal{A}.$$

3. *Suppose* L *has finite characteristic. Then there exists a positive integer* h*, called the* height *of* ϕ*, such that* $a_i = 0$ *above unless* $h|i$.

The rank r of a Drinfeld module is its most important invariant. The case $r = 1$ corresponds to the cyclotomic theory in characteristic 0, whereas the case $r = 2$ corresponds to elliptic curves. The case $r > 2$ has some similarities with abelian varieties "of dimension $r/2$", but the analogue is not very satisfying. The "correct" analogues of abelian varieties are in fact T-modules (see [31, chapter 5]), which we will not deal with here.

1.1.2 The morphisms

Now that we have our objects, we need to define the morphisms.

Definition 1.1.3 *Let* ϕ, ϕ' *be Drinfeld modules over* L*. A* morphism $f \in Hom(\phi, \phi')$ *from* ϕ *to* ϕ' *is an element* $f \in L\{\tau\}$ *such that*

$$f\phi_a = \phi'_a f \quad \forall a \in \mathcal{A}.$$

If $f \neq 0$*, we call* f *an* isogeny.

A morphism $f \in \mathrm{Hom}(\phi, \phi')$ is usually written as $f : \phi \to \phi'$, but keep in mind that here f is not a map between sets. Now the set of Drinfeld $\mathcal{A}$-modules of rank r over L, together with the morphisms defined above, form a category, which we denote by $\mathrm{Drin}^r_{\mathcal{A}}(L)$. A morphism $f \in \mathrm{Hom}(\phi, \phi')$ is an isomorphism if and only if $f \in (L\{\tau\})^* = L^*$.

If there exists an isogeny between $f : \phi \to \phi'$, then ϕ and ϕ' have the same rank. Any morphism $f \in \mathrm{Hom}(\phi, \phi')$ is just a polynomial in τ (or in X^q), hence acts on $\mathbb{G}_{a,L}$. So we may define the kernel $\ker f$ to be the (geometric) kernel of this action. If $f \neq 0$, then this kernel is finite (consider f as an element of $L[X^q]$, then $\ker f$ is just the set of roots of f in the algebraic closure $\bar{L}$). It is also an $\mathcal{A}$-module: Let $x \in \ker f$ and $a \in \mathcal{A}$, then $f(a \cdot x) = f \circ \phi_a(x) = \phi'_a \circ f(x) = \phi'_a(0) = \rho(a)0 = 0$.

We will now exhibit a correspondence between isogenies and their kernels. We do this only for L of generic characteristic, as this is the only case we will need. The reader may consult [31, §4.7] for the general case.

Proposition 1.1.4 *Suppose that L has generic characteristic. Let ϕ be a Drinfeld module over L, and H a finite $\mathcal{A}$-submodule of $\bar{L}$. Then there exists a Drinfeld module ϕ' over L and an isogeny $f : \phi \to \phi'$ such that* $\ker f = H$.

The Drinfeld module ϕ' will also be written as $\phi' = \phi/H$, and called the quotient of ϕ by H. Next, we define the dual of an isogeny.

Proposition 1.1.5 *Let $f : \phi \to \phi'$ be an isogeny. Then there exists an isogeny $\hat{f} : \phi' \to \phi$ such that $\hat{f}f = \phi_a$ and $f\hat{f} = \phi'_a$ for some $a \in \mathcal{A}$.*

The isogeny $\hat{f}$ is called the *dual* of f, in perfect analogy with the elliptic curve case. It follows also that isogenies give rise to an equivalence relation between Drinfeld modules. So it makes sense to say that ϕ is isogenous to ϕ'.

Definition 1.1.6 *Let $N \in \mathcal{A}$ and $f : \phi \to \phi'$ an isogeny. Then f is* cyclic of degree N, *if*

$$\ker f \cong \mathcal{A}/N\mathcal{A} \qquad \text{as } \mathcal{A}\text{-modules.}$$

Note, however, that $N \in A$ is not a number, so this is not the degree of a map in the usual sense. But then again, f is not a map in the usual sense, either. We point out that if $\ker f \cong \mathcal{A}/N\mathcal{A}$ for some $N \in \mathcal{A}$, then

$$\ker \hat{f} \cong (\mathcal{A}/N\mathcal{A})^{r-1},$$

where r is the rank of ϕ. In particular, if $r = 2$ then the dual of a cyclic isogeny is again cyclic.

Let $\mathfrak{a}$ be an ideal in $\mathcal{A}$. Consider the ideal $I_{\phi,\mathfrak{a}} = \{\phi_a \mid a \in \mathfrak{a}\}$ in $L\{\tau\}$. As $L\{\tau\}$ is left principal we may write $I_{\phi,\mathfrak{a}} = L\{\tau\} \cdot \phi_{\mathfrak{a}}$ for a unique monic twisted polynomial $\phi_{\mathfrak{a}} \in L\{\tau\}$. We may define the set of $\mathfrak{a}$-torsion points of ϕ by

$$\begin{aligned} \phi[\mathfrak{a}] &= \{x \in \bar{L} \mid \phi_a(x) = 0 \ \forall a \in \mathfrak{a}\} \\ &= \ker \phi_{\mathfrak{a}} \end{aligned}$$

Proposition 1.1.7 *Let $\mathfrak{a} \subset \mathcal{A}$ be an ideal, with prime factorization $\mathfrak{a} = \prod \mathfrak{p}^{e_\mathfrak{p}}$. Then $\phi[\mathfrak{a}] \cong \prod \phi[\mathfrak{p}^{e_\mathfrak{p}}]$ as $\mathcal{A}$-modules and $\phi[\mathfrak{p}^{e_\mathfrak{p}}] \cong (\mathcal{A}/\mathfrak{p}^{e_\mathfrak{p}})^g$, where*

$$g = \begin{cases} r - h & \text{if } \mathfrak{p} \text{ is the characteristic of } L \\ r & \text{otherwise,} \end{cases}$$

and where r and h denote the rank and height of ϕ, respectively.

We next consider endomorphisms of Drinfeld modules. We have

$$\mathrm{End}(\phi) = \mathrm{Hom}(\phi, \phi) = \{f \in L\{\tau\} \mid f\phi_a = \phi_a f \ \ \forall a \in \mathcal{A}\}$$

so $\mathrm{End}(\phi)$ is just the centralizer of $\phi(\mathcal{A})$ in $L\{\tau\}$. It clearly contains $\phi(\mathcal{A}) \cong \mathcal{A}$, and for any $n \in \mathcal{A}$ we denote by $[n]$ the endomorphism ϕ_n. We can consider this to be our multiplication by n map, just like the case for elliptic curves. The structure of endomorphism rings is given by

Proposition 1.1.8 *Let ϕ be a Drinfeld $\mathcal{A}$-module of rank r over L. Then*

1. *End(ϕ) is a projective $\mathcal{A}$-module of rank $\leq r^2$.*
2. *If L has generic characteristic, then End(ϕ) is commutative and has rank $\leq r$.*
3. *End(ϕ) $\otimes_{\mathcal{A}} \mathcal{K}$ is a finite-dimensional division algebra over $\mathcal{K}$.*
4. *End(ϕ) $\otimes_{\mathcal{A}} \mathcal{K}_\infty$ is a finite-dimensional division algebra over $\mathcal{K}_\infty$.*

Definition 1.1.9 *If ϕ is a Drinfeld module of rank r and generic characteristic, then we say that ϕ has* complex multiplication (CM) *if End(ϕ) has rank r over $\mathcal{A}$.*

In §1.2 we will give more details on the theory of complex multiplication, which is nearly identical to the classical theory for elliptic curves.

If we set $r = 2$ in Propositions 1.1.7 and 1.1.8 then we see a marked similarity with elliptic curves.

1.1.3 The action of Pic($\mathcal{A}$)

Let $\mathfrak{a}$ be an ideal in $\mathcal{A}$, then as above we have $I_{\phi,\mathfrak{a}} = L\{\tau\} \cdot \phi_{\mathfrak{a}}$. Clearly, $I_{\phi,\mathfrak{a}}$ is carried to itself by multiplication on the right by any ϕ_x, $x \in \mathcal{A}$. Therefore, for every $x \in \mathcal{A}$ there is a uniquely defined $\phi'_x \in L\{\tau\}$ such that

$$\phi_{\mathfrak{a}}\phi_x = \phi'_x\phi_{\mathfrak{a}}.$$

This ϕ' is just the quotient $\phi/\ker\phi_{\mathfrak{a}}$, hence is again a Drinfeld module, and we denote it by $\phi' = \mathfrak{a} * \phi$. It can be characterized as the unique Drinfeld module ϕ' which is isogenous to ϕ via the isogeny $\phi_{\mathfrak{a}}$. This action has the following properties (see [34, Lemmas 4.4 and 4.5]).

Proposition 1.1.10

1. *Let $\mathfrak{a} = w\mathcal{A}$ be a principal ideal, and let $\mu \in L^*$ be the leading coefficient of ϕ_w. Then $\phi_{\mathfrak{a}} = \mu^{-1}\phi_w$ and $(\mathfrak{a} * \phi)_x = \mu^{-1}\phi_x\mu$ for all $x \in \mathcal{A}$.*
2. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero ideals of $\mathcal{A}$. Then*

$$\phi_{\mathfrak{ab}} = (\mathfrak{b} * \phi)_{\mathfrak{a}}\phi_{\mathfrak{b}}$$

and

$$\mathfrak{a} * (\mathfrak{b} * \phi) = (\mathfrak{ab}) * \phi.$$

Let $M^r_{\mathcal{A}}(L)$ denote the set of isomorphism classes of rank r Drinfeld $\mathcal{A}$-modules over L. Then from Proposition 1.1.10 follows that the ideals of $\mathcal{A}$ act on $M^r_{\mathcal{A}}(L)$, and the principal ideals act trivially. So in particular, Pic($\mathcal{A}$) acts on $M^r_{\mathcal{A}}(L)$.

1.1.4 Analytic theory of Drinfeld modules

It is not obvious that Drinfeld modules, these remarkable embeddings of $\mathcal{A}$ into a large, non-commutative ring, even exist at all. In this section we will show how to produce any number of Drinfeld modules over $\mathbf{C}_\infty$, using analytic methods, much like the construction of complex elliptic curves as tori $\mathbb{C}/\Lambda$. For this we will use analysis in $\mathbf{C}_\infty$.

Definition 1.1.11 *A* lattice *of rank $r \geq 1$ is a discrete $\mathcal{A}$-submodule Λ of $\mathbf{C}_\infty$ such that $\mathcal{K}_\infty\Lambda$ has dimension r over $\mathcal{K}_\infty$.*

Note that $\mathbf{C}_\infty$ has infinite dimension over $\mathcal{K}_\infty$, so in particular, $\mathbf{C}_\infty$ contains lattices of any rank $r \geq 1$. This is in marked contrast with $\mathbb{C}$, which only contains lattices (in the above sense) of rank 1 and 2. This is also the reason that there don't seem to be any decent characteristic 0 analogues of Drinfeld modules of rank $r > 2$.

We want to associate a Drinfeld module of rank r to each lattice Λ of rank r. The naïve approach would be to form the quotient $\mathbf{C}_\infty/\Lambda$, but this is just homeomorphic to $\mathbf{C}_\infty$ itself, so it appears that we have not gained anything. But this is not true. We shall see below that the quotient $\mathbf{C}_\infty/\Lambda$ is endowed with a non-trivial $\mathcal{A}$-module structure, and this will give us our Drinfeld module.

Definition 1.1.12 *The* exponential function *associated to the lattice Λ is given by*

$$e_\Lambda(z) = z \prod_{0 \neq \lambda \in \Lambda} \left(1 - \frac{z}{\lambda}\right).$$

This function simultaneously plays the role of exp (for $r = 1$) and the Weierstraß-$\wp$ function (for $r = 2$). It has the following properties.

Proposition 1.1.13 *e_Λ is an entire function, and satisfies the following properties.*

1. *$e_\Lambda : \mathbf{C}_\infty \to \mathbf{C}_\infty$ is surjective and $\mathbb{F}_q$-linear.*
2. *e_Λ is Λ-periodic, has simple zeros on Λ and has no other zeros.*
3. *Let $c \in \mathbf{C}_\infty^*$, then $c\Lambda$ is again a lattice and we have*

$$e_{c\Lambda}(z) = ce_\Lambda(c^{-1}z). \tag{1.2}$$

Let Λ be a rank r lattice in $\mathbf{C}$, and let $a \in \mathcal{A}$, then multiplication by a is a map from Λ to Λ, which gives rise to the following commutative diagram, with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbf{C}_\infty & \xrightarrow{e_\Lambda} & \mathbf{C}_\infty & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle \phi_a^\Lambda} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbf{C}_\infty & \xrightarrow{e_\Lambda} & \mathbf{C}_\infty & \longrightarrow & 0. \end{array}$$

This gives us a map

$$\begin{aligned} \phi^\Lambda : \mathcal{A} &\longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,\mathbf{C}_\infty}) \\ a &\longmapsto \phi_a^\Lambda. \end{aligned}$$

One can show that ϕ^Λ so constructed is a Drinfeld $\mathcal{A}$-module of rank r over $\mathbf{C}_\infty$. Now (1.2) translates to

$$c\phi_a^\Lambda = \phi_a^{c\Lambda} c,$$

so that the homotheties between lattices indeed correspond to morphisms of the corresponding Drinfeld modules. On the other hand, one can show that every rank r Drinfeld module over $\mathbf{C}_\infty$ arises from a rank r lattice in this way. So we have

Theorem 1.1 (Drinfeld) *The functor $\Lambda \mapsto \phi^\Lambda$ is an equivalence between the categories $\{$Lattices of rank r in $\mathbf{C}_\infty$, homotheties$\}$ and $Drin_{\mathcal{A}}^r(\mathbf{C}_\infty)$.*

1.1.5 Rational Drinfeld modules

From now on, and for the rest of this thesis, we will restrict ourselves to the following situation.

$\mathcal{X} = \mathbb{P}^1$ is the projective line over $\mathbb{F}_q$.
$\infty = (1:0)$ is the usual point at infinity, which has degree $d_\infty = 1$.
$\mathcal{A} = \mathbb{F}_q[T] = A$ is the ring of polynomials in the variable T over $\mathbb{F}_q$.
$\mathcal{K} = \mathbb{F}_q(T) = k$ is the field of rational functions over $\mathbb{F}_q$.
$v_\infty(x) = \deg(x)$ is the usual degree map, normalized by $\deg(T) = 1$.
$|\cdot|_\infty = |\cdot|$ is the usual absolute value, given by $|x| = q^{\deg(x)}$.
$\mathcal{K}_\infty = \mathbb{F}_q((1/T)) = k_\infty$ is the field of formal Laurent series in $1/T$.
$\mathbf{C}_\infty = \hat{\bar{k}}_\infty = \mathbf{C}$ is the completion of the algebraic closure of k_∞. We equip it with the canonical inclusion $\rho : A \hookrightarrow \mathbf{C}$ to give it the structure of an A-field of generic characteristic.

Drinfeld A-modules with coefficients in a subfield L of $\mathbf{C}$ are called *rational*[1] Drinfeld modules.

Then any rational Drinfeld module of rank r is uniquely determined by ϕ_T, as T generates A over $\mathbb{F}_q$. Let

$$\phi_T = \sum_{i=0}^{r} a_i \tau^i, \quad \text{where } a_0 = T \text{ and } a_r \neq 0. \tag{1.3}$$

Clearly, for any $a_0, \ldots, a_r \in L$ with $a_0 = T$ and $a_r \neq 0$ the relation (1.3) defines a Drinfeld module over L of rank r. On the other hand, let ϕ and ϕ' be two Drinfeld modules over L of rank r. Then $f \in \mathrm{Hom}(\phi, \phi')$ is an isomorphism if and only if $f\phi_T = \phi'_T f$. From the commutation relation (1.1) follows that this is equivalent to $a_i = f^{q^i - 1} a'_i$ for all $i = 0, \ldots, r$ in the notation of (1.3). In particular, this shows

[1] Here "rational" refers to the underlying polynomial ring $A = \mathbb{F}_q[T]$. It does not mean that the coefficients need to lie in k.

Proposition 1.1.14 *Let M^r denote the moduli space of rational Drinfeld modules of rank r. Then M^r has dimension $r-1$.*

One may show that M^r is in fact an affine algebraic variety. For more details of these moduli spaces, in a far more general setting, see for example [60]. For the purposes of this thesis we are only interested in $M^2(\mathbf{C})$, which is one-dimensional.

Let ϕ be a Drinfeld A-module of rank 2 over a field L. Then ϕ is uniquely determined by

$$\phi_T = T\tau^0 + g\tau + \Delta\tau^2, \qquad \text{where } \Delta \neq 0, \tag{1.4}$$

and two such Drinfeld modules are isomorphic (over L) if and only if there exists some $f \in L^*$ such that $g = f^{q-1}g'$ and $\Delta = f^{q^2-1}\Delta$. This suggests the following definition.

Definition 1.1.15 *Let ϕ be a rank 2 Drinfeld module over L defined by (1.4). Then the j-*invariant *of ϕ is defined by*

$$j(\phi) = \frac{g^{q+1}}{\Delta}.$$

We see that if $\phi \cong \phi'$ then $j(\phi) = j(\phi')$. Conversely, if $j(\phi) = j(\phi')$ then ϕ and ϕ' are isomorphic over $\bar{L}$. On the other hand, given any $j \in L$, then $\Delta = 1$ and $g = j^{1/(q+1)}$, for any choice of $(q+1)$st root, define a Drinfeld module ϕ via (1.4) with $j(\phi) = j$. So we have shown that $j : M^2(\bar{L}) \to \mathbb{A}^1(\bar{L})$ is a bijection, exactly as is the case for elliptic curves.

1.2 Complex multiplication

1.2.1 Imaginary quadratic function fields

In this subsection we will make a brief detour to define some basic notions concerning "imaginary" quadratic function fields. Our basic reference to general facts on function fields is [65].

We assume throughout that q is odd, to avoid complications.

We first classify quadratic extensions of k according to the behaviour of the place ∞.

Proposition 1.2.1 *Let q be odd and K a quadratic extension of k. Then K is a Kummer extension and can be written in the form $K = k(\sqrt{d})$, for a non-square element $d \in A$. Let $m = \deg(d)$. Then*

1. *∞ ramifies in K/k if and only if m is odd.*
2. *∞ is inert in K/k if and only if m is even and the leading coefficient of d is not a square in $\mathbb{F}_q$.*
3. *∞ is split in K/k if and only if m is even and the leading coefficient of d is a square in $\mathbb{F}_q$.*

Definition 1.2.2 *A quadratic extension K of k is called* imaginary *if ∞ is not split in K/k, in other words, ∞ extends to a unique place of K. Equivalently, K is imaginary if it has no embedding into k_∞, which explains the terminology.*

So K is quadratic imaginary in the cases 1 and 2 of Proposition 1.2.1.

Let $K = k(\sqrt{d})$, and d' be the square-free part of d. Then the integral closure of A in K is $\mathcal{O}_K = A[\sqrt{d'}]$, which we call the *ring of integers* of K. By an *order* in K we mean a subring of $\mathcal{O}_K$ of the form $\mathcal{O} = A[f\sqrt{d'}] = A + f\mathcal{O}_K$, for some $f \in A$. Note that, unlike the case for number fields, the ring $\mathcal{O}_K$ has many subrings of finite index which are not of the form $A + f\mathcal{O}_K$, for example $\mathcal{O} = \mathbb{F}_p + f\mathcal{O}_K$. However, we will see that the orders we have defined are the only subrings of K that appear as endomorphism rings of rank 2 Drinfeld modules over $\mathbf{C}$. The element f is called the *conductor* of the order $\mathcal{O} = A + f\mathcal{O}_K$. The index of $\mathcal{O}$ in $\mathcal{O}_K$ is given by $[\mathcal{O}_K : \mathcal{O}] = |f|$.

Let $\mathcal{O}$ be the order of conductor f in $\mathcal{O}_K$. As in the classical case, $\mathcal{O}$ is not integrally closed unless $f \in \mathbb{F}_q^*$, so in general $\mathcal{O}$ is not a Dedekind domain, and not all fractional $\mathcal{O}$-ideals are invertible. But as usual, the set of invertible fractional $\mathcal{O}$-ideals form a group $I(\mathcal{O})$, and the principal fractional $\mathcal{O}$-ideals form a subgroup $P(\mathcal{O})$. Then the quotient $I(\mathcal{O})/P(\mathcal{O}) = \mathrm{Pic}(\mathcal{O})$ is called the *class group* of $\mathcal{O}$, and is finite.

Let $I_f(\mathcal{O})$ be the monoid of $\mathcal{O}$-ideals prime to f, i.e. those ideals $\mathfrak{a} \subset \mathcal{O}$ for which $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$, and let $P_f(\mathcal{O})$ be the principal ideals in $I_f(\mathcal{O})$. We further define $I_f = I_f(\mathcal{O}_K)$ and let $P_{A,f} = \{x\mathcal{O}_K \mid x \equiv a \bmod f,\ a \in A,\ (a, f) = 1\}$. Then, as in the number field case (see e.g. [41, Chapter 8]), we have isomorphisms

$$\mathrm{Pic}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}) \cong I_f(\mathcal{O})/P_f(\mathcal{O}) \cong I_f/P_{A,f}.$$

1.2.2 Ring class fields

Almost all books on global class field theory treat only the number field case, with the occasional comment that the function field case is similar. In this subsection we define ring class fields for imaginary quadratic function fields. Our basic reference for global fields and idèles is [12], and for global class field theory we use [66], which also treats the function field case (but leaves some proofs to [4]).

Let K be a function field. We fix the following notation.

- $\mathbb{P}_K$ denotes the set of places of K.
- For $P \in \mathbb{P}_K$ we denote by v_P the valuation associated to P.
- $\mathcal{O}_P = \{x \in K \mid v_P(x) \geq 0\}$ is the valuation ring.
- $\mathfrak{p} = \{x \in K \mid v_P(x) > 0\}$ is the maximal ideal. We sometimes identify P with $\mathfrak{p}$.
- $U_P = U_P^0 = \mathcal{O}_P^* = \{x \in K \mid v_P(x) = 0\}$ is the unit group.
- $U_P^n = 1 + \mathfrak{p}^n = \{x \in K \mid v_P(x - 1) \geq n\} = \{x \in K \mid x \equiv 1 \bmod \mathfrak{p}^n\}$.

- $\tilde{K}_P = \mathcal{O}_P^*/\mathfrak{p}$ is the residue field.
- $|P| = \#\tilde{K}_P$ is the norm of P.
- K_P is the completion of K at the place P.

Then K_P^* is a topological group, with a neighborhood base around 1 given by $U_P^n,\ n \geq 1$. We denote by J_K the group of idèles of K, i.e. the restricted product of the K_P^*, $P \in \mathbb{P}_K$, with respect to the open subgroups U_P. We identify K^* with its image in J_K under the diagonal mapping $x \mapsto (x, x, x, \ldots)$. Thus we may define the *idèle class group* by

$$C_K = J_K/K^*.$$

For a finite extension L/K we denote by $N_{L/K}$ the norm map

$$\begin{array}{rcl} N_{L/K} : J_L & \longrightarrow & J_K \\ (a_Q)_{Q\in\mathbb{P}_L} & \longmapsto & \left(\prod_{Q|P} N_{L_Q/K_P}(a_Q)\right)_{P\in\mathbb{P}_K}. \end{array}$$

As $K^* \supset N_{L/K}(L^*)$ the norm induces a map on idèle class groups, again denoted by $N_{L/K} : C_L \to C_K$.

For a finite set of places $S \subset \mathbb{P}_K$ we let J_K^S be the subgroup of idèles (a_P) with $a_P = 1$ for all $P \in S$. Let L/K be a Galois extension, unrammified outside S. Now let $P \in \mathbb{P}_K \smallsetminus S$, let $Q \in \mathbb{P}_L$ be a place above P, and define the *decomposition group* $D_{Q|P}(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(Q) = Q\}$. Then, by reduction modulo Q, we get a surjection $D_{Q|P}(L/K) \to \mathrm{Gal}(\tilde{L}_Q/\tilde{K}_P)$, which is an isomorphism as $Q|P$ is unrammified. The group $\mathrm{Gal}(\tilde{L}_Q/\tilde{K}_P)$ is generated by a Frobenius element $\phi : x \mapsto x^{|P|}$. We let $\sigma_Q \in D_{Q|P}(L/K)$ be the preimage of ϕ, which we also call the *Frobenius for* Q. For any $\tau \in \mathrm{Gal}(L/K)$ we have $\tau\sigma_Q\tau^{-1} = \sigma_{\tau(Q)}$, and we denote by σ_P the conjugacy class of σ_Q in $\mathrm{Gal}(L/K)$, for any $Q|P$. When L/K is abelian, this conjugacy class contains only one element, which we also denote by $\sigma_P = \sigma_Q$ for all $Q|P$. Notice that a place P splits completely in L/K if and only if $\sigma_P = 1$.

Let L/K be abelian. Then we obtain the *Artin map*:

$$\begin{array}{rcl} (\star, L/K) : J_K^S & \longrightarrow & \mathrm{Gal}(L/K) \\ a = (a_P) & \longmapsto & (a, L/K) = \prod_{P\in\mathbb{P}_K\smallsetminus S} \sigma_P^{v_P(a_P)}. \end{array} \tag{1.5}$$

We now state the main theorems of global class field theory.

Theorem 1.2 (Reciprocity Theorem) *Let L/K be an abelian extension, and $S \subset \mathbb{P}_K$ a finite set of places, including the ramified places of L/K. Then there exists a unique surjective continuous homomorphism (also called the* Artin map*)*

$$(\star, L/K) : J_K \longrightarrow Gal(L/K)$$

which coincides with the map (1.5) on J_K^S. The kernel is given by

$$\ker(\star, L/K) = K^* N_{L/K}(J_L).$$

For an intermediate field $K \subset L' \subset L$ we have $(\star, L/K)|_{J_{L'}} = (\star, L'/K)$.

We give $\mathrm{Gal}(L/K)$ the discrete topology in the theorem above. As $K^* \subset \ker(\star, L/K)$ the Artin map induces a map on idèle class groups

$$(\star, L/K) : C_K \longrightarrow \mathrm{Gal}(L/K)$$

which is surjective with kernel $\ker(\star, L/K) = N_{L/K}(C_J)$, and hence we get an isomorphism

$$C_K/N_{L/K}(C_J) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

The group $N_{L/K}(C_J)$ is open and of finite index in C_K. Conversely, any such subgroup corresponds to a class field.

Theorem 1.3 (Existence Theorem) *Let $N \subset C_K$ be an open subgroup of finite index. Then there exists a finite abelian extension L of K such that N is the kernel of the Artin map*

$$N = \ker\Big((\star, L/K) : C_K \longrightarrow Gal(L/K)\Big).$$

We want to define the ring class field of an order $\mathcal{O}$ in the quadratic imaginary field K. In order to apply Theorem 1.3, we must first realise $\mathrm{Pic}(\mathcal{O})$ as a quotient of C_K. We recall that $\mathrm{Pic}(\mathcal{O}) \cong I_f/P_{A,f}$. This suggests the following definitions. Write

$$fK = \prod_{P \in \mathbb{P}_K} \mathfrak{p}^{n_P}.$$

Notice that every $n_P \geq 0$, as $f \in A\cdot$

Let $U_{A,f,P} = \{x \in U_P \mid x \equiv a \bmod P^{n_P},\ a \in A,\ P \nmid a\}$. This is an open subgroup of U_P, indeed we may write it as

$$U_{A,f,P} = \bigcup_{[a] \in A/(\mathfrak{p} \cap A)^{n_P}} a \cdot U_P^{n_P},$$

where the a's form a finite set of representatives of $A/(\mathfrak{p} \cap A)$. We also define

$$J_K(f) = J_K \cap \Big(\prod_{P \nmid f} K_P^* \times \prod_{P \mid f} U_{A,f,P}\Big),$$

$$W_K(f) = K_\infty^* \times \prod_{P \nmid f\infty} U_P \times \prod_{P \mid f} U_{A,f,P},$$

and

$$K_{A,f} = \{x \in K \mid x \equiv a \bmod f,\ a \in A,\ (a,f) = 1\} = \{x \in K \mid (x) \in P_{A,f}\},$$

which we view as a subgroup of $J_K(f)$.

Proposition 1.2.3 *With the above notation we have*

$$J_K/K^* W_K(f) \cong I_f/P_{A,f} \cong Pic(\mathcal{O}).$$

Proof. We have a surjective map

$$i : J_K(f) \longrightarrow I_f;\ (a_P) \longmapsto \prod_{P \nmid \infty} \mathfrak{p}^{v_P(a_P)}.$$

Notice that for $P|f$ we have $v_P(a_P) = 0$, so the map is well-defined.

The kernel is $\ker(i) = W_K(f)$, hence $J_K(f)/W_K(f) \cong I_f$ and thus

$$J_K(f)/K_{A,f}W_K(f) \cong I_f/P_{A,f} \cong \mathrm{Pic}(\mathcal{O}). \tag{1.6}$$

Next, the injection $J_K(f) \hookrightarrow J_K$ induces a map $J_K(f) \to J_K/K^*$ with kernel $K^* \cap J_K(f) = K_{A,f}$, so we have

$$J_K(f)/K_{A,f} \hookrightarrow J_K/K^*. \tag{1.7}$$

But it follows from the weak approximation theorem that (1.7) is surjective. Indeed, let $(a_P) \in J_K$, then there exists some $b \in K^*$ such that $a_P/b \in U_P^{n_P}$ for all $P|f$. Then $(a_P/b) \in J_K(f)$ is a preimage of (a_P) in J_K/K^*. Hence (1.7) is an isomorphism. Combining this with (1.6) give the desired result.

□

Now let $N_{\mathcal{O}} = K^*W_K(f)/K^*$. We have

$$C_K/N_{\mathcal{O}} = J_K/K^*W_K(f) \cong \mathrm{Pic}(\mathcal{O}),$$

which is finite. Furthermore, $N_{\mathcal{O}}$ is open in C_K, as each $U_{A,f,P}$ is open in K_P^*, and of finite index. So by Theorem 1.3 there exists a class field $L = K_{\mathcal{O}} = K[f]$, which we call the *Ring Class Field*, corresponding to $N_{\mathcal{O}}$, with the following properties.

Proposition 1.2.4 *The field $K_{\mathcal{O}}$ is Galois over k. The place ∞ splits completely in the extension $K_{\mathcal{O}}/K$, which is unramified outside f. We have*

$$Gal(K_{\mathcal{O}}/K) \cong Pic(\mathcal{O}).$$

Proof sketch. The factor K_∞^* in $W_K(f)$ insures that K_∞ lies in the kernel of the Artin map, so ∞ splits completely. On the other hand, $W_K(f)$ is contained in

$$V_K(f) = K_\infty \times \prod_{P \nmid f\infty} U_P \times \prod_{P|f} U_P^{n_P}$$

which defines, in exactly the same way as above, the *Ray Class Field* $H(f)$ with modulus f (see for example [46]), which is unramified outside f. Thus $K_{\mathcal{O}}$ is contained in $H(f)$, and is also unramified outside f. It remains to show that $K_{\mathcal{O}}$ is Galois over k. Let σ denote "complex conjugation", i.e. the extension of the non-trivial element of $\mathrm{Gal}(K/k)$ to K^{sep}, the separable closure of K. It acts trivially on $W_K(f)$, hence fixes $K_{\mathcal{O}}$. It follows that $\#\mathrm{Aut}(K_{\mathcal{O}}/k) = [K_{\mathcal{O}} : k]$ and hence $K_{\mathcal{O}}$ is Galois over k.

□

1.2.3 The Čebotarev Theorem for function fields

We briefly state the Čebotarev Theorem for function fields, which we will need later in the thesis.

Let F/K be a finite Galois extension of function fields over $\mathbb{F}_q$. Let $S \subset \mathbb{P}_K$ be a finite set of places including all the ramified ones. We identify the finite places with prime ideals of $\mathcal{O}_K$. We have a homomorphism

$$I(\mathcal{O}_K) \longrightarrow J_K; \quad \mathfrak{a} = \prod \mathfrak{p}^{n_P} \longmapsto (\pi_P^{n_P})$$

which maps ideals to idèles, where π_P is a chosen uniformizer for $\mathfrak{p}$ in $\mathcal{O}_P$. We let $I^S(\mathcal{O}_K)$ denote the ideals prime to the places of S, then we may compose the above map with the Artin map to obtain

$$(\star, L/K) : I^S(\mathcal{O}_K) \longrightarrow \mathrm{Gal}(L/K),$$

which we again call the Artin map. This also induces a map, once again called the Artin map,

$$(\star, L/K) : \mathrm{Pic}(\mathcal{O}) \longrightarrow \mathrm{Gal}(L/K),$$

as $\mathrm{Pic}(\mathcal{O}) \cong I^S(\mathcal{O}_K)/P_{A,f}$ where S is the set of places dividing f.

Now let T be a separating transcendental element of K, i.e. an element such that K is a finite separable extension of $\mathbb{F}_q(T)$, where $\mathbb{F}_q$ is the exact field of constants of K. Let L be the algebraic closure of $\mathbb{F}_q$ in F. Let g_K and g_F denote the genus of K and F, respectively. Define the following degrees:

$$\begin{array}{rcll} d & = & [K : \mathbb{F}_q(T)], & \\ n_g & = & [F : LK] & \text{the } \textit{geometric extension degree}, \\ n_c & = & [L : \mathbb{F}_q] & \text{the } \textit{constant extension degree}. \end{array}$$

Denote by $\phi : x \mapsto x^q$ the Frobenius of $\mathrm{Gal}(L/\mathbb{F}_q)$. Let $\mathcal{C}$ be a conjugacy class in $\mathrm{Gal}(F/K)$, and define

$$C_{F/K}(\mathcal{C}, t) = \{\mathfrak{p} \in \mathbb{P}_K \mid \text{unramified in } F/K,\ (\mathfrak{p}, L/K) = \mathcal{C},\ \deg \mathfrak{p} = t\}.$$

Then we have (see [23, Prop.5.16])

Theorem 1.4 (Čebotarev) *Let a be a positive integer such that $\tau|_L = \phi^a|_L$ for all $\tau \in \mathcal{C}$. If $t \not\equiv a \bmod n_c$, then $C_{F/K}(\mathcal{C}, t) = \emptyset$. If $t \equiv a \bmod n_c$ then*

$$\left| \#C_{F/K}(\mathcal{C}, t) - \frac{\#\mathcal{C}}{n_g} \cdot \frac{q^t}{t} \right| < 4\#\mathcal{C}(d^2 + g_F d/2 + g_F/2 + g_K + 1)q^{t/2}.$$

We will only need the following special case:
$K = k = \mathbb{F}_q(T)$, so $d = 1$ and $g_K = 0$.
$\mathcal{C} = \{1\}$ (so $a = 0$) and

$$\pi_F(t) = \#C_{F/K}(\mathcal{C}, t) = \#\{\mathfrak{p} \in \mathbb{P}_K \mid \text{split completely in } F/K\}.$$

Then we have

Theorem 1.5 (Čebotarev) *If $n_c \nmid t$ then $\pi_F(t) = 0$. If $n_c | t$ then*

$$\left| \pi_F(t) - \frac{1}{n_g} \cdot \frac{q^t}{t} \right| < 4(g_F + 2)q^{t/2}.$$

In particular, we see that the set of primes of K that split in F has density $1/n_g \geq 1/[F : K]$.

1.2.4 Complex multiplication

Let ϕ be a rank 2 Drinfeld A-module over $\mathbf{C}$. Then we say that ϕ has *complex multiplication* (CM) if $\mathrm{End}(\phi)$ has rank 2 over A (equivalently $\mathrm{End}(\phi)$ is strictly larger than A). Let Λ be the lattice associated to ϕ. Then we see, as in the case for elliptic curves, that

$$\mathrm{End}(\phi) \cong \mathrm{End}(\Lambda) = \{x \in \mathbf{C} \mid x\Lambda \subset \Lambda\}.$$

We may write $\Lambda \cong \Lambda_z = \langle z, 1\rangle$, for some $z \in \Omega = \mathbf{C} \smallsetminus k_\infty$. Then if $A \subsetneq \mathrm{End}(\Lambda)$, we see as in the classical case that z satisfies a quadratic equation $az^2 + bz + c = 0$, with $a, b, c \in A$. We denote by $\mathrm{Discr}(z) = d = b^2 - 4ac$ the *discriminant* of z. As Λ_z is a rank 2 lattice, we get $z \notin k_\infty$ and hence $\sqrt{d} \notin k_\infty$. It follows that $K = k(z) = k(\sqrt{d})$ is an imaginary quadratic field over k, called the *CM field* of ϕ. Moreover,

$$\mathcal{O} = \mathrm{End}(\Lambda) = A[\sqrt{d}]$$

is an order in K.

Conversely, let $\mathcal{O}$ be an order in the quadratic imaginary field K. Then any invertible ideal $\mathfrak{a} \subset \mathcal{O}$ is a rank 2 lattice in $\mathbf{C}$, and hence gives rise to a Drinfeld module $\phi^{\mathfrak{a}}$ with $\mathrm{End}(\phi^{\mathfrak{a}}) \cong \mathrm{End}(\mathfrak{a}) = \mathcal{O}$, as $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal. We denote by $j(\mathfrak{a})$ the j-invariant of the Drinfeld module $\phi^{\mathfrak{a}}$.

Let $\mathfrak{b} \in \mathcal{O}$ be another invertible ideal. Then the morphism of lattices

$$\mathfrak{a} \longrightarrow \mathfrak{b}^{-1}\mathfrak{a}$$

corresponds to an isogeny of Drinfeld modules

$$f : \phi^{\mathfrak{a}} \longrightarrow \phi^{\mathfrak{b}^{-1}\mathfrak{a}}$$

with kernel isomorphic to $\mathcal{O}/\mathfrak{b}$ as an A-module.

We now state the Main Theorem of Complex Multiplication for rational Drinfeld modules of rank 2 (this is the only case we need. For a more general treatement, see [33]). The version we state below is from [26].

Theorem 1.6 (Main Theorem of Complex Multiplication) *Let ϕ be a Drinfeld A-module of rank 2 over $\mathbf{C}$ with complex multiplication. Let $\mathcal{O} = End(\phi)$, which is an order of conductor f in the imaginary quadratic field $K = \mathcal{O} \otimes_A k$. Then $j = j(\phi)$ is integral over A and $K(j)$ is the ring class field of K with respect to $\mathcal{O}$. In particular, $K(j)/K$ is unramified outside f, ∞ splits completely in $K(j)/K$ and the Artin map gives an isomorphism*

$$Pic(\mathcal{O}) \cong Gal(K(j)/K).$$

If $\mathfrak{a}$ and $\mathfrak{b}$ are invertible ideals in $\mathcal{O}$ and $\sigma_{\mathfrak{b}} = (\mathfrak{b}, K(j)/K) \in Gal(K(j)/K)$, then

$$\sigma_{\mathfrak{b}} j(\mathfrak{a}) = j(\mathfrak{b}^{-1}\mathfrak{a}).$$

In particular, suppose $\mathfrak{p}$ is a prime of k, which splits completely in K, $\mathfrak{p}K = \mathfrak{p}_1\mathfrak{p}_2$, and does not divide the conductor f of $\mathcal{O}$. Then there is an isogeny $\phi \to \sigma_{\mathfrak{p}_1}(\phi)$ with kernel isomorphic to $\mathcal{O}/\mathfrak{p}_1 \cong A/\mathfrak{p}$, in other words cyclic of degree $\mathfrak{p}$. This is the most important property of CM Drinfeld modules, which we exploit in our proof of the André-Oort Conjecture for products of Drinfeld modular curves.

Another approach to Drinfeld modules with complex multiplication is to view ϕ as a rank 1 Drinfeld $\mathcal{O}$-module. This is a natural view, as ϕ is an embedding of A into $\mathbf{C}\{\tau\}$, and $\mathcal{O} \cong \mathrm{End}(\phi)$ is the centralizer of $\phi(A)$ in $\mathbf{C}\{\tau\}$, and is furthermore commutative. So we actually have an embedding of $\mathcal{O}$ into $\mathbf{C}\{\tau\}$. The difference is that $\mathcal{O}$ is not a Dedekind domain, so one has to develop the whole theory of Drinfeld modules (at least for rank 1) in this more general case. This was done by Hayes [33], where he uses this to explicitely construct essentially *all* class fields for global function fields. So he has solved Kronecker's Jugendtraum in the function field case. We remark that in this situation the ideals of $\mathcal{O}$ act on ϕ as described in §1.1.3. Then Theorem 1.6 says that this action coincides with the $\mathrm{Pic}(\mathcal{O})$-action given by $\mathrm{Gal}(K(j)/K)$ via the Artin map.

1.3 Drinfeld modular curves

1.3.1 The Drinfeld upper half-plane

Definition 1.3.1 *The* Drinfeld upper half-plane *is the space*

$$\Omega = \mathbb{P}^1(\mathbf{C}) \smallsetminus \mathbb{P}^1(k_\infty).$$

The group $G = PGL_2(k_\infty)$ acts on it by fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

Ω is in fact a rigid analytic space. For an introduction to rigid analytic geometry we refer the reader to [64] and [67], and to [7] for a full treatment.

Ω plays the role of the double Poincaré half-plane $\mathfrak{H}^{\pm}$, rather than $\mathfrak{H}$, as one cannot translate the notion of "positive imaginary part" into characteristic p.

Unlike the case for $\mathfrak{H}$ (or $\mathfrak{H}^{\pm}$), the action of $\mathrm{PGL}_2(k_\infty)$ on Ω is not transitive, as $\mathbf{C}$ is infinite dimensional over k_∞. Basically, the $\mathrm{PGL}_2(k_\infty)$-orbits are much smaller than Ω. This also means that the stabilizers of different points can behave differently. If $z \in \Omega$ is fixed by some $1 \neq \gamma_0 \in \mathrm{PGL}_2(k_\infty)$, then z satisfies a quadratic equation

$$c_0 z^2 + (d_0 - a_0)z - b_0 = 0$$

over k_∞, and we say that z is a *quadratic point*. In this case we have

$$\begin{aligned} \mathrm{Stab}_G(z) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid cz^2 + (d-a)z - b = 0,\ ad - bc \neq 0 \right\} \big/ Z(k_\infty) \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{array}{l} c = \lambda c_0, (d-a) = \lambda(d_0 - a_0), \\ b = \lambda b_0,\ ad - bc \neq 0 \end{array} \right\} \big/ Z(k_\infty), \end{aligned}$$

where $Z(k_\infty) \cong k_\infty^*$ denotes the group of scalar matrices.

We see that $\mathrm{Stab}_G(z)$ is a closed one-dimensional Lie sub-group of G.

On the other hand, if $z \in \Omega$ does not satisfy a quadratic equation over k_∞ then we say it is *non-quadratic* and we have $\mathrm{Stab}_G(z) = \{1\}$.

1.3.2 Quotients by group actions

It follows from Theorem 1.1 that classifying isomorphism classes of Drinfeld modules over $\mathbf{C}$ is equivalent to classifying homothety classes of lattices in $\mathbf{C}$. As in the classical case, any lattice Λ in $\mathbf{C}$ is homothetic to a lattice $\Lambda_z = \langle z, 1\rangle$ for some $z \in \Omega$, and

$$\Lambda_{z_1} \cong \Lambda_{z_2} \Longleftrightarrow z_2 = \gamma(z_1) \text{ for some } \gamma \in \Gamma = \mathrm{PGL}_2(A).$$

Now to a point $z \in \Omega$ we may associate the Drinfeld module $\phi^z = \phi^{\Lambda_z}$ corresponding to the lattice Λ_z, and its j-invariant $j(z) = j(\phi^z)$. From the above discussion follows that we have bijections

$$\begin{array}{rcl} \mathrm{PGL}_2(A)\backslash\Omega & \longleftrightarrow & \{\text{homothety classes of lattices}\} \\ & \longleftrightarrow & \{\text{isomorphism classes of Drinfeld modules}\} \\ & \overset{j}{\longleftrightarrow} & \mathbb{A}^1(\mathbf{C}) \end{array}$$

We can say more. The quotient $Y(1) = \mathrm{PGL}_2(A)\backslash\Omega$ is a rigid analytic variety, and we have a rigid analytic isomorphism

$$j : Y(1) = \mathrm{PGL}_2(A)\backslash\Omega \xrightarrow{\sim} \mathbb{A}^1(\mathbf{C}).$$

We generalize this construction to quotients by the action of *congruence* subgroups, to obtain Drinfeld modular curves. Our standard references for this section are [67, 68] and [27, 28, 29].

Let $N \in A$ with $\deg(N) \geq 1$ and define

$$\begin{array}{rcll} \Gamma(N) & = & \{\gamma \in \mathrm{GL}_2(A) \mid \gamma \equiv 1 \bmod N\}/Z(\mathbb{F}_q^*) \subset \mathrm{PGL}_2(A) & (1.8) \\ & = & \{\gamma \in \mathrm{GL}_2(A) \mid (\gamma \bmod N) \in Z(\mathbb{F}_q^*)\}/Z(\mathbb{F}_q^*) \subset \mathrm{PGL}_2(A), & (1.9) \\ \Gamma_0(N) & = & \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A) \mid c \equiv 0 \bmod N \right\} /Z(\mathbb{F}_q^*) \subset \mathrm{PGL}_2(A). & \end{array}$$

We first verify that the two groups (1.8) and (1.9) really are equal. Clearly (1.8) is contained in (1.9). On the other hand, let $\gamma \in \mathrm{GL}_2(A)$ be such that $\tilde{\gamma} \in Z(\mathbb{F}_q^*)$, where we denote reduction mod N by $\tilde{\ }$. Let $\gamma' = \gamma\tilde{\gamma}^{-1} \in \mathrm{GL}_2(A)$ (which we may, as $\mathbb{F}_q^* = A^* \subset A$). Then clearly γ and γ' respresent the same element in (1.9), and $\tilde{\gamma}' = 1$, which shows that (1.8) and (1.9) are the same group.

Definition 1.3.2 *A subgroup $\Gamma \subset PGL_2(A)$ is called a* congruence subgroup *if Γ contains $\Gamma(N)$ for some $N \in A$.*

Let $\Gamma \subset \mathrm{PGL}_2(A)$ be a congruence subgroup. Then we may form the quotient

$$Y_\Gamma = \Gamma \backslash \Omega$$

as above. This is again a rigid analytic space, and one can show that Y_Γ also has the structure of an irreducible affine algebraic curve over $\mathbf{C}$, called a *Drinfeld modular curve*. For two special Drinfeld modular curves, we use the following notation:

$$\begin{aligned} Y(N) &= \Gamma(N) \backslash \Omega \quad \text{and} \\ Y_0(N) &= \Gamma_0(N) \backslash \Omega. \end{aligned}$$

From now on we treat the Y_Γ's as affine algebraic curves. They are in fact coarse moduli schemes parametrising Drinfeld modules with some appropriate level structure.

The curve $Y_0(N)$ is the coarse moduli space parametrising isomorphism classes of pairs (ϕ, C), where $C \cong A/NA$ is an A-submodule of $\phi[N]$, as in the elliptic curve case (but they're not the same curves!). As we have an equivalence between A-submodules of $\mathbb{G}_{a,\mathbf{C}}$ and isogenies (Proposition 1.1.4), we see that $Y_0(N)$ also parametrizes isomorphism classes of triples (ϕ, ϕ', f), where $f : \phi \to \phi'$ is a cyclic isogeny of degree N. We denote a typical point in $Y_0(N)$ by (ϕ, C), $(\phi \to \phi')$ or even $(\phi \to \phi/C)$.

The curves $Y(N)$ and $Y_0(N)$ can be compactified by adding finitely many cusps (see for example [29]), giving projective algebraic curves denoted by $X(N)$ and $X_0(N)$, respectively.

1.3.3 The curves $Y(N)$, $Y_0(N)$ and $Y_2(N)$

As $\Gamma(N) \subset \Gamma_0(N) \subset \mathrm{PGL}_2(A)$, we get canonical maps, which we refer to as coverings, $Y(N) \to Y_0(N) \to Y(1) \cong \mathbb{A}^1$. We now investigate the Galois theory of these coverings.

As in the classical case, the covering $Y(N)/Y(1)$ is Galois (see [25]), with Galois group

$$\begin{aligned} \mathrm{Gal}(Y(N)/Y(1)) &\cong \mathrm{PGL}_2(A)/\Gamma(N) \\ &\cong \{\alpha \in \mathrm{GL}_2(A/NA) \mid \det(\alpha) \in \mathbb{F}_q^*\}/Z(\mathbb{F}_q^*) \\ &= G(N)/Z(\mathbb{F}_q^*), \end{aligned} \tag{1.10}$$

where the second isomorphism is induced by reduction mod N of $\mathrm{PGL}_2(A)$, which has kernel $\Gamma(N)$. Here we have introduced the notation

$$G(N) = \{\alpha \in \mathrm{GL}_2(A/NA) \mid \det(\alpha) \in \mathbb{F}_q^*\}.$$

The curve $Y_0(N)$ corresponds via Galois theory to the Borel subgroup of (1.10):

$$B(N) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(A/NA) \mid ad \in \mathbb{F}_q^* \right\} / Z(\mathbb{F}_q^*).$$

We see that $\mathrm{Gal}(Y(N)/Y(1))$ is not in general isomorphic to $\mathrm{PSL}_2(A/NA)$ (which does hold in the characteristic 0 case), so we define another modular curve[2]:

$$\begin{aligned}\Gamma_2(N) &= \{\gamma \in \mathrm{GL}_2(A) \mid (\gamma \bmod N) \in Z((A/NA)^*)\}/Z(\mathbb{F}_q^*) \subset \mathrm{PGL}_2(A),\\ Y_2(N) &= \Gamma_2(N)\backslash\Omega.\end{aligned}$$

Proposition 1.3.3 *The curve $Y_2(N)$ is Galois over $Y(1)$ and covers $Y_0(N)$. Suppose that N is square-free and that every prime factor $\mathfrak{p}$ of N has even degree. Then Gal$(Y_2(N)/Y(1)) \cong PSL_2(A/NA)$.*

Proof. Firstly, $\Gamma(N) \subset \Gamma_2(N) \subset \Gamma_0(N)$, so that we have coverings $Y(N) \to Y_2(N) \to Y_0(N)$. Now under reduction mod N of $\mathrm{PGL}_2(A)$, the subgroup $\Gamma_2(N)$ corresponds to the subgroup

$$H(N) = Z((A/NA)^*) \cap G(N)$$

of all scalar matrices in $G(N)$. Then $H(N)/Z(\mathbb{F}_q^*)$ is a normal subgroup of $G(N)/Z(\mathbb{F}_q^*)$. Hence, by the Galois theory of coverings (or, if the reader prefers, of the respective function fields) follows that $Y_2(N)$ is Galois over $Y(1)$, with Galois group

$$\mathrm{Gal}(Y_2(N)/Y(1)) \cong G(N)/H(N) \subset \mathrm{PGL}_2(A/NA),$$

which is in fact the subgroup of $\mathrm{PGL}_2(A/NA)$ of those elements with determinant in $\mathbb{F}_q^*$. In particular, $G(N)/H(N)$ contains $\mathrm{PSL}_2(A/NA)$

Now suppose N is square-free, and that every prime factor of N has even degree. Then $A/NA \cong \prod_{i=1}^m (A/\mathfrak{p}_i A)$, and every element of $\mathbb{F}_q^*$ is a square in $(A/NA)^*$. To see this, notice that the standard embedding $\mathbb{F}_q \hookrightarrow A/NA$ corresponds to the diagonal embedding

$$\begin{aligned}\mathbb{F}_q &\hookrightarrow \prod_{i=1}^m A/\mathfrak{p}_i A\\ x &\mapsto ((x \bmod \mathfrak{p}_1), \ldots, (x \bmod \mathfrak{p}_m)) = (x, \ldots, x).\end{aligned}$$

Now as $\deg(\mathfrak{p}_i)$ is even follows that $\mathbb{F}_{q^2} \hookrightarrow A/\mathfrak{p}_i A$ and so $x \in \mathbb{F}_q$ is a square in $A/\mathfrak{p}_i A$, for every $i = 1, \ldots, m$. It follows that $G(N)/H(N) = \mathrm{PSL}_2(A/NA)$. □

1.3.4 Modular curves in $\mathbb{A}^n$

In this thesis we consider $\mathbb{A}^n$ as the moduli space of n-tuples of Drinfeld modules, via the map $(\phi^1, \ldots, \phi^n) \to (j(\phi^1), \ldots, j(\phi^n))$. We are interested in the distribution of *CM points* in $\mathbb{A}^n(\mathbf{C})$, that is points $(j(\phi^1), \ldots, j(\phi^n))$ for which every ϕ^i has complex multiplication. In particular, we will prove (Chapter 3) that the Zariski-closure of a set of CM points is a so-called *modular variety.*

[2]There already exist (Drinfeld) modular curves $Y_1(N)$, although they don't appear in this thesis, which is why we use the notation $Y_2(N)$

This is an analogue of (a special case of) the André-Oort Conjecture. In order to define modular varieties we must first define the modular curves in $\mathbb{A}^n$. That is the aim of this section.

We first investigate the image of $Y_0(N)$ in the affine plane $\mathbb{A}^2$. Using the j-invariant we obtain the most natural map

$$\begin{array}{rcl}(j\times j): Y_0(N) & \longrightarrow & \mathbb{A}^2 \\ (\phi\to\phi') & \longmapsto & (j(\phi), j(\phi')).\end{array}$$

The image, which we denote by $Y_0'(N)$, is the locus of an irreducible polynomial $\Phi_N(t_1,t_2)\in A[t_1,t_2]$ (see [5]). In general the image is not smooth.

We are principally interested in the curves $Y_0'(N)$ over $\mathbf{C}$. From now on, by a point of $Y_0'(N)$ we mean a $\mathbf{C}$-valued point. Let $z,z'\in\Omega$. Then ϕ^z and $\phi^{z'}$ are isogenous if and only if there exists some $\sigma\in \mathrm{PGL}_2(k)$ with $z'=\sigma(z)$. View σ as an element of $\mathrm{GL}_2(k)$ and let $a\in A$ be such that the four entries of $a\sigma$ are in A and relatively prime, and let $N=\det(a\sigma)$. We call N the *degree* of σ. Then there exists a cyclic isogeny of degree N between ϕ^z and $\phi^{z'}$. Notice that a is uniquely determined up to a unit, and thus N is determined up to the square of a unit. $Y_0'(N)$ is thus given as the image of the map

$$\begin{array}{rcl}\Omega & \longrightarrow & \mathbb{A}^2(\mathbf{C}) \\ z & \longmapsto & (j(z), j(\sigma(z))).\end{array}$$

This suggests the construction of modular curves in $\mathbb{A}^n$. Let $\sigma_1,\dots,\sigma_n\in \mathrm{PGL}_2(k)$, and consider the map

$$\begin{array}{rcl}\rho:\Omega & \longrightarrow & \mathbb{A}^n(\mathbf{C}) \\ z & \longmapsto & (j(\sigma_1(z)),\dots,j(\sigma_n(z))).\end{array} \tag{1.11}$$

The image lies on an irreducible algebraic curve $Y\subset\mathbb{A}^n$. We will investigate this curve.

One checks (as in §B.4) that we have $\rho(z)=\rho(z')$ if and only if $z'=\gamma(z)$ for some $\gamma\in\Gamma=\cap_{i=1}^n\sigma_i^{-1}\mathrm{PGL}_2(A)\sigma_i$. It follows that the image of (1.11) is a model of $Y_\Gamma=\Gamma\backslash\Omega$, and we denote it by Y_Γ'.

Let $\sigma_2'=\sigma_2\sigma_1^{-1},\dots,\sigma_n'=\sigma_n\sigma_{n-1}^{-1}$, and $\sigma_1'=\sigma_1$, so that

$$(\sigma_1,\ \sigma_2,\dots,\sigma_n)=(\sigma_1',\ \sigma_2'\sigma_1',\ \sigma_3'\sigma_2'\sigma_1',\dots,\sigma_n'\sigma_{n-1}'\cdots\sigma_2'\sigma_1').$$

Let N_i be the degree of σ_i'. Then the curve Y is irreducible (being the rigid analytic image of Ω) and algebraic, defined by a prime factor of the ideal

$$\langle\Phi_{N_2}(t_1,t_2),\Phi_{N_3}(t_2,t_3),\dots,\Phi_{N_n}(t_{n-1},t_n)\rangle\subset A[t_1,t_2,\dots,t_n]. \tag{1.12}$$

Let $Y_0'(N_2,\dots,N_n)$ denote the algebraic curve in $\mathbb{A}^n$ defined by the ideal (1.12), then we may discribe it as follows.

$$\begin{array}{rl}Y_0'(N_2,\dots,N_n)= & \{(x_1,\dots,x_n)\in\mathbb{A}^n \mid \text{there exist cyclic isogenies} \\ & x_{i-1}\to x_i \text{ of degree } N_i \text{ for all } i=2,\dots,n\}.\end{array}$$

We let $p_{i,j}:\mathbb{A}^n\to\mathbb{A}^2$ denote projection onto the ith and jth coordinates. Then we have the following characterization of modular curves in $\mathbb{A}^n$.

Proposition 1.3.4 *Let $Y \subset \mathbb{A}^n$ be an irreducible algebraic curve. Then the following are equivalent.*

1. *Y is an irreducible component of $Y_0'(N_2, \ldots, N_n)$*
2. *Y is the image of the map $z \mapsto (j(\sigma_1(z)), \ldots, j(\sigma_n(z)))$, where N_i is the degree of $\sigma_i \sigma_{i-1}^{-1}$ for $i = 2, \ldots, n$.*
3. *There exists $1 \leq i \leq n$ such that $p_{ij}(Y) = Y_0'(M_{ij})$ for some $M_{ij} \in A$ for all $j \neq i$.*
4. *$p_{i-1,i}(Y) = Y_0'(N_i)$ for all $i = 2, \ldots, n$.*

Proof. (1) $\Leftrightarrow$ (2): It is clear that the points $\sigma_{i-1}(z)$ and $\sigma_i(z)$ are linked by a cyclic isogeny of degree N_i, for all $i = 2, \ldots, n$, so the image of the map (1.11) forms an irreducible component of $Y_0'(N_2, \ldots, N_n)$. On the other hand, every point of $Y_0'(N_2, \ldots, N_n)(\mathbf{C})$ is of the form $(j(\sigma_1(z)), \ldots, j(\sigma_n(z)))$ for some $z \in \Omega$ and some $(\sigma_1, \ldots, \sigma_n) \in \mathrm{PGL}_2(k)^n$, so every irreducible component of $Y_0'(N_2, \ldots, N_n)$ arises in this way.

(1) $\Leftrightarrow$ (4): Clearly $p_{i-1,i}(Y_0'(N_2, \ldots, N_n))$ is an irreducible component of $Y_0'(N_i)$, which is irreducible, for each i. Conversely, if a curve Y projects onto the $Y_0'(N_i)$'s, then it must be contained in $Y_0'(N_2, \ldots, N_n)$ by definition.

Similarly (1) $\Leftrightarrow$ (3).

□

Definition 1.3.5 *A permutation $\pi \in S_n$ acts on $\mathbb{A}^n$ by permuting the coordinates, and the resulting automorphism of $\mathbb{A}^n$ is called a* permutation of coordinates.

Definition 1.3.6 *A curve Y satisfying the conditions of Proposition 1.3.4 is called a* pure modular curve*, and an irreducible algebraic curve Y in $\mathbb{A}^n$ is called* modular *if, up to permutation of coordinates, it is given as the product of a CM point in $\mathbb{A}^m$ and a pure modular curve in $\mathbb{A}^{n-m}$, where $0 \leq m < n$.*

We will prove in Chapter 3 that the modular curves are precisely those curves in $\mathbb{A}^n$ containing infinitely many CM points.

1.3.5 Degeneracy maps and Hecke correspondences

Let C be an A-submodule of $\mathbf{C}$ (via a Drinfeld module ϕ) with $C \cong A/NA$. For any element $d|N$ we denote by $C[d]$ the unique A-submodule of C isomorphic to A/dA, so $C[d]$ can be considered as the submodule of d-division points of C. We also have $C[d] = \phi[d] \cap C$. Let $N, M \in A$ and $d|M$. Then we define the *d-th degeneracy map* by

$$\begin{array}{rcl} \beta_d : Y_0(NM) & \longrightarrow & Y_0(N) \\ (\phi \to \phi/C) & \longmapsto & (\phi/C[d] \to \phi/C[dN]), \end{array}$$

which comes from the factorization

$$\phi \xrightarrow{d} \phi/C[d] \xrightarrow{N} \phi/C[dN] \xrightarrow{M/d} \phi/C.$$

Using the cases $d = 1$ and $d = M$, we can construct the usual Hecke correspondences on $Y_0(N)$: We denote by T_M the image of

$$\begin{aligned} \beta_1 \times \beta_M : Y_0(NM) &\longrightarrow Y_0(N)^2 \\ (\phi \to \phi/C) &\longmapsto \Big((\phi \to \phi/C[N]), (\phi/C[M] \to \phi/C)\Big), \end{aligned}$$

which can also be written as the image of Ω under the map

$$z \longmapsto \Big((\phi^z \to \phi^{Nz}),\ (\phi^{Mz} \to \phi^{MNz})\Big).$$

We note that there is a commutative diagram of cyclic isogenies

$$\begin{array}{ccc} \phi & \xrightarrow{N} & \phi/C[N] \\ \downarrow{\scriptstyle M} & & \downarrow{\scriptstyle M} \\ \phi/C[M] & \xrightarrow{N} & \phi/C. \end{array}$$

We now define Hecke correspondences in a more general case. Let $\Gamma_1, \ldots, \Gamma_n$ be congruence subgroups of $\mathrm{PGL}_2(A)$, and consider the modular curves $Y_i = \Gamma_i \backslash \Omega$. Let $\sigma_1, \ldots, \sigma_n, \in \mathrm{PGL}_2(k)$. Then the image of the map

$$\begin{aligned} \Omega &\longrightarrow Y_1 \times \cdots \times Y_n \\ z &\longmapsto (\sigma_1(z), \ldots, \sigma_n(z)) \end{aligned}$$

is called a Hecke correspondence on $Y = Y_1 \times \cdots \times Y_n$ and is denoted $T_{N_2,N_3,\ldots,N_n}$, where the degrees N_i are defined as in the previous section. The image is also sometimes referred to as a modular curve in Y. Note that Y no longer comes with any specific affine embedding. In fact we can just as well consider the compactifications X_i of Y_i and denote by $T_{N_2,N_3,\ldots,N_n}$ the closure of $T_{N_2,N_3,\ldots,N_n}$ in $X = X_1 \times \cdots \times X_n$. Let $\Gamma = \cap_{i=1}^n \sigma_i^{-1} \Gamma_i \sigma_i$, then the above Hecke correspondences are birational to $Y_\Gamma = \Gamma \backslash \Omega$ and the compactification X_Γ of Y_Γ, respectively.

Note that for $\Gamma_i = \mathrm{PGL}_2(A)$ for $i = 1, \ldots, n$ this gives us the modular curves defined in the previous section. If $n = 2$, $\Gamma_1 = \Gamma_2 = \Gamma_0(N)$ and $\sigma_2 \sigma_1^{-1}$ has degree M, then we get back our previous construction of the Hecke correspondence T_M on $Y_0(N)^2$ (and on $X_0(N)^2$).

The curve $Y_0'(M)$ in $\mathbb{A}^2$ can be considered as a correspondence on $\mathbb{A}^1$, which we will call the *Hecke operator* $T_{\mathbb{A}^1,M}$. It sends subsets of $\mathbb{A}^1(\mathbf{C})$ to subsets of $\mathbb{A}^1(\mathbf{C})$, and is determined by

$$\begin{aligned} T_{\mathbb{A}^1,M}(\{x\}) &= \{y \in \mathbb{A}^1 \mid (x, y) \in Y_0'(M)\} \\ &= \{y \in \mathbb{A}^1 \mid \text{There exists a cyclic isogeny } x \to y \text{ of degree } M\}. \end{aligned}$$

We will give a thorough treatment of Hecke operators in Chapter 2.

A word on terminology is in order. By a Hecke *correspondence* we will mean a subcurve of a product of modular curves (e.g. $X_0(N)$ or $\mathbb{A}^1$) arising from isogeny conditions between the factors. By a Hecke *operator* we will mean the action on the set of subsets of a product of modular curves $X = \prod_{i=1}^n X_i$ arising from a Hecke *correspondence* in X^2.

1.3.6 Modular varieties

We now define the modular subvarieties of $\mathbb{A}^n$, which are the characteristic p analogues of the subvarieties of Hodge type of the Shimura variety $\mathbb{A}^n$ over $\mathbb{C}$.

Recall that a point $x \in \mathbb{A}^n(\mathbf{C})$ is called a CM point if every coordinate of x is the j-invariant of a Drinfeld module with complex multiplication.

Definition 1.3.7 *An irreducible algebraic variety X in $\mathbb{A}^n$ is said to be a* modular variety *if it is isomorphic, via some permutation of coordinates $\pi \in S_n$, to a variety of the form*

$$\mathbb{A}^{n_0} \times \prod_{i=1}^{g} Y'_{\Gamma_i} \times \{x\} \tag{1.13}$$

where each Y'_{Γ_i} is a pure modular curve in $\mathbb{A}^{n_i}$ and x is a CM point in $\mathbb{A}^{n_{g+1}}$, and $n = n_0 + \cdots + n_{g+1}$. A reducible variety is modular if all its irreducible components are modular. The data

$$(\pi, n_0, Y'_{\Gamma_1}, \ldots, Y'_{\Gamma_g})$$

is called the type *of X.*

A modular variety is pure *if it is the product of pure modular curves (including $\mathbb{A}^1$), i.e. if the projections $p_i : X \to \mathbb{A}^1$ are dominant on every irreducible component of X.*

We point out that for a given $B > 0$, there are only finitely many different types of modular varieties X with $\deg(X) \leq B$. This follows because the degrees of the modular polynomials $\Phi_M(t_1, t_2)$ increase with $|M|$. See Chapter 2 for a discussion of the degrees of modular curves, and for a proof of this claim (Proposition 2.1.7).

In this case, translating the André-Oort conjecture to characteristic p suggests

Theorem 1.7 *Let X be an irreducible algebraic variety in $\mathbb{A}^n$. Then X contains a Zariski-dense set of CM points if and only if X is modular.*

(This theorem also goes by the names of Theorem 0.8 and Theorem 3.5). It is clear that the CM points on a modular variety are Zariski-dense, as a modular curve contains infinitely many CM points. The converse, of course, is the hard part.

We now make a number of elementary observations. Let $I \subset \{1, \ldots, n\}$ and denote by $p_I : \mathbb{A}^n \to \mathbb{A}^I$ the projection onto the coordinates listed in I.

Proposition 1.3.8

1. *Let $X \subset \mathbb{A}^n$ be a modular variety. Then $p_I(X)$ is a modular variety in $\mathbb{A}^I$.*

2. *Let $Y \subset \mathbb{A}^I$ be a modular variety. Then $p_I^{-1}(Y)$ is a modular variety in $\mathbb{A}^n$.*

3. *Every irreducible component of the intersection of modular varieties is modular.*

4. *Let $Z \subset \mathbb{A}^n$ be an irreducible variety of dimension d, then Z is an irreducible component of*
$$\bigcap_{\substack{I \subset \{1,\ldots,n\} \\ \#I = d+1}} p_I^{-1}(p_I(Z)). \tag{1.14}$$

In particular, it suffices to prove Theorem 1.7 for hypersurfaces in $\mathbb{A}^n$.

Proof. The first three claims follow directly from the definition of modular varieties. We prove (4). Let $(x_1, \ldots, x_n)$ be a generic point of X. Then, after a permutation of coordinates, we may assume that $\{x_1, \ldots, x_d\}$ is a transcendence basis for the function field $\mathbf{C}(X)$, and the other x_j, $j > d$ are algebraic over $\mathbf{C}(x_1, \ldots, x_d)$. Let $I_j = \{1, \ldots, d, j\}$ for $j > d$. Then $\dim(p_{I_j}(Z)) = d$ and $Z_j = p_{I_j}^{-1}(p_{I_j}(Z))$ is the hypersurface in $\mathbb{A}^n$ defined by the algebraic relation of x_j over the $x_1, \ldots, x_d$'s. It follows that the intersection $\cap_{j=d+1}^n Z_j$ is a variety defined by the relations linking each x_j to the $x_1, \ldots, x_d$'s, hence has dimension at most d. It follows that the intersection (1.14) has dimension at most d. But as (1.14) contains Z, it has dimension exactly d, and the result follows.

Now if $Z \subset \mathbb{A}^n$ is a variety, which we want to show modular, then from the above follows that it suffices to show that each $p_I(Z) \subset \mathbb{A}^I$ is modular, for $\#I = d + 1$. These are hypersurfaces, so if we can prove Theorem 1.7 for hypersurfaces, then we can also prove it for Z.

□

In the more general case, let $Z = \prod_{i=1}^n X_i$ be a product of modular curves $X_i =$ (compactification of $\Gamma_i \backslash \Omega$), where the Γ_i's are congruence subgroups of $\mathrm{PGL}_2(A)$. A point $x = (z_1, \ldots, z_n)$ in Z is a CM point if (a representative in Ω of) every z_i is quadratic imaginary (i.e. the corresponding Drinfeld module, ignoring the level structure, has complex multiplication).

Definition 1.3.9 *An irreducible subvariety X of Z is* modular *if there is a partition $\{1, \ldots, n\} = \coprod_{i=0}^{g+1} S_i$, and X is given by*
$$X = \prod_{i \in S_0} X_i \times \prod_{j=1}^{g} T_j \times \{x\} \tag{1.15}$$

where each T_j is a Hecke correspondence in $\prod_{i \in S_j} X_i$ and x is a CM point in $\prod_{i \in S_{g+1}} X_i$. As before, a reducible subvariety is modular if all its irreducible components are modular, and is pure if the projections $p_i : X \to X_i$ are dominant for each i from every irreducible component of X.

In this setting we have

Theorem 1.8 *Let X be an irreducible subvariety of Z. Then X contains a Zariski-dense set of CM points if and only if X is modular.*

We will prove Theorems 1.7 and 1.8 in Chapter 3.

We will now see that this additional level of generality does not give us anything new, i.e. *level structures don't matter.*

Proposition 1.3.10 *The statements of Theorems 1.7 and 1.8 are equivalent.*

Proof. It is clear that Theorem 1.7 is a special case of Theorem 1.8. The converse is not much harder. Let $Z = \prod_{i=1}^{n} X_i$ be a product of modular curves $X_i = (\Gamma_i \backslash \Omega) \cup \{\text{cusps}\}$. Firstly, we may throw away the cusps, as they don't correspond to Drinfeld modules, hence are not CM points. So let $Z' = \prod_{i=1}^{n} Y_i$ be the affine part of Z, where each $Y_i = \Gamma \backslash \Omega$ is the affine part of X_i. Then a subvariety X of Z is modular if and only if $X' = X \cap Z'$ is modular in Z'.

Next, let $p_i : Y_i = \Gamma_i \backslash \Omega \to \mathrm{PGL}_2(A) \backslash \Omega \cong \mathbb{A}^1$ be the standard projections, induced by the inclusions $\Gamma_i \subset \mathrm{PGL}_2(A)$, and consider their product $p : Z' \to \mathbb{A}^n$. A moment's reflection reveals that a subvariety X of Z' is modular according to Definition 1.3.9 if and only if $p(X) \subset \mathbb{A}^n$ is modular according to Definition 1.3.7. Likewise CM points of Z' correspond to CM points of $\mathbb{A}^n$ and dense sets correspond to dense sets. So the two formulations are in fact equivalent. □

In view of this equivalence, we will only concern ourselves with CM points and subvarieties in $\mathbb{A}^n$, which requires less cumbersome notation, knowing that analogous results hold automatically for products of Drinfeld modular curves.

Chapter 2

Hecke operators

In this chapter we will investigate the action of Hecke operators on affine varieties. The last two sections contain an analogue for Drinfeld modular curves of Edixhoven's fundamental theorem (Theorem 0.6), as well as a generalization to subvarieties of higher dimensions.

2.1 Basic definitions

Throughout this chapter, $\mathfrak{m}$ denotes a monic square-free element of A.

For $I \subset \{1, \ldots, n\}$, we denote by

$$p_I : \mathbb{A}^n \longrightarrow \mathbb{A}^I$$

the projection onto the ith coordinates, $i \in I$.

2.1.1 Hecke operators and Hecke orbits

Definition 2.1.1 *The* Hecke operator $T_{\mathbb{A}^n,\mathfrak{m}}$ *on* $\mathbb{A}^n$ *is the correspondence given by the image of*

$$\begin{array}{rcl} Y_0'(\mathfrak{m})^n & \longrightarrow & \mathbb{A}^n \times \mathbb{A}^n \\ ((x_1, y_1), \ldots, (x_n, y_n)) & \longmapsto & ((x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)). \end{array}$$

We may also view $T_{\mathbb{A}^n,\mathfrak{m}}$ *as a map from subsets of* $\mathbb{A}^n(\mathbf{C})$ *to subsets of* $\mathbb{A}^n(\mathbf{C})$*, generated by its action on single points:*

$$T_{\mathbb{A}^n,\mathfrak{m}} : (x_1, \ldots, x_n) \mapsto \{(y_1, \ldots, y_n) \quad | \quad \begin{array}{l} \textit{There exist cyclic isogenies } x_i \to y_i \\ \textit{of degree } \mathfrak{m} \textit{ for all } i = 1, \ldots, n\}. \end{array}$$

We also use the notation $T_{\mathfrak{m}}$ when the $\mathbb{A}^n$ is clear. We notice that the operator $T_{\mathfrak{m}}$ is symmetric, in the sense that $x \in T_{\mathfrak{m}}(y) \Leftrightarrow y \in T_{\mathfrak{m}}(x)$. We also notice that $T_{\mathfrak{m}}$ is defined over k. Let $X = \cup_{i=1}^r X_i$ be a variety in $\mathbb{A}^n$, with irreducible components $X_1, \ldots, X_r$. Then

$$T_{\mathfrak{m}}(X) = p_2(T_{\mathbb{A}^n,\mathfrak{m}} \cap (X \times \mathbb{A}^n)),$$

where $p_2 : \mathbb{A}^n \times \mathbb{A}^n \to \mathbb{A}^n$ denotes the projection onto the second copy of $\mathbb{A}^n$. So $T_{\mathfrak{m}}(X)$ is also a variety in $\mathbb{A}^n$, and $T_{\mathfrak{m}}(X) = \cup_{i=1}^r T_{\mathfrak{m}}(X_i)$. We recall the function

$$\psi(\mathfrak{m}) = |\mathfrak{m}| \prod_{\mathfrak{p}|\mathfrak{m}} \left(1 + \frac{1}{|\mathfrak{p}|}\right),$$

where the product ranges over monic primes $\mathfrak{p}|\mathfrak{m}$. The curve $Y_0'(\mathfrak{m})$ is defined by the modular polynomial $\Phi_{\mathfrak{m}}(t_1, t_2) \in A[t_1, t_2]$, which is symmetrical in t_1 and t_2, and has degree $\psi(\mathfrak{m})$ in t_1 (and in t_2), see [5]. It follows that each $T_{\mathfrak{m}}(X_i)$ has at most $\psi(\mathfrak{m})^n$ irreducible components (as each point has $\psi(\mathfrak{m})^n$ images), each of dimension equal to $\dim(X_i)$. So if Y is an irreducible variety in $\mathbb{A}^n$, of the same dimension as X_i, and if $Y \subset T_{\mathfrak{m}}(X_i)$, then Y is an irreducible component of $T_{\mathfrak{m}}(X_i)$.

Now suppose that $X \subset T_{\mathfrak{m}}(X)$. In this case we say that X is *stabilized* by $T_{\mathfrak{m}}$. Then each X_i is an irreducible component of some $T_{\mathfrak{m}}(X_j)$. We may restrict $T_{\mathbb{A}^n,\mathfrak{m}}$ to X as follows.

Definition 2.1.2 *Let X be a variety in $\mathbb{A}^n$, and suppose all of its irreducible components have the same dimension. If $X \subset T_{\mathbb{A}^n,\mathfrak{m}}(X)$, then the Hecke operator* restricted to X *is defined by*

$$T_{X,\mathfrak{m}} = \textit{union of components of } T_{\mathbb{A}^n,\mathfrak{m}} \cap (X \times X) \textit{ of maximal dimension.}$$

Whenever we use the notation $T_{X,\mathfrak{m}}$, then it is implicit that X is stabilized by $T_{\mathbb{A}^n,\mathfrak{m}}$. The correspondence $T_{X,\mathfrak{m}}$ is still surjective in the sense that the two projections $p_X : T_{X,\mathfrak{m}} \to X$ are surjective. In fact we have more.

$$T_{X,\mathfrak{m}} = \bigcup_{(i,j)\in J} T_{X,\mathfrak{m},(i,j)},$$

where $T_{X,\mathfrak{m},(i,j)} \subset X_i \times X_j$ is a finite union of irreducible components, each a surjective correspondence from X_i to X_j. The set $J \subset \{1, \ldots, r\}^2$ is the induced correspondence on the finite set of irreducible components of X. We may compose Hecke correspondences, and we have the standard property

Proposition 2.1.3 *Let $\mathfrak{m}_1, \mathfrak{m}_2 \in A$ be relatively prime. Then*

$$T_{\mathfrak{m}_1} \circ T_{\mathfrak{m}_2} = T_{\mathfrak{m}_1\mathfrak{m}_2}.$$

Proof. The proof is similar to the classical case, and follows because the kernel of the composition of two cyclic isogenies of degree $\mathfrak{m}_1$ and $\mathfrak{m}_2$ must be of the form $A/\mathfrak{n}_1 \times A/\mathfrak{n}_2$ for some $\mathfrak{n}_1, \mathfrak{n}_2$ satisfying $\mathfrak{n}_1\mathfrak{n}_2 = \mathfrak{m}_1\mathfrak{m}_2$. But if $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are relatively prime, then the Chinese remainder theorem gives

$$A/\mathfrak{n}_1 A \times A/\mathfrak{n}_2 \cong A/\mathfrak{m}_1\mathfrak{m}_2 A,$$

and the result follows. We will not need this result.

□

Definition 2.1.4 *Let $X \subset \mathbb{A}^n$ be a variety (possibly $X = \mathbb{A}^n$), and $S \subset X$ a subset. Then the* Hecke orbit *of S under $T_{X,\mathfrak{m}}$ is given by*

$$T^{\infty}_{X,\mathfrak{m}}(S) = \{x \in X \mid x \in T^{d}_{X,\mathfrak{m}}(S), \text{ for some } d \geq 1\}.$$

(Here $T^{d}_{X,\mathfrak{m}}$ means $T_{X,\mathfrak{m}}$ iterated d times.)

Write $X = \cup_{i=1}^{r} X_i$. As there are only finitely many correspondences on the finite set of irreducible components of X, we have

$$T^{\infty}_{X,\mathfrak{m}}(X_i) = T^{d}_{X,\mathfrak{m}}(X_i) = \bigcup_{j \in I} X_j$$

for some $d \in \mathbb{N}$ sufficiently large, and some $I \subset \{1, \ldots, r\}$. We also have

$$T^{\infty}_{X,\mathfrak{m}}(X_i) = T^{\infty}_{X,\mathfrak{m}}(X_j)$$

for every $j \in I$. So we may decompose X into a finite disjoint union of Hecke orbits, each orbit being generated by each of its irreducible components. If $S \subset X_i$ is Zariski-dense, then $T^{\infty}_{X,\mathfrak{m}}(S)$ is Zariski-dense in all of $T^{\infty}_{X,\mathfrak{m}}(X_i)$.

2.1.2 Some intersection theory

We need to define the *degree* of a variety $X \subset \mathbb{A}^n$. For our purposes, the most naïve definition will do.

Definition 2.1.5 *Let $X \subset \mathbb{A}^n$ be an irreducible variety of dimension d. We define*

$$\deg(X) = \sup\{\#(X \cap H) \quad | \quad H \text{ a linear variety of codimension } d \text{ in } \mathbb{A}^n \text{ for which this intersection has dimension zero}\}.$$

If X is not irreducible, then $\deg(X)$ *is the sum of the degrees of its irreducible components of maximal dimension.*

There exist more high-brow definitions for the degree, for example in terms of the Hilbert polynomial associated to the homogenization of the coordinate ring of X (see [32]). The degree has the following properties.

Proposition 2.1.6 *Let $X \subset \mathbb{A}^n$ be a variety of dimension d.*

1. *X has at most* $\deg(X)$ *irreducible components of maximal dimension.*
2. *If $Y \subset \mathbb{A}^n$ is another variety, then* $\deg(X \cap Y) \leq \deg(X)\deg(Y)$.
3. *Let $I \subset \{1, \ldots, n\}$, $\#I = d$ such that $p_I : X \to \mathbb{A}^I$ is dominant. Then the degree of the projection p_I is at most* $\deg(X)$.
4. $\psi(\mathfrak{m}) \leq \deg(Y_0'(\mathfrak{m})) \leq 2\psi(\mathfrak{m})$.
5. $\deg(T_{\mathbb{A}^n,\mathfrak{m}}(X)) \leq 2^n \psi(\mathfrak{m})^n \deg(X)$.

Proof. (1) is obvious.

(2) is a version of Bézout's Theorem. Denote by $\overline{X}$ and $\overline{Y}$ the Zariski-closures of X and Y in $\mathbb{P}^n$. Then [24, Example 8.4.6] tells us that $\deg(\overline{X} \cap \overline{Y}) \leq \deg(\overline{X}) \deg(\overline{Y})$, from which the result follows. (Here the degree of a projective variety is defined the same way).

(3) follows because the fibre $p_I^{-1}(x)$ for $x \in \mathbb{A}^I$ is the intersection of X with a linear subspace of codimension d.

(4). The curve $Y_0'(\mathfrak{m})$ is given by the modular polynomial $\Phi_\mathfrak{m}(t_1, t_2)$, which has degree $\psi(\mathfrak{m})$ in each variable t_1 and t_2. Hence the total degree is at most $2\psi(\mathfrak{m})$. There is also an exact expression for the degree, see Proposition 2.2.1 below.

(5). $T_{\mathbb{A}^n,\mathfrak{m}}(X)$ is the projection onto the second copy of $\mathbb{A}^n$ of the intersection $T_{\mathbb{A}^n,\mathfrak{m}} \cap (X \times \mathbb{A}^n)$. The result now follows from (2) and (4). □

Let $X \subset \mathbb{A}^n$ be a modular variety. Recall from Definition 1.3.7 that this means that there exists some permutation of coordinates $\pi \in S_n$, such that we may write

$$\pi(X) = \mathbb{A}^{n_0} \times \prod_{i=1}^{g} Y_i \times \{x\},$$

Where each Y_i is a pure modular curve in $\mathbb{A}^{n_i}$, $x \in \mathbb{A}^{n_{g+1}}$ is a CM point and $n = n_0 + \cdots + n_{g+1}$. Recall further that the data $(\pi, n_0, Y_1, \ldots, Y_g)$ is called the *type* of X.

Proposition 2.1.7 *Let $B > 0$ and $n \in \mathbb{N}$ be given. Then there are only finitely many different types of modular varieties $X \subset \mathbb{A}^n$ with $\deg(X) \leq B$.*

Proof. There are only finitely many permutations of coordinates $\pi \in S_n$, and $\deg(X) \geq \prod_{i=1}^{g} \deg(Y_i)$. So it remains to show that there are only finitely many pure modular curves $Y \subset \mathbb{A}^n$ with degree less than a given bound. Let $p_{\{i,i+1\}}(Y) = Y_0'(N_i)$ for $i = 1, \ldots, n-1$. Now $\deg(Y) \geq \deg(p_{\{i,i+1\}}(Y)) \geq \psi(N_i)$ for all i. There are only finitely many possible values for N_i with $\psi(N_i)$ bounded, and thus only finitely many possibilities for Y. □

2.2 Points stabilized by Hecke operators

We are interested in the *stable points* of $T_{\mathbb{A}^1,\mathfrak{m}}$, i.e. those $x \in \mathbb{A}^1$ satisfying $x \in T_{\mathbb{A}^1,\mathfrak{m}}(x)$. If this is the case, then x has a cyclic endomorphism of degree $\mathfrak{m}$, hence x must be a CM point, as the "multiplication by n" endomorphisms ϕ_n have kernels $\phi[n] \cong (A/nA)^2$, which are not cyclic.

Clearly $x \in T_{\mathbb{A}^1,\mathfrak{m}}(x)$ if and only if x is a root of the modular polynomial $\Phi_\mathfrak{m}(t,t)$. To list some properties of this polynomial, we need some notation. Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let $H_\mathcal{O}(t)$ be the minimal polynomial of $j(\mathcal{O}) = j(\phi^\mathcal{O})$ in K. Then we have (see [69])

$$H_\mathcal{O}(t) = \prod_{[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})} (t - j(\mathfrak{a})) \qquad \text{if } q \text{ is odd,}$$

$$H_{\mathcal{O}}(t) = \prod_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O})} (t - j(\mathfrak{a}))^2 \qquad \text{if } q \text{ is even.}$$

We are only interested in the case where q is odd. An element $\alpha \in \mathcal{O}$ is *primitive* if it cannot be written in the form $\alpha = r\beta$, with $r \in k,\ \deg(r) > 0$ and $\beta \in \mathcal{O}$. We set

$$\gamma(\mathcal{O}, \mathfrak{m}) = \#(\{\alpha \in \mathcal{O} \mid \alpha \text{ is primitive and } N_{K/k}(\alpha) \in \mathbb{F}_q^*\mathfrak{m}\}/\mathcal{O}^*).$$

Then we have (see [5] and [69])

Proposition 2.2.1 *Let $\mathfrak{m} \in A$ be monic and square-free.*

1. *There exists a constant $c_{\mathfrak{m}} \in \mathbf{C}$ such that*

$$\Phi_{\mathfrak{m}}(t, t) = c_{\mathfrak{m}} \prod_{\mathcal{O}} H_{\mathcal{O}}(t)^{\gamma(\mathcal{O},\mathfrak{m})},$$

   where the product is over all orders $\mathcal{O}$, but is finite as almost all the $\gamma(\mathcal{O}, \mathfrak{m})$'s are zero.

2. *The degree of $\Phi_{\mathfrak{m}}(t, t)$ is given by*

$$2 \sum_{\substack{a|\mathfrak{m} \\ \deg(a) > \deg(\mathfrak{m})/2}} |a| \ + \sum_{\substack{a|\mathfrak{m} \\ \deg(a) = \deg(\mathfrak{m})/2}} \frac{(q-2)|\mathfrak{m}| + |\mathfrak{m} - a^2|}{(q-1)|\mathfrak{m}|^{1/2}}.$$

We now fix some CM point $x \in \mathbb{A}^1$ and ask for which (monic) primes $\mathfrak{p} \in A$ we have $x \in T_{\mathbb{A}^1,\mathfrak{p}}(x)$. Let $\mathcal{O} = \mathrm{End}(x)$ be an order in K. Then we must have $\mathfrak{p}\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1$ (and thus also $\mathfrak{p}_2$) is principal in $\mathcal{O}$. If $\mathfrak{p}_1 = \mathfrak{p}_2$, then $\mathfrak{p}$ is ramified, which can only hold for finitely many $\mathfrak{p}$. If $\mathfrak{p}_1 \neq \mathfrak{p}_2$ are principal, then we say $\mathfrak{p}$ is *split principal* in $\mathcal{O}$. A prime $\mathfrak{p}$ is split principal in $\mathcal{O}$ if and only if $\mathfrak{p}$ splits completely in the ring class field $K_{\mathcal{O}}$, hence from Theorem 1.5 we see that the density (Dirichlet density, but we may even use the naïve density) of such primes in A is at least $1/[K_{\mathcal{O}} : k] = 1/2\#\mathrm{Pic}(\mathcal{O})$. In particular, there are infinitely many of them. In §§2.4 and 2.5 we will study *stable varieties* of Hecke operators.

We now derive another property of the curves $Y_0'(\mathfrak{m})$. This is a lower bound on $\#T_{\mathfrak{m},\mathbb{A}^1}(x)$ for a point $x \in \mathbb{A}^1$.

Proposition 2.2.2 *There exists a function $f : \mathbb{N} \to \mathbb{N}$ with $\lim_{n\to\infty} f(n) = \infty$ such that*

$$\#\{y \in \mathbf{C} \mid (x, y) \in Y_0'(\mathfrak{m})\} > f(|\mathfrak{m}|)$$

for all $x \in \mathbb{A}^1$.

Proof. Fix some $x \in \mathbb{A}^1$. Then there are exactly $\psi(\mathfrak{m})$ points y_i (counting multiplicities) such that there exist cyclic isogenies $x \to y_i$ of degree $\mathfrak{m}$. We want to bound these multiplicities. Suppose $y_1 = y_2 = y$. Then we have two distinct cyclic isogenies $f, g : x \to y$. Denote by $\hat{f}$ the dual isogeny of f, then $\alpha = \hat{f} \circ g \in \mathrm{End}(x)$ has norm $\mathfrak{m}^2$. As f and g are distinct, α is not any "multiplication by a" map, i.e. $\alpha \notin A$. It follows that x must be a CM point, and $\mathcal{O} = \mathrm{End}(x)$ is an order in an imaginary quadratic function field.

Let $\gamma(\mathfrak{m}) = \#\{\alpha \in \mathcal{O} \mid N(\alpha) = \mathfrak{m}\}/\mathcal{O}^*$. We have $\gamma(P) \leq 2$ for a prime $P \in A$, so $\gamma(P^e) \leq e + 1$ and in general

$$\gamma(\mathfrak{m}) \leq \prod_{P|\mathfrak{m}} (e_P + 1), \quad \text{for } \mathfrak{m} = \prod_{P|\mathfrak{m}} P^{e_P}.$$

There cannot be more that $\gamma(\mathfrak{m}^2)$ distinct cyclic isogenies of degree $\mathfrak{m}$ from x to y. So the number of different $y_i \in \mathbb{A}^1$ with $(x, y_i) \in Y_0'(\mathfrak{m})$ is at least

$$\psi(\mathfrak{m})/\gamma(\mathfrak{m}^2) \geq \prod_{P|\mathfrak{m}} \frac{P^{e_P} + P^{e_P - 1}}{2e_P + 1}$$

which is clearly bounded from below by an increasing function of $|\mathfrak{m}|$.

□

2.3 Surjectivity of projections

Proposition 2.3.1 *If $X_j \subset T^{\infty}_{X,\mathfrak{m}}(X_i)$, then $p_I : X_j \to \mathbb{A}^I$ is dominant if and only if $p_I : X_i \to \mathbb{A}^I$ is dominant. So every component in a Hecke orbit "behaves the same" under projections.*

Proof. Clearly it suffices to show that if $p_I : X_i \to \mathbb{A}^I$ is dominant, and $X_j \subset T_{X,\mathfrak{m}}(X_i)$, then $p_I : X_j \to \mathbb{A}^I$ is also dominant.

Let $x_I \in \mathbb{A}^I$ be a generic point. Then there is some $x \in X_i$ with $p_I(x) = x_I$. At least one point $y \in T_{X,\mathfrak{m}}(x)$ lies on X_j, and $p_I(y) = y_I \in T_{\mathbb{A}^I,\mathfrak{m}}(x_I)$. So it follows that every generic $x \in \mathbb{A}^I$ is $\mathfrak{m}$-isogenous to some y_I coming from X_j, in other words, $T_{\mathbb{A}^I,\mathfrak{m}}(p_I(X_j))$ is Zariski-dense in $\mathbb{A}^I$. Hence $\dim(p_I(X_j)) = \dim(T_{\mathbb{A}^I,\mathfrak{m}}(p_I(X_j))) = \dim(\mathbb{A}^I) = \#I$, and so $p_I(X_j)$ is Zariski-dense in $\mathbb{A}^I$, as required.

□

Theorem 2.1 *Let $X \subset \mathbb{A}^n$ be a variety all of whose components have the same dimension, and suppose that $X \subset T_{\mathfrak{m}}(X)$ for some square-free $\mathfrak{m} \in A$ which is a product of distinct primes $\mathfrak{p} \in A$ of even degree satisfying $|\mathfrak{p}| \geq \max(13, \deg X)$. Let $x \in X$ lie on an irreducible component X_i of X for which the projection $p_I : X_i \to \mathbb{A}^I$ is dominant. Then the projection of finite sets*

$$p_I : T_{X,\mathfrak{m}}(x) \longrightarrow T_{\mathbb{A}^I,\mathfrak{m}}(p_I(x)) \tag{2.1}$$

is surjective.

Proof. We first show that it suffices to prove this theorem for generic $x \in X$, rather than all $x \in X$.

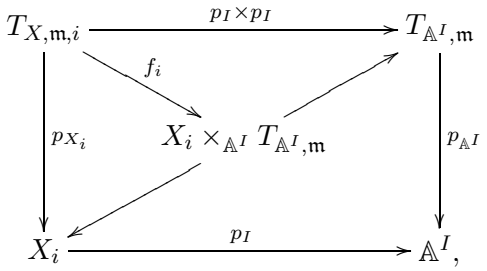
The following characterization of Hecke operators is actually discussed in more detail in §2.4.2. Denote by $\Delta^*_{\mathfrak{m}}$ the set of 2×2 matrices with coefficients in A which have no factor in common, and whose determinant is a unit times $\mathfrak{m}$. Then $\mathrm{GL}_2(A)$ acts from the right on $\Delta^*_{\mathfrak{m}}$. Let t_i for $i = 1, \ldots, \psi(\mathfrak{m})$ be a set of representatives for the cosets $\Delta^*_{\mathfrak{m}}/\mathrm{GL}_2(A)$. The matrices t_i act on Ω by fractional linear transformations, as usual. The action of $T_{\mathbb{A}^1,\mathfrak{m}}$ is given by $T_{\mathbb{A}^1,\mathfrak{m}}(x) = \cup_{i=1}^{\psi(\mathfrak{m})} j(t_i(z))$ where $z \in \Omega$ is any preimage of $x \in \mathbb{A}^1$ under j. Similarly, denote by $t_{n,i} = (t_{i_1}, \ldots, t_{i_n})$ for $i \in \{1, \ldots, \psi(\mathfrak{m})\}^n$ chosen representatives for the action of $T_{\mathbb{A}^n,\mathfrak{m}}$. Then the action of $T_{X,\mathfrak{m}}$ is given by $T_{X,\mathfrak{m}}(x) = \cup_{i \in J} j(t_{n,i}(z))$ for some subset $J \subset \{1, \ldots, \psi(\mathfrak{m})\}^n$ and for a preimage $z \in \Omega^n$ of $x \in X$ under the map $(j, \ldots, j) : \Omega^n \longrightarrow \mathbb{A}^n$.

Now if (2.1) holds for a generic $x \in X$, then it follows that the projection

$$p_I : J \longrightarrow \{1, \ldots, \psi(\mathfrak{m})\}^I$$

is surjective, from which in turn follows that (2.1) holds for all x.

So we suppose $x \in X$ is generic. Denote by $T_{X,\mathfrak{m},i} = T_{X,\mathfrak{m}} \cap (X_i \times X)$ the restriction of the source of the Hecke correspondence $T_{X,\mathfrak{m}}$ to the component X_i. Consider the following diagram



where the vertical arrows are projections onto the sources of the respective correspondences, and the horizontal arrows are projections onto the coordinates in I. There exists a canonical map f_i from $T_{X,\mathfrak{m},i}$ to the fibred product $X_i \times_{\mathbb{A}^I} T_{\mathbb{A}^I,\mathfrak{m}}$, which is generically finite, as $p_{X_i} : T_{X,\mathfrak{m},i} \to X_i$ is generically finite. Clearly $X_i \times_{\mathbb{A}^I} T_{\mathbb{A}^I,\mathfrak{m}}$ has the same dimension as $T_{X,\mathfrak{m}}$ and X, and it is irreducible, as we will show below. It follows that f_i is dominant.

Now let $x_I = p_I(x)$, and let $y_I \in T_{\mathbb{A}^I,\mathfrak{m}}(x_I)$. Then $(x, (x_I, y_I))$ is a generic point on the fibred product, hence has a preimage (x, y) under f_i. We see that $y \in T_{X,\mathfrak{m},i}(x) = T_{X,\mathfrak{m}}(x)$ and $p_I(y) = y_I$, so we have shown that (2.1) is surjective.

It remains to show that $X_i \times_{\mathbb{A}^I} T_{\mathbb{A}^I,\mathfrak{m}}$ is irreducible. This will follow if the function fields of X_i and $T_{\mathbb{A}^I,\mathfrak{m}} \cong (Y_0'(\mathfrak{m}))^I$ over $\mathbf{C}$ are linearly disjoint over the function field of $\mathbb{A}^I$ over $\mathbf{C}$. Recall from Proposition 1.3.3 that the modular curve $Y_2(\mathfrak{m})$ covers $Y_0(\mathfrak{m})$ and is Galois over $Y(1) = \mathbb{A}^1$ with Galois group

$$\mathrm{Gal}(Y_2(\mathfrak{m})/Y(1)) \cong \mathrm{PSL}_2(A/\mathfrak{m}A) \cong \prod_{\mathfrak{p}|\mathfrak{m}} \mathrm{PSL}_2(A/\mathfrak{p}A).$$

On the other hand, let L be an intermediate field $\mathbf{C}(\mathbb{A}^I) \subset L \subset \mathbf{C}(X_i)$ which is purely transcendental over $\mathbf{C}(\mathbb{A}^I)$ and for which $[\mathbf{C}(X_i) : L] \leq \deg(X_i) \leq \deg(X)$ is finite. One can take $L = \mathbf{C}(\mathbb{A}^J)$, where $J \supset I$ is chosen such that the projection $p_J : X \to \mathbb{A}^J$ is dominant and generically finite. Then $L \cap \mathbf{C}(Y_2(\mathfrak{m})^I) = \mathbf{C}(\mathbb{A}^I)$, and $\mathbf{C}(Y_2(\mathfrak{m})^I)$ is Galois over $\mathbf{C}(\mathbb{A}^I)$ (with group $\mathrm{PSL}_2(A/\mathfrak{m}A)^I$), so it follows from Galois theory (see e.g. [58, Theorem 5.6.1]) that L and $\mathbf{C}(Y_2(\mathfrak{m})^I)$ are linearly disjoint over $\mathbf{C}(\mathbb{A}^I)$. Denote by $L_\mathfrak{m}$ the field $L \otimes_{\mathbf{C}(\mathbb{A}^I)} \mathbf{C}(Y_2(\mathfrak{m})^I)$. Then we have

$$\begin{aligned} \mathbf{C}(X_i) \otimes_{\mathbf{C}(\mathbb{A}^I)} \mathbf{C}(T_{\mathbb{A}^I,\mathfrak{m}}) &\subset \mathbf{C}(X_i) \otimes_{\mathbf{C}(\mathbb{A}^I)} \mathbf{C}(Y_2(\mathfrak{m})^I) \\ &= \mathbf{C}(X_i) \otimes_L L \otimes_{\mathbf{C}(\mathbb{A}^I)} \mathbf{C}(Y_2(\mathfrak{m})^I) \\ &= \mathbf{C}(X_i) \otimes_L L_\mathfrak{m}. \end{aligned}$$

But now $L_\mathfrak{m}$ is Galois over L, with group $\mathrm{Gal}(L_\mathfrak{m}/L) \cong \mathrm{PSL}_2(A/\mathfrak{m}A)^I$. Moreover, as $|\mathfrak{p}| \geq |13|$ for all $\mathfrak{p}|\mathfrak{m}$, it follows that this group has no subgroup of index less that $|\mathfrak{p}| + 1$ (Corollary A.2.1). On the other hand, $[\mathbf{C}(X_i) : L] \leq \deg(X) < |\mathfrak{p}| + 1$, so $\mathbf{C}(X_i) \cap L_\mathfrak{m} = \mathbf{C}(\mathbb{A}^I)$. It follows again from Galois theory that $\mathbf{C}(X_i)$ and $L_\mathfrak{m}$ are linearly disjoint. Hence $\mathbf{C}(X_i) \otimes_L L_\mathfrak{m}$ and $\mathbf{C}(X_i) \otimes_{\mathbf{C}(\mathbb{A}^I)} \mathbf{C}(T_{\mathbb{A}^I,\mathfrak{m}})$ are fields, and $X_i \times_{\mathbb{A}^I} T_{\mathbb{A}^I,\mathfrak{m}}$ is irreducible, as required.

□

For the next two corollaries, we assume $X \subset \mathbb{A}^n$ is a variety, with irreducible components X_i, $i = 1, \ldots, r$, which are all of the same dimension. We assume further that $X \subset T_{\mathbb{A}^n,\mathfrak{m}}(X)$ for some square-free $\mathfrak{m} \in A$, composed of distinct primes $\mathfrak{p} \in A$, each of even degree and satisfying $|\mathfrak{p}| \geq \max(13, \deg X)$.

Corollary 2.3.2 *Suppose that the projection $p_1 : X_i \to \mathbb{A}^1$ onto the first coordinate is dominant for all $i = 1, \ldots, r$. Let $x_1 \in \mathbb{A}^1$ such that $x_1 \in T_{\mathbb{A}^1,\mathfrak{m}}(x_1)$. Let $X_{x_1} = X \cap (\{x_1\} \times \mathbb{A}^{n-1})$. Then*

$$X_{x_1} \subset T_{X,\mathfrak{m}}(X_{x_1}).$$

Proof. Let $x \in X_{x_1}$. Then setting $I = \{1\}$ in Theorem 2.1, we see that

$$p_1 : T_{X,\mathfrak{m}}(x) \longrightarrow T_{\mathbb{A}^1,\mathfrak{m}}(x_1)$$

is surjective. Let $y \in T_{X,\mathfrak{m}}(x)$ be a preimage of $x_1 \in T_{\mathbb{A}^1,\mathfrak{m}}(x_1)$. Then $y \in X_{x_1}$ and $x \in T_{X,\mathfrak{m}}(y)$, hence $x \in T_{X,\mathfrak{m}}(X_{x_1})$, as required.

□

Corollary 2.3.3 *Let $x \in X_i$. Then the Hecke orbit $T^\infty_{X,\mathfrak{m}}(x)$ is Zariski-dense in the Hecke orbit $T^\infty_{X,\mathfrak{m}}(X_i)$.*

Proof. Let $I \subset \{1, \ldots, n\}$ be such that $\#I = \dim(X)$ and the projection $p_I : X_i \to \mathbb{A}^I$ is dominant. From Theorem 2.1 we get a surjection

$$p_I : T^\infty_{X,\mathfrak{m}}(x) \longrightarrow T^\infty_{\mathbb{A}^I,\mathfrak{m}}(p_I(x)).$$

This last set is Zariski-dense in $\mathbb{A}^I$, as $T^\infty_{\mathbb{A}^I,\mathfrak{m}}(p_I(x)) = \prod_{j\in I} T^\infty_{\mathbb{A}^1,\mathfrak{m}}(x_j)$ is a product of infinite subsets of $\mathbb{A}^1$. As the projection $p_I : X \to \mathbb{A}^I$ is generically finite, it follows that $T^\infty_{X,\mathfrak{m}}(x)$ must be Zariski-dense on at least one component X_j of $T^\infty_{X,\mathfrak{m}}(X_i)$. But

$$T^\infty_{X,\mathfrak{m}}(x) = T^\infty_{X,\mathfrak{m}}\Big(T^\infty_{X,\mathfrak{m}}(x)\Big),$$

and it follows that $T^\infty_{X,\mathfrak{m}}(x)$ is Zariski dense on the whole Hecke orbit $T^\infty_{X,\mathfrak{m}}(X_j) = T^\infty_{X,\mathfrak{m}}(X_i)$.

□

Remark. As $T_\mathfrak{m}$ is defined over k, we may replace the word "irreducible" by "F-irreducible" everywhere in the preceding sections, for any field $F \supset k$ over which the relevant varieties are defined. In particular, it follows from Corollary 2.3.3 above, that if X is a variety defined over F, X_i is an F-irreducible component of X, and $x \in X_i$, then the Hecke orbit $T^\infty_{X,\mathfrak{m}}(x)$ is Zariski-dense on X_i.

2.4 Curves stabilized by Hecke operators

We are now ready to prove a fundamental result (Theorem 2.2 below): a characterization of the modular curves $Y_0'(N)$ in terms of Hecke operators.

Theorem 2.2 *Let $Y \subset \mathbb{A}^2$ be an irreducible algebraic curve, and suppose $Y \subset T_{\mathbb{A}^2,\mathfrak{m}}(Y)$ for some square-free $\mathfrak{m} \in A$, $|\mathfrak{m}| > 1$, composed of primes $\mathfrak{p} \in A$ of even degree satisfying $|\mathfrak{p}| \geq \max(13, \deg Y)$. Then $Y = Y_0'(N)$ for some $N \in A$.*

The proof will occupy the rest of this section.

2.4.1 Preimages in Ω^2

If $Y = \{x\} \times \mathbb{A}^1$ or $Y = \mathbb{A}^1 \times \{x\}$, then x is a CM point (as it is stabilized by $T_{\mathbb{A}^1,\mathfrak{m}}$), and so Y is modular. So we may assume that the projections $p_i : Y \to \mathbb{A}^1$ are dominant, and have degree $1 \leq d_i \leq \deg(Y)$, for $i = 1, 2$.

We consider the space Ω^2, on which $G := \mathrm{PGL}_2(k_\infty)^2$ acts. We also define the following groups: $S := \mathrm{PSL}_2(k_\infty)^2$, $\Gamma := \mathrm{PGL}_2(A)^2$, and $\Sigma := \mathrm{PSL}_2(A)^2$. The map $\pi = (j \times j) : \Omega^2 \to \mathbb{A}^2$ is a rigid analytic map, and is a quotient for the action of the discrete group Γ. Let $X \subset \Omega^2$ be an irreducible component of the rigid analytic variety $\pi^{-1}(Y)$. Then $\pi^{-1}(Y)$ is the Γ-orbit of X, which we write as $\pi^{-1}(Y) = \Gamma \cdot X$. Let G_X be the stabilizer of X under the action of G. We also define $S_X := G_X \cap S$, $\Gamma_X := G_X \cap \Gamma$, and $\Sigma_X := G_X \cap \Sigma$. Our aim is to investigate the structure of S_X, under the hypothesis that $Y \subset T_\mathfrak{m}(Y)$, and hence conclude that Y must be a modular curve.

So our whole approach is similar to that of Edixhoven [19], but with slightly different details, for example the action of G on Ω^2 is not transitive, the topology is ultrametric, and Lie theory works a bit differently in characteristic p, so we replace it by explicit calculations.

Just a word on notation: we use p_1, p_2, p_I etc. to denote projections between affine spaces, (e.g. $p_2 : \mathbb{A}^2 \to \mathbb{A}^1$ denotes projection onto the second coordinate),

or from Ω^2 to Ω. On the other hand, we use pr_1, pr_2 etc. to denote projections on the linear groups, so for example $pr_1 : G \to \mathrm{PGL}_2(k_\infty)$ denotes projection onto the first copy of G.

The next three lemmas hold for an arbitrary curve X (with non-constant projections).

Lemma 2.4.1 *The group G_X is a closed analytic subgroup of G.*

Proof. This is immediate, as G_X is the stabilizer of the closed set X under the continuous action of the analytic group G. □

Lemma 2.4.2 *The two projections from G_X to $PGL_2(k_\infty)$ are injective.*

Proof. Let $K = \ker(pr_2 : G_X \to \mathrm{PGL}_2(k_\infty))$. Then K is in fact the stabilizer of X in $\mathrm{PGL}_2(k_\infty) \times \{1\}$, and stabilizes $X_z = X \cap (\Omega \times \{z\})$, for any $z \in \Omega$. But X_z is discrete, hence any $g \in K$ which is small enough must fix every element of X_z (the action is continuous, if g is too small then it can't move an element of X_z far enough to reach any other point of X_z). But we may choose z in such a way that X_z contains a non-quadratic element, whose stabilizer is trivial, hence $g = 1$. It follows that K is discrete. Now $K \lhd \mathrm{PGL}_2(k_\infty) \times \{1\}$, which has no non-trivial discrete normal subgroups (Proposition A.2.3), thus $K = \{1\}$. The same holds for the other projection. □

Lemma 2.4.3 *$pr_i(\Gamma_X)$ has index at most d_i in $PGL_2(A)$.*

Proof. We factor the map π as follows:

$$\Omega \times \Omega \xrightarrow{\pi_1} \mathbb{A}^1 \times \Omega \xrightarrow{\pi_2} \mathbb{A}^1 \times \mathbb{A}^1$$

$$X \longrightarrow W \longrightarrow Y$$

Here $W = \pi_1(X)$ is an irreducible component of $Z = \pi_2^{-1}(Y) = \mathrm{PGL}_2(A) \cdot W$. Let S be the set of all y's in Y for which every (equivalently at least one) point of $\pi^{-1}(y)$ lies in more than one component of $\pi^{-1}(Y)$. Then S lies in the finite set consisting of the singular points of Y as well as those with at least one coordinate equal to 0.

Let $Y' = Y - S$, and let X' and W' be the corresponding preimages. Then X' has the property that for every $\gamma \in \Gamma$, either $\gamma(X') = X'$ or $X' \cap \gamma(X') = \emptyset$. The same holds for W' with respect to $\mathrm{PGL}_2(A)$. From this follows that the map $\pi : X' \to Y'$ is a quotient for the action of Γ_X, and $\pi_2 : W' \to Y'$ is a quotient for the action of $pr_2(\Gamma_X)$. It follows that $pr_2(\Gamma_X)$ is the stabilizer of W for the action of $\mathrm{PGL}_2(A)$, hence the irreducible components of Z correspond to the cosets $\mathrm{PGL}_2(A)/pr_2(\Gamma_X)$, so the index is the number of these components.

On the other hand, $Z = \pi_2^{-1}(Y)$ is the fibered product of the maps $p_2 : Y \to \mathbb{A}^1$ and $j : \Omega \to \mathbb{A}^1$, hence it has at most d_2 irreducible components. Again, the same holds for the other projection. □

2.4.2 The structure of S_X

Now we make use of the fact that $Y \subset T_{\mathfrak{m}}(Y)$.

Firstly, we need yet another description of the Hecke operators $T_{\mathbb{A}^1,\mathfrak{m}}$. For the following discussion of primitive matrices, see [5].

Let $\mathrm{Mat}(A)$ denote the set of 2×2 matrices over A. We say that $\alpha \in \mathrm{Mat}(A)$ is *primitive* if the four entries of α have no factor in common. We define

$$\Delta_{\mathfrak{m}} = \{\alpha \in \mathrm{Mat}(A) \mid \det(\alpha) = \mu\mathfrak{m} \text{ for some } \mu \in \mathbb{F}_q^*\},$$

$$\Delta_{\mathfrak{m}}^* = \{\alpha \in \Delta_{\mathfrak{m}} \mid \alpha \text{ is primitive}\}.$$

Now $\mathrm{GL}_2(A)$ acts on $\Delta_{\mathfrak{m}}^*$ by left and right multiplication. It is known that $\mathrm{GL}_2(A)$ acts left (respectively right) transitively on the right (respectively left) $\mathrm{GL}_2(A)$-cosets of $\Delta_{\mathfrak{m}}^*$, but we won't need this fact.

Choose representatives $t_i, i = 1, \ldots, \psi(\mathfrak{m})$ of the right cosets $\Delta_{\mathfrak{m}}^*/\mathrm{GL}_2(A)$. We may choose the t_i's to be the elements of the form

$$t_i = \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix},$$

where a_i and d_i are monic, with $a_i d_i = \mathfrak{m}$ and $|b_i| < |d_i|$. Let $I = \{1, \ldots, \psi(\mathfrak{m})\}$ denote our index set. The t_i's act on Ω as usual by fractional linear transformations.

The action of the Hecke operator $T_{\mathfrak{m}}$ on $\mathbb{A}^1$ is given by $T_{\mathfrak{m}}(x) = \{j(t_i(z)) \mid i \in I\}$, for any choice of $z \in j^{-1}(x)$. We let $t_{ij} := (t_i, t_j),\ i, j \in I$ be the corresponding representatives for the action of $T_{\mathbb{A}^2,\mathfrak{m}}$ on $\mathbb{A}^2$.

Now $T_{\mathbb{A}^2,\mathfrak{m}}(Y) = \{\pi(t_{ij}(X)) \mid i, j \in I\}$, and each $\pi(t_{ij}(X))$ is irreducible, so $Y \subset T_{\mathbb{A}^2,\mathfrak{m}}(Y)$ means that for a specific pair (i, j), we have $Y = \pi(t_{ij}(X))$, i.e. $t_{ij}(X) \subset \pi^{-1}(Y)$, so $\gamma_{ij} t_{ij} \in G_X$ for some $\gamma_{ij} \in \Gamma$.

So far we have only found one non-trivial element in G_X, it is time to find some more. Let $J = \{(i, j) \in I \times I \mid t_{ij}(X) \subset \pi^{-1}(Y)\}$. As above, every $(i, j) \in J$ gives us an element $\gamma_{ij} t_{ij} \in G_X$. Let $y \in Y$ and $x \in \pi^{-1}(y) \subset X$. Then the induced Hecke operator on Y is given by $T_{Y,\mathfrak{m}}(y) = \{\pi(t_{ij}(x)) \mid (i, j) \in J)\}$.

From Theorem 2.1 we know that the projection onto the first factor

$$p_1 : T_{Y,\mathfrak{m}}(y) \to T_{\mathbb{A}^1,\mathfrak{m}}(y_1)$$

is surjective. It follows that $p_1 : J \to I$ is surjective. This means that for every $i \in I$, $H_1 := pr_1(G_X)$ contains $g_i = \gamma_i t_i$ for some $\gamma_i \in \mathrm{PGL}_2(A)$. We want to show that H_1 is large, in particular, we will show that H_1 contains $\mathrm{PSL}_2(k_\infty)$, so $pr_1(S_X) = \mathrm{PSL}_2(k_\infty)$.

From Lemma 2.4.3 follows that $\mathrm{PGL}_2(A) \cap H_1$ has finite index in $\mathrm{PGL}_2(A)$. Let R be a finite set of representatives of $\mathrm{PGL}_2(A)/(\mathrm{PGL}_2(A) \cap H_1)$. $\mathrm{GL}_2(A)$ acts from the right on the set of left cosets $\mathrm{GL}_2(A)\backslash\Delta_{\mathfrak{m}}^*$. We claim that for any string $i_1 \ldots i_n$ of elements in I, and any $a \in \mathrm{GL}_2(A)$, we can construct an element of the form $\gamma t_{i_n} t_{i_{n-1}} \cdots t_{i_1} a$ in H_1, for some $\gamma \in R$ depending on the string and on a. Indeed, by induction we need only show that, given $a_1 \in \mathrm{GL}_2(A)$ and $i_1 \in I$, we can construct an element of the form $\gamma_1 t_{i_1} a_1$ in H_1. This element

is constructed as follows. Let a_1 act from the right on the coset $\mathrm{GL}_2(A) \cdot t_{i_1}$, to obtain another coset $\mathrm{GL}_2(A) \cdot t_{i_1} a = \mathrm{GL}_2(A) \cdot t_j$. Then $t_{i_1} a = \gamma'_j t_j$, and mulitplying on the left with a suitable element γ_1 of R gives $\gamma_1 t_{i_1} a = \gamma_j t_j = g_j \in H_1$. This proves the claim.

Multiplying by a suitable power of the scalar $\mathfrak{m}$, we see that for any $x \in A[1/\mathfrak{m}]$ and any $a \in \mathrm{GL}_2(A)$, there exists $\gamma_{x,a} \in R$ such that $\gamma_{x,a} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} a \in H_1$.

The group $\mathrm{PSL}_2(A[1/\mathfrak{m}])$ is generated by $\mathrm{PSL}_2(A)$ and elements of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ (see Proposition A.3.1). Then for any $g \in \mathrm{PSL}_2(A[1/\mathfrak{m}])$, we can construct an element $\gamma_g g \in H_1$, for some $\gamma_g \in R$, obtained by multiplying together suitable elements of the form $\gamma_{x,a} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} a \in H_1$. It follows that $H_1 \cap \mathrm{PSL}_2(A[1/\mathfrak{m}])$ has finite index in $\mathrm{PSL}_2(A[1/\mathfrak{m}])$.

Now we make a brief detour.

Lemma 2.4.4 *G_X is not discrete*

Proof. Assume that G_X is discrete. Choose a non-quadratic point $x = (x_1, x_2)$ in X. Then its orbit $G_X \cdot x$ is discrete in X, so $\pi(G_X \cdot x)$ is discrete in Y, as $\Gamma_X \subset G_X$ and $\pi : X \to Y$ is a quotient by Γ_X. Next, $p_1(\pi(G_X \cdot x))$ is discrete in $\mathbb{A}^1$ (as $p_1 : Y \to \mathbb{A}^1$ is finite), and thus $j^{-1}\Big(p_1(\pi(G_X \cdot x))\Big)$ is discrete in Ω. But from above we see that this set contains the orbit $\Big(H_1 \cap \mathrm{PSL}_2(A[1/\mathfrak{m}])\Big) \cdot x_1$, which is not discrete. This is a contradiction.

□

So we see that G_X is a closed analytic subgroup of G, but is not discrete. Moreover, the projections $pr_i : S_X \to \mathrm{PSL}_2(k_\infty)$ are dominant and injective, so it must follow that S_X is itself an analytic group of the same dimension as $\mathrm{PSL}_2(k_\infty)$ (namely 3). It follows that $pr_1 : G_X \to \mathrm{PGL}_2(k_\infty)$ must be surjective on some open neighborhood of the identity, and hence $H_1 = pr_1(G_X)$ has an interior point. It follows that H_1 is closed in $\mathrm{PGL}_2(k_\infty)$.

Now, $\mathrm{PSL}_2(A[1/\mathfrak{m}])$ is dense in $\mathrm{PSL}_2(k_\infty)$, so it follows (via Proposition A.3.2) that $H_1 \cap \mathrm{PSL}_2(k_\infty)$ has finite index in $\mathrm{PSL}_2(k_\infty)$. From Proposition A.2.4 it now follows that H_1 contains $\mathrm{PSL}_2(k_\infty)$.

Similarly, $H_2 = pr_2(G_X) \subset \mathrm{PGL}_2(k_\infty)$ also contains $\mathrm{PSL}_2(k_\infty)$.

It follows from Goursat's lemma (Proposition A.3.3) that G_X is of the form

$$G_X = \{(g, \rho(g)) \mid g \in H_1\}$$

for some isomorphism $\rho : H_1 \to H_2 \subset \mathrm{PGL}_2(k_\infty)$. From Corollary A.2.6 now follows that ρ restricts to an automorphism of $\mathrm{PSL}_2(k_\infty)$, and so

$$S_X = \{(g, \rho(g)) \mid g \in \mathrm{PSL}_2(k_\infty)\}$$

for some $\rho \in \mathrm{Aut}(\mathrm{PSL}_2(k_\infty))$.

Every automorphism of $\mathrm{PSL}_2(k_\infty)$ is of the form $g \mapsto h g^\sigma h^{-1}$ for some $h \in \mathrm{PGL}_2(k_\infty)$ and $\sigma \in \mathrm{Aut}(k_\infty)$ (Proposition A.3.4).

2.4.3 Completing the proof of Theorem 2.2

By the definition of Σ_X and the structure of S_X, we see that $h \cdot pr_1(\Sigma_X)^\sigma \cdot h^{-1} \subset \mathrm{PSL}_2(A)$. On the other hand, Lemma 2.4.3 tells us that $pr_i(\Sigma_X)$ has finite index in $\mathrm{PSL}_2(A)$. This in turn severely restricts h and σ:

Proposition 2.4.5 *Let G be a subgroup of finite index in $PSL_2(A)$, and suppose that $hG^\sigma h^{-1} \subset PGL_2(k)$, for some $h \in PGL_2(k_\infty)$ and $\sigma \in Aut(k_\infty)$. Then $h \in PGL_2(k)$ and $\sigma(T) = uT + v$ for some $u \in \mathbb{F}_q^*$, $v \in \mathbb{F}_q$, and $\sigma(\mathbb{F}_q) = \mathbb{F}_q$.*

Proof. Firstly, let $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and let $r = \det(h)$. As k_∞^*/k_∞^{*2} may be represented by $\{1, \alpha, T, \alpha T\}$, for some non-square $\alpha \in \mathbb{F}_q$, we may assume that $r \in k$.

Denote by $B_1 = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ and $B_2 = \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$ the two Borel subgroups of $\mathrm{PSL}_2(A)$. They are infinite, and G has finite index in $\mathrm{PSL}_2(A)$, so it follows from Lemma A.3.5 that $G \cap B_1$ and $G \cap B_2$ are of finite index in B_1 and B_2, respectively. It follows that the subgroups $A_1^+ = \{x \in A^+ \mid \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in G\}$ and $A_2^+ = \{x \in A^+ \mid \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \in G\}$ have finite index in A^+, hence their intersection $A_0^+ = A_1^+ \cap A_2^+$ also has finite index in A^+.

Now for every $x \in A_0^+$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^\sigma \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 - \frac{ac}{r}\sigma(x) & \frac{a^2}{r}\sigma(x) \\ -\frac{c^2}{r}\sigma(x) & 1 + \frac{ac}{r}\sigma(x) \end{pmatrix} \in \mathrm{PGL}_2(k).$$

This means that $\exists \lambda \in k_\infty$ such that

$$\lambda\Big(1 - \frac{ac}{r}\sigma(x)\Big),\ \lambda\frac{a^2}{r}\sigma(x),\ \lambda\frac{c^2}{r}\sigma(x),\ \lambda\Big(1 + \frac{ac}{r}\sigma(x)\Big) \in k.$$

Thus we get $\lambda(1 - \frac{ac}{r}\sigma(x)) + \lambda(1 + \frac{ac}{r}\sigma(x)) = 2\lambda \in k$, and it follows that

$$ac\sigma(x),\ a^2\sigma(x),\ c^2\sigma(x) \in k. \tag{2.2}$$

Likewise, from $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}^\sigma \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in \mathrm{PGL}_2(k)$ follows

$$bd\sigma(x),\ b^2\sigma(x),\ d^2\sigma(x) \in k. \tag{2.3}$$

Furthermore, we get

$$c_0 = \frac{a}{c} = \frac{ac\sigma(x)}{c^2\sigma(x)} \in k, \quad \text{and} \quad d_0 = \frac{b}{d} = \frac{bd\sigma(x)}{d^2\sigma(x)} \in k. \tag{2.4}$$

Now from $0 \neq r = ad - bc = (c_0 - d_0)cd \in k$ we get

$$cd \in k \quad \text{and} \quad ab \in k. \tag{2.5}$$

It follows in turn that

$$\frac{a}{b}\sigma(x) = \frac{a^2\sigma(x)}{ab} \in k \quad \text{and} \quad \frac{c}{d}\sigma(x) = \frac{c^2\sigma(x)}{cd} \in k. \tag{2.6}$$

Next we compute

$$\frac{c^2}{d^2} = \frac{c_0 c \cdot c\sigma(x)}{d_0 d \cdot d\sigma(x)} \cdot \frac{d_0}{c_0} = \frac{ac\sigma(x)}{bd\sigma(x)} \cdot \frac{d_0}{c_0} \in k,$$

which, combined with (2.6) gives us

$$\sigma(x)^2 \in k \qquad \forall x \in A_0^+. \tag{2.7}$$

Now as A_0^+ has finite index in A^+ it follows that we must have a pair $x_1 \neq x_2 \in A_0^+$ such that $y = x_1^2 - x_2^2 \in A_0^+$. We have $\sigma(y) = \sigma(x_1)^2 - \sigma(x_2)^2 \in k$. Substituting this y in for x in (2.6) shows that in fact

$$\frac{a}{b} \in k,\ \frac{c}{d} \in k \quad \text{and} \quad \frac{a}{d} = \frac{a}{b}\frac{b}{d} \in k. \tag{2.8}$$

It follows firstly that h is defined over k up to a scalar, so $h \in \mathrm{PGL}_2(k)$, and secondly that $\sigma(x) \in k$ for all $x \in A_0^+$. As this group has finite index in A^+, it follows from Lemma A.3.6 that A_0^+ generates all of k, so $\sigma(x) \in k$ for all $x \in k$. It remains to characterize those automorphisms σ for which $\sigma(k) \subset k$.

Let $R = \mathbb{F}_q[[1/T]] = \{x \in k_\infty \mid |x| \leq 1\}$. Then R is the unique valuation ring of k_∞. It is characterized by the property: $x \in R$ or $x^{-1} \in R$ for all $x \in k_\infty$ and $R \neq k_\infty$. This property must be preserved by σ, so $\sigma(R) \subset R$. So σ also preserves $k \cap R = A$, and the only automorphisms that send polynomials to polynomials are of the form $\sigma(T) = uT + v$, for some $u \in \mathbb{F}_q^*,\ v \in \mathbb{F}_q$, and $\sigma(\mathbb{F}_q) = \mathbb{F}_q$.

□

We now conclude the proof of Theorem 2.2.

Proof of Theorem 2.2. From the above Proposition follows that

$$S_X = \{(g, hg^\sigma h^{-1}) \mid g \in \mathrm{PSL}_2(k_\infty)\},$$

where $h \in \mathrm{PGL}_2(k)$, $\sigma(T) = uT + v$ and $\sigma(\mathbb{F}_q) = \mathbb{F}_q$. There is some $t \in \mathbb{N}$ such that $\sigma(\alpha) = \alpha^{p^t}$ for all $\alpha \in \mathbb{F}_q$, as $\sigma|_{\mathbb{F}_q} \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

We let $f = (T^q - T)^{q-1}$, then $\sigma(f) = f$. Let $F = \mathbb{F}_p((1/f))$. This is a complete subfield of k_∞ and σ acts trivially on F.

Now fix some non-square $\alpha \in \mathbb{F}_q$, and define the set

$$P = \{z \in \Omega \mid z^2 = \alpha e,\ 0 \neq e \in F\}.$$

This is an uncountable subset of $\Omega = \mathbf{C} \smallsetminus k_\infty$, as $\sqrt{\alpha} \notin k_\infty$.

Next, we notice that $\sigma(\alpha e) = \alpha^{p^t} e = \beta^2 \alpha e$, where we set $\beta = \alpha^{(p^t-1)/2} \in \mathbb{F}_q^*$ (remember that p is odd).

Let $z_1 = \sqrt{\alpha e} \in P$ and

$$S_1 = \mathrm{Stab}_{\mathrm{PSL}_2(F)}(z_1) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a = d,\ b = c\alpha e,\ ad - bc = 1 \right\} / \{\pm 1\},$$

which is a one-dimensional Lie-group over F.

Now let $z_2 \in \Omega$ such that $(z_1, z_2) \in X$, and consider the "S_1-orbit" of (z_1, z_2):

$$\{(g(z_1), hg^\sigma h^{-1}(z_2)) \mid g \in S_1\} \subset X \cap (\{z_1\} \times \Omega).$$

This set is discrete, but the group S_1 is not, hence there exists some non-trivial $g \in S_1$ such that g fixes z_1 (by definition of S_1) and $hg^\sigma h^{-1}$ fixes z_2. But g^σ fixes the point $z_1^\sigma := \sqrt{\sigma(\alpha e)} = \beta z_1$, so we see that $hg^\sigma h^{-1}$ fixes both z_2 and $h(\beta z_1) = h'(z_1)$, where we have written $h' = h \circ \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{PGL}_2(k)$. However, any non-trivial element of $\mathrm{PGL}_2(k_\infty)$ fixes at most two points of Ω, namely a conjugate pair of quadratic points. So z_2 and $h'(z_1)$ are conjugate. So we get either $z_2 = h'(z_1)$ or $z_2 = h'(-z_1)$. The second equality follows from the fact that the conjugate of z_1 is $-z_1$, and the action of h' is compatible with conjugation (if x, y are conjugates, then $\{x, y\}$ are the fixed points of some $g \in \mathrm{PGL}_2(k_\infty)$, hence $\{h(x), h(y)\}$ are the fixed points of hgh^{-1}, hence are again conjugate). Lastly, as $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{PGL}_2(A)$, it follows that $j(z_1) = j(-z_1)$, so we get either $(j(z_1), j(h'(z_1)))$ or $(j(-z_1), j(h'(-z_1)))$ on the curve Y in $\mathbb{A}^2(\mathbf{C})$.

Let $a \in A$ be such that the entries of the matrix ah' are in A and have no factor in common, and let $N = \det(ah')$. Then the curve $\{(j(z), j(h(z))) \mid z \in \Omega\}$ in $\mathbb{A}^2(\mathbf{C})$ is just $Y_0'(N)(\mathbf{C})$ (recall §1.3.4).

We see that the points $(j(z_1), j(h'(z_1)))$ and $(j(-z_1), j(h'(-z_1)))$ also lie on $Y_0'(N)$ (which is independent of z_1). We get such a point for each $z_1 \in P$, and P is uncountable whereas the fibres of j are countable, so it follows that $Y(\mathbf{C}) \cap Y_0'(N)(\mathbf{C})$ is infinite, hence $Y = Y_0'(N)$. This completes the proof of Theorem 2.2.

□

Corollary 2.4.6 *Let $Y \subset \mathbb{A}^n$ be an irreducible algebraic curve, and suppose that $Y \subset T_{\mathbb{A}^n,\mathfrak{m}}(Y)$ for some square-free $\mathfrak{m} \in A$, composed of primes $\mathfrak{p}$ of even degree and satisfying $|\mathfrak{p}| \geq \max(13, \deg Y)$. Then Y is a modular curve.*

Proof. Up to some permutation of coordinates, we have

$$Y = Y' \times \{y\},$$

where $y \in \mathbb{A}^{n-m}$ is a point and $Y' \subset \mathbb{A}^m$ is a curve for which all the projections $p_i : Y' \to \mathbb{A}^1$ are dominant, for some $1 \leq m \leq n$. Then Y' and y are stabilized by the Hecke operators $T_{\mathbb{A}^m,\mathfrak{m}}$ and $T_{\mathbb{A}^{n-m},\mathfrak{m}}$, respectively, from which follows that y is a CM point. It remains to show that Y' is a pure modular curve. If $m = 1$ then $Y' = \mathbb{A}^1$, which is modular by definition. So we suppose that $m \geq 2$ and consider the projections $Y_i = p_{1,i}(Y') \subset \mathbb{A}^2$, for all $i = 2, \ldots m$. Now each Y_i is stabilized by $T_{\mathbb{A}^2,\mathfrak{m}}$, so from Theorem 2.2 follows that each $Y_i = Y'(N_i)$ for some $N_i \in A$. Our result now follows from Proposition 1.3.4.

□

2.5 Varieties stabilized by Hecke operators

In this section we generalize Theorem 2.2 to subvarieties of higher dimensions.

Theorem 2.3 *Let F be a field lying between k and $\mathbf{C}$. Let $X \subset \mathbb{A}^n$ be an F-irreducible variety, containing a CM point $x \in X(\mathbf{C})$. Suppose that $X \subset T_{\mathbb{A}^n,\mathfrak{m}}(X)$ where $\mathfrak{m} \in A$ is monic and square-free, composed of primes $\mathfrak{p}$ of even degree and satisfying $|\mathfrak{p}| \geq \max(13, \deg X)$. Then X is a modular variety.*

Proof. We know from Corollary 2.3.3, and the subsequent Remark, that the Hecke orbit $S' = T^{\infty}_{X,\mathfrak{m}}(x)$ is Zariski-dense in X. In particular, it is Zariski-dense on every (geometrically) irreducible component, and we now replace X by one of these components, so we assume that X is geometrically irreducible. We let $S = S' \cap X(\mathbf{C})$, and let x denote a point of S. All the points in S are CM points, isogenous coordinate-wise to x. As CM points are defined over k^{sep}, so is X. So we may assume that X is defined over a finite Galois extension (again denoted F) of k.

Step 1. Write $x = (x_1, \ldots, x_n)$, and let $\mathcal{O}_i = \mathrm{End}(x_i)$ be an order of conductor f_i in the imaginary quadratic field K_i, for each $i = 1, \ldots, n$. Set $K = K_1 \cdots K_n$ and $f = f_1 \cdots f_n$, and define

$$\mathcal{P} = \{l \in A \mid \text{monic prime, of even degree, split completely in } FK \text{ and } l \nmid f\mathfrak{m}\}.$$

This set has density at least $1/2[FK : k]$ (Čebotarev). In particular, it is infinite.

Let $x' = (x'_1, \ldots, x'_n) \in S$, then each $\mathcal{O}'_i = \mathrm{End}(x'_i)$ is an order of conductor f'_i in K_i (the CM fields are the same, as x_i and x'_i are isogenous). Furthermore, all the prime factors of f'_i are factors of f_i and of $\mathfrak{m}$. It follows that every $l \in \mathcal{P}$ splits also in $\mathcal{O}'_i$. Set $M = K(x'_1, \ldots, x'_n)$ and let $\mathfrak{L}$ be a prime of FM lying over l. Denote by $\mathfrak{L}_M$, $\mathfrak{L}_{FK}$, $\mathfrak{L}_i$ and $\mathfrak{l}_i$ the restriction of $\mathfrak{L}$ to the fields M, FK, $K_i(x'_i)$ and K_i, respectively. From Theorem 1.6 follows that l is unramified in M, hence also in FM. Let $\sigma = (\mathfrak{L}_{FM}, FM/k)$ be the Frobenius element. Set $\sigma_i = \sigma|_{K_i(x'_i)} = (\mathfrak{L}_i, K_i(x'_i)/k)$. As l splits in K_i, we have in fact $\sigma_i = (\mathfrak{L}_i, K_i(x'_i)/K_i)$. Now CM theory (Theorem 1.6) tells us that there is a cyclic isogeny $x'_i \to \sigma_i(x'_i)$ of degree l. Now σ fixes F (as l splits completely in F), and we have coordinate-wise cyclic isogenies of degree l from x' to $\sigma(x')$, from which follows that we have

$$x' \in X \cap T_{\mathbb{A}^n,l}(X^{\sigma}) = X \cap T_{\mathbb{A}^n,l}(X).$$

This holds for every x' in the Zariski-dense set S, so it follows that

$$X \subset T_{\mathbb{A}^n,l}(X). \tag{2.9}$$

Moreover, (2.9) holds for every $l \in \mathcal{P}$.

Step 2. Now we use induction on $d = \dim(X)$. If $d = 1$ then the result already follows from Corollary 2.4.6. Now suppose $d \geq 2$, and that the result is already known for lower dimensions.

We may assume without loss of generality that the projection $p_1 : X \to \mathbb{A}^1$ is dominant. Now we may choose an infinite subset $\{x^1, x^2, \ldots, \} \subset S$ of points, written $x^j = (x_1^j, \ldots, x_n^j)$, such that the first coordinates x_1^j are distinct, for $j \in \mathbb{N}$. For each j we may find $l_j \in \mathcal{P}$ such that $x_1^j \in T_{\mathbb{A}^1, l_j}(x_1^j)$ and $|l_j| \geq \max(13, \deg X)$. In fact, $\mathcal{P}$ contains infinitely many such primes, namely those which are split principal in $\mathrm{End}(x_i^j)$ (and of even degree) for each $i = 1, \ldots, n$ (recall §2.2).

For each $j \in \mathbb{N}$ we consider the "slice"

$$X_j = X \cap (\{x_1^j\} \times \mathbb{A}^{n-1}),$$

which satisfies $X_j \subset T_{X,l_j}(X_j)$ (Corollary 2.3.2), $\dim(X_j) = d - 1$ and $x_j \in X_j$. Let X_j' be an irreducible component of X_j containing x^j. Then the Hecke orbit $T_{X_j,l_j}^{\infty}(x_j)$ is Zariski-dense in X_j' (and on the other irreducible components in the same Hecke orbit). As in Step 1 above, we can find infinitely many primes $\mathfrak{p}$ such that $T_{\mathbb{A}^n,\mathfrak{p}}$ stabilizes X_j', so from the induction hypothesis follows that X_j' is modular.

Now $\deg(X_j') \leq \deg(X)$, and there are only finitely many types of modular varieties of bounded degree (Proposition 2.1.7), so it follows that we have an infinite subset $I \subset \mathbb{N}$ and some $\pi \in S_n$ such that, after permutation of coordinates by π,

$$X_j' = Y \times \{y_j\} \quad \forall j \in I,$$

where $Y \subset \mathbb{A}^{n-m}$ is a fixed modular variety, and $y_j \in \mathbb{A}^m$ is a CM point, for some $m \geq 1$. The Zariski-closure of the set $\{X_j' \mid j \in I\}$ is closed in X and has dimension at least $\dim(X_j') + 1 = \dim(X)$, hence is equal to X.

Consider the intersection $X \cap (Y \times \mathbb{A}^m)$. It is Zariski-closed and contains all the X_j', hence contains X. Consider the projection onto the last m coordinates $p : X \to \mathbb{A}^m$. The fibres of this projection contain Y, hence have dimension at least $d - 1$. It follows that the image $Y' \subset \mathbb{A}^m$ of the projection, which is irreducible, has dimension at most 1 and contains the infinite set of points $y_j,\ j \in I$. Hence Y' is an irreducible curve in $\mathbb{A}^m$. We get $X \subset Y \times Y'$ and $\dim(X) = \dim(Y \times Y')$, so it follows that $X = Y \times Y'$. Moreover, Y' is stabilized by the Hecke operators $T_{\mathbb{A}^m,l}$ for all $l \in \mathcal{P}$, hence is itself modular. It follows that X is modular, which is what we set out to prove.

□

Lastly, we remark that all of the results in this chapter also hold in characteristic 0 (after some elementary translations), except possibly for some details in the proof of Theorem 2.2. This doesn't matter, as the characteristic 0 version of Theorem 2.2 has already been proved by Edixhoven [19]. In fact, his proof inspired the proof of the characteristic p version presented here.

Chapter 3

Heights of CM points

This can be considered the main chapter of this thesis. In it we prove an analogue of the André-Oort conjecture for products of Drinfeld modular curves.

3.1 Class numbers

The aim of this first section is to derive a lower bound for the class number of an order in an imaginary quadratic function field. Our standard reference to facts about function fields is [65].

3.1.1 Zeta functions

Let F be a function field of genus g with $\mathbb{F}_q$ as exact field of constants. Let $P \in \mathbb{P}_F$ be a place of F with residue field $\tilde{F}_P$. The *degree* of P is $\deg(P) = [\tilde{F}_P : \mathbb{F}_q]$. Let $D \in \mathrm{Div}(F)$ be a divisor, $D = \sum_{P \in \mathbb{P}_F} n_P \cdot P$. Then the degree of D is defined as $\deg(D) = \sum_{P \in \mathbb{P}_F} n_P \deg(P)$. We note that principal divisors all have degree zero (a function has the same number of zeros and poles), and we define the *class group* of F to be the group of degree zero divisors modulo principal divisors, $\mathrm{Pic}(F) = \mathrm{Div}^0(F)/F^*$. We let $h = \#\mathrm{Pic}(F)$ denote the class number, which is finite. The purpose of this subsection is to estimate h.

Denote by A_n the number of effective divisors of degree n of F, for $n \geq 0$.

Lemma 3.1.1 *Suppose $n > 2g - 2$. Then*

$$A_n = \frac{h}{q-1}(q^{n+1-g} - 1).$$

Definition 3.1.2 *The* zeta function *of F is defined by the power series*

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n \ \in \mathbb{C}[[t]].$$

The zeta function has many important properties, of which we list some:

Theorem 3.1

1. *$Z(t)$ is a rational function, $Z(t) = \frac{L(t)}{(1-t)(1-qt)}$, where $L(t) \in \mathbb{Z}[t]$ is a polynomial of degree $2g$.*

2. *The class number of F is given by $h = L(1)$.*

3. **(Euler product)** *For $|t| < q^{-1}$ we have*

$$Z(t) = \prod_{P \in \mathbb{P}_F} (1 - t^{\deg(P)})^{-1}.$$

4. **(Functional equation)** *The zeta function satisfies*

$$Z(t) = q^{g-1} t^{2g-2} Z(1/qt).$$

5. **(Riemann Hypothesis)** *Write $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$ in $\mathbb{C}[t]$. Then the numbers α_i are algebraic integers and satisfy $|\alpha_i| = \sqrt{q}$ for all $i = 1, \ldots, 2g$.*

The places of degree one of F are called *rational places*, and correspond to the $\mathbb{F}_q$-rational points of the curve $\mathcal{X}$ corresponding to F. Counting them is important, and has applications in coding theory. The number of rational places is A_1. We have the following important corollary of the Riemann Hypothesis (Theorem 3.1(5) above).

Corollary 3.1.3 (Hasse-Weil bound)

$$|A_1 - (q+1)| \leq 2g\sqrt{q}.$$

Now we want to estimate h. Using Theorem 3.1(2) we get $h = \prod_{i=1}^{2g}(\alpha_i - 1)$, and from the Riemann hypothesis

$$|\sqrt{q} - 1|^{2g} \leq h \leq |\sqrt{q} + 1|^{2g}. \tag{3.1}$$

Unfortunately, the lower bound is only useful if $q \geq 5$. For general q we have the following bound, which was shown to me by Henning Stichtenoth.

Proposition 3.1.4 *If $g \geq 1$ then*

$$h \geq \frac{(q-1)(q^{2g} - 2gq^g + 1)}{2g(q^{g+1} - 1)}.$$

Note that this also gives us a lower bound of order q^g, like (3.1), but is valid for all q.

Proof. We consider the constant field extension $F' = \mathbb{F}_{q^{2g}}F$ of F of degree $2g$. The exact field of constants of F' is $\mathbb{F}_{q^{2g}}$. Let N' denote the number of rational (that is, $\mathbb{F}_{q^{2g}}$-rational) places of F'. The Hasse-Weil bound gives us

$$N' \geq q^{2g} - 2gq^g + 1.$$

Let $Q \in \mathbb{P}_{F'}$ be one such rational place of F', and $P \in \mathbb{P}_F$ the unique place of F lying under Q. As Q has degree one we get $\tilde{F'}_Q = \mathbb{F}_{q^{2g}}$, and hence

$$2g = [\mathbb{F}_{q^{2g}} : \mathbb{F}_q] = [\tilde{F'}_Q : \mathbb{F}_q] = [\tilde{F'}_Q : \tilde{F}_P][\tilde{F}_P : \mathbb{F}_q] = f(Q|P)\deg(P),$$

and so $\deg(P)$ divides $2g$. It follows that $\frac{2g}{\deg(P)} \cdot P$ is an effective divisor of degree $2g$ of F. As there are at most $2g$ places Q above P, we see that in this way we have constructed at least $N'/2g$ effective divisors of degree $2g$ of F. On the other hand, Lemma 3.1.1 tells us that there are exactly

$$\frac{h}{q-1}(q^{2g+1-g} - 1)$$

such places, so we get

$$\frac{h}{q-1}(q^{g+1} - 1) \geq \frac{N'}{2g} \geq \frac{q^{2g} - 2gq^g + 1}{2g},$$

from which the result follows.

□

3.1.2 Class numbers of orders

We assume that q is odd in the rest of this chapter. We now let $F = K = k(\sqrt{D})$ be an imaginary quadratic extension of $k = \mathbb{F}_q(T)$, where $D \in A$ is square-free. Then the genus of K is given by

$$g = \begin{cases} (\deg(D) - 1)/2 & \text{if } \deg(D) \text{ is odd} \\ (\deg(D) - 2)/2 & \text{if } \deg(D) \text{ is even.} \end{cases}$$

Let $\mathfrak{p} \in A$ be a prime of k. Then we define the *Kronecker symbol* χ as follows.

$$\chi(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits in } K/k \\ -1 & \text{if } \mathfrak{p} \text{ is inert in } K/k \\ 0 & \text{if } \mathfrak{p} \text{ is ramified in } K/k \end{cases}$$

Then, as in the classical case, we have (see for example [59, Prop. 17.9])

Theorem 3.2 *Let $\mathcal{O}$ be an order of conductor f in K, and let $h = h_K$ denote the class number of K. Then*

$$\#Pic(\mathcal{O}) = \frac{h}{[\mathcal{O}_K^* : \mathcal{O}^*]}|f| \prod_{\mathfrak{p}|f} \left(1 - \frac{\chi(\mathfrak{p})}{|\mathfrak{p}|}\right).$$

Combining this with Proposition 3.1.4, we can bound $\#\mathrm{Pic}(\mathcal{O})$ from below:

$$\begin{aligned}
\#\mathrm{Pic}(\mathcal{O}) &= \frac{h}{[\mathcal{O}_K^* : \mathcal{O}^*]}|f|\prod_{\mathfrak{p}|f}\left(1-\frac{\chi(\mathfrak{p})}{|\mathfrak{p}|}\right) \\
&\geq \frac{h}{[\mathcal{O}_K^* : \mathcal{O}^*]}|f|\prod_{\mathfrak{p}|f}\left(1-\frac{1}{|\mathfrak{p}|}\right) \\
&\geq C_1 h|f|/\log|f| \\
&\geq C'_\varepsilon q^{g(1-\varepsilon)}|f|^{1-\varepsilon} \\
&\geq C_\varepsilon |Df^2|^{\frac{1}{2}-\varepsilon}, \qquad (3.2)
\end{aligned}$$

for every $\varepsilon > 0$ and positive constants C_1, C_ε and C'_ε.

Similarly, using (3.1), we get the upper bound

$$\#\mathrm{Pic}(\mathcal{O}) \leq B_\varepsilon |Df^2|^{\frac{1}{2}+\varepsilon}. \qquad (3.3)$$

3.2 Estimating the j-invariant

In this section we estimate the j-invariant using analytic methods, following the first part of [10]. We point out that later parts of that paper (the part concerning supersingular reduction) has been shown to contain errors, but we will only use results from the first (and supposedly correct) part.

3.2.1 Uniformizations

We first need some definitions. Let $i \in \mathbb{N}$ and define

$$[i] = T^{q^i} - T \ \in A,$$

$$D_i = [i][i-1]^q \cdots [1]^{q^{i-1}} = \prod_{j=0}^{i-1}(T^{q^i} - T^{q^j}),$$

$$\bar{\pi} = (-[1])^{1/(q-1)}\prod_{i=1}^{\infty}\left(1-\frac{[i]}{[i+1]}\right) = (T-T^q)^{1/(q-1)}\prod_{i=1}^{\infty}\left(1-\frac{T^{q^i}-T}{T^{q^{i+1}}-T}\right) \in \mathbf{C}.$$

The element $\bar{\pi}$, which is determined up to the choice of a $(q-1)$st root of $-[1]$, plays the same role in characteristic p as does the constant $\pi = 3.14159\ldots$ in characteristic zero. It is known to be transcendental over k. See [31, Chapter 3] for more details.

We have

$$|\bar{\pi}| = q^{q/(q-1)}.$$

We recall from Chapter 1 the exponential function e_Λ associated to a lattice Λ. We will only need it for the rank 1 lattice A, in which case it is called the *Carlitz exponential*, which was first studied by Carlitz [11],

$$e_A(z) = z\prod_{0\neq a\in A}\left(1-\frac{z}{a}\right).$$

We have

$$e_{\bar{\pi}A}(z) = \bar{\pi} e_A(z/\bar{\pi}) = \sum_{i=0}^{\infty} D_i^{-1} z^{q^i}.$$

The lattice $\bar{\pi}A$ gives rise to the *Carlitz module*, the rank 1 Drinfeld A-module determined by

$$\phi_T = T\tau^0 + \tau,$$

which is the first Drinfeld module to have been studied. Note that every rank 1 Drinfeld A-module over $\mathbf{C}$ is isomorphic (over $\mathbf{C}$) to the Carlitz module, as follows from Proposition 1.1.14, for example.

Next, we define

$$t(z) = (\bar{\pi} e_A(z))^{-1}.$$

This will play the role of the uniformizer $q(z) = \exp(2\pi i z)$ in the classical theory.

Any rank 2 Drinfeld A-module over $\mathbf{C}$ is determined by

$$\phi_T = T\tau^0 + g\tau + \Delta\tau^2, \quad \Delta \neq 0,$$

and therefore the association $z \mapsto \phi^z$ induces functions

$$\Delta : \Omega \longrightarrow \mathbf{C}; \;\; z \mapsto \Delta(z)$$

and

$$g : \Omega \longrightarrow \mathbf{C}; \;\; z \mapsto g(z).$$

These are in fact holomorphic maps (in the non-archimedian analysis on $\mathbf{C}$), and are the most basic examples of *Drinfeld modular functions*. They are uniformized by $t(z)$ as follows (see [30]).

$$\Delta(z) = -\bar{\pi}^{q^2-1} t(z)^{q-1} \prod_{a \in A,\, a \text{ monic}} \Big(t(z)^{|a|} / t(az) \Big)^{(q^2-1)(q-1)} \tag{3.4}$$

$$g(z) = \bar{\pi}^{q-1} \Big(1 - [1] \sum_{a \in A,\, a \text{ monic}} t(az)^{q-1} \Big). \tag{3.5}$$

As $j(z) = g(z)^{q+1}/\Delta(z)$, this gives us a uniformization of j, too.

Definition 3.2.1 *Let $z \in \Omega$. Then we define*

$$\begin{aligned} |z|_A &= \inf_{a \in A} |z - a|, \quad \textit{and} \\ |z|_i &= \inf_{x \in k_\infty} |z - x|. \end{aligned}$$

The imaginary modulus $|z|_i$ *plays the role of* $|\Im(z)|$ *in the classical case.*

Then we start by estimating $t(z)$ (see [10, Lemma 2.6.1]):

Proposition 3.2.2 *Let $z \in \Omega$, and suppose that $|z|_A = |z|_i$. Put $n = \lceil \max(\log_q |z|_A, 0) \rceil$. Then there exists some $\zeta \in \mathbf{C}$, $|\zeta| < 1$, such that*

$$\begin{aligned} t(z) &= (\bar{\pi} z / T^n)^{-q^n} (1 - (z/T^n)^{q-1})^{-q^n} (1 + \zeta) \\ |t(z)| &= |\bar{\pi} z / T^n|^{-q^n} \end{aligned}$$

Plugging this into the series (3.4) and (3.5), one obtains [10, Lemma 2.6.9]

Proposition 3.2.3 *Suppose that $z \in \Omega$ with $|z|_A > q^{-1}$.*

1. *There exists some $\zeta \in \mathbf{C}$ with $|\zeta| < \max(1, |T^q t(z)^{q-1}|)$, such that*

$$\begin{aligned} j(z) &= -t(z)^{-(q-1)}(1 - T^q t(z)^{q-1} + \zeta)^{q+1}, \\ |j(z)| &= |t(z)|^{-(q-1)}|1 - T^q t(z)^{q-1}|^{q+1}. \end{aligned}$$

2. *All the zeros of $j(z)$ are of order $q+1$. More precisely, if $u \in \mathbb{F}_{q^2} \smallsetminus \mathbb{F}_q$ satisfies $|u - z| \leq q^{-1}$, then there exists some $\zeta \in \mathbf{C}$ with $|\zeta| < 1$ such that*

$$\begin{aligned} j(z) &= T^q u^{-2}(1 - u^{q-1})^{-2}(z - u)^{q+1}(1 + \zeta), \\ |j(z)| &= q^q |z - u|^{q+1}. \end{aligned}$$

3.2.2 The quadratic fundamental domain

We want to apply Proposition 3.2.3 to the j-invariant of a CM Drinfeld module. For this, we need to come to terms with the moduli $|\cdot|_A$ and $|\cdot|_i$.

Let $\mathcal{O}$ be an order in the imaginary quadratic function field $K = k(\sqrt{D})$, where D is square-free. Then any ideal $\mathfrak{a} \subset \mathcal{O}$ is a rank 2 lattice in $\mathbf{C}$. It follows that $\mathfrak{a}$ is homothetic to the lattic $\Lambda_z = \langle z, 1 \rangle$, for some $z \in \Omega$. This z is determined up to $\mathrm{PGL}_2(A)$-action, so we would like to have a fundamental domain for this action. Unfortunately, a perfect analogue of the classical fundamental domain for the $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathfrak{H}$ does not seem to exist, but if we're only interested in quadratic z, then we do have the next best thing.

Definition 3.2.4 *The* quadratic fundamental domain *is*

$$\begin{aligned} \mathcal{D} = \{ z \in \Omega \quad | \quad & z \text{ satisfies an equation of the form } az^2 + bz + c = 0, \\ & \text{where } a, b, c \in A, \ a \text{ is monic, } |b| < |a| \leq |c|, \\ & \text{and } \gcd(a, b, c) = 1 \}. \end{aligned}$$

In general we're only interested in $\mathcal{D} \cap K$, which we denote $\mathcal{D}_K$. In this case we have, for any $z \in \mathcal{D}_K$, that $K = k(\sqrt{d})$, where $d = b^2 - 4ac$ is the discriminant of z.

Proposition 3.2.5

1. *Any rank 2 lattice in K is homothetic to Λ_z for some $z \in \mathcal{D}_K$.*

2. *If $z \in \mathcal{D}_K$, then $|z|_i = |z|_A = |z| \geq 1$.*

Proof. (1) The proof is identical to the classical case.

(2) It suffices to show that $|z|_i = |z| \geq 1$, as clearly $|z|_i \leq |z|_A \leq |z|$. Write $z = (-b + \sqrt{d})/2a$, where $d = b^2 - 4ac$. Then $|d| = |b^2 - 4ac| = |ac| \geq |a^2|$ and $|d| \leq |c^2|$. Hence $|z| = |\sqrt{d}/2a| \geq 1$.

We can only get $|z - x| < |z|$ for $x \in k_\infty$ if $|x| = |z|$. We distinguish two cases.

(a) If ∞ is ramified in K/k, then $\deg(d)$ is odd and $v_\infty(\sqrt{d}/2a) = v_\infty(\sqrt{d}) - v_\infty(2a) \in \frac{1}{2}\mathbb{Z} \smallsetminus \mathbb{Z}$ is half integral, so $|x| \neq |z|$ and $|z - x| \geq |z| \ \ \forall x \in k_\infty$.

(b) If ∞ is inert, then $\deg(d)$ is even, but its leading coefficient is not a square in $\mathbb{F}_q$. So even though there exists $x = \sum_{n \geq n_0} a_n T^{-n} \in k_\infty = \mathbb{F}_q((1/T))$ with $\deg(x) = n_0 = \deg(\sqrt{d}/2a)$, the leading coefficient of $\sqrt{d}/2a$ as a Laurent series in $1/T$ is not in $\mathbb{F}_q$, so the leading terms of x and $\sqrt{d}/2a$ cannot cancel. Hence $|z - x| = |x| = |z|$ in this case.

□

Now let ϕ be a CM Drinfeld module, with $\mathrm{End}(\phi) = \mathcal{O}$ an order in K. Then $\phi = \phi^z$ for some $z \in \mathcal{D}_K$. Let $d = \mathrm{Discr}(z)$, then $\mathcal{O} = \mathrm{End}(\Lambda_z) = A[\sqrt{d}] = A[f\sqrt{D}]$ is an order of conductor f in $K = k(\sqrt{D})$, where D is the square-free part of d. We estimate $j(\phi) = j(z)$ as follows.

Theorem 3.3 *Suppose q is odd. Let $z = (-b + \sqrt{d})/2a \in \mathcal{D}_K$. Then*

1. *If $|z| = 1$ then $|j(z)| \leq 1/q$.*
2. *If $|z| > 1$ then $|j(z)| = B_q^{|z|}$, where*

$$B_q = \begin{cases} q^q & \text{if } \deg(d) \text{ is even} \\ q^{\sqrt{q}(q+1)/2} & \text{if } \deg(d) \text{ is odd.} \end{cases}$$

In particular, $|z| \mapsto |j(z)|$ is an increasing function on $\mathcal{D}_K$.

Proof. We just follow the proof of [10, Theorem 2.8.2], using the fact that $|z|_A = |z|_i = |z|$ when $z \in \mathcal{D}_K$. Then all the calculations of [10] work and we do not need to assume that d be square-free (i.e. that z correspond to a Drinfeld module with complex multiplication by the full ring of integers $\mathcal{O}_K$ of K).

We first need a definition. For $x \in \bar{k}_\infty$ we let $\omega(x)$ denote the (unique) element of $\overline{\mathbb{F}}_q$ satisfying

$$|x - \omega(x)T^{-v_\infty(x)}| < |x|.$$

We call $\omega(x)$ the *leading coefficient* of x. For $x \in k_\infty$, this is just the leading coefficient of x viewed as a Laurent series in $1/T$. Throughout the proof, ζ will denote some element (not always the same) in $\mathbf{C}$ satisfying $|\zeta| < 1$.

Now let $n = \lceil \max(\log|z|, 0) \rceil$, so $|z| = q^{n-\varepsilon}$ with $\varepsilon \in \{0, \frac{1}{2}\}$. More precisely, $\varepsilon = \frac{1}{2}$ if and only if $\deg(d)$ is odd (i.e. ∞ ramifies in K/k).

Case 1. We first suppose that $n = 0$. Then $|z| = 1$, as $z \in \mathcal{D}_K$, and $\varepsilon = 0$. Let $u = \omega(z)$. As $z \in K$, we clearly have $u \in \mathbb{F}_{q^2}$. On the other hand, as $\deg(d)$ is even, $\omega(d)$ is not a square in $\mathbb{F}_q$, whence $u = \sqrt{\omega(d)}/2 \notin \mathbb{F}_q$ (recall that a is monic). It follows that $u \in \mathbb{F}_{q^2} \smallsetminus \mathbb{F}_q$, and we apply Proposition 3.2.3(2) to obtain

$$|j(z)| = q^q |z - u|^{q+1} \leq q^{-1},$$

as $|z - u| \leq q^{-1}$.

Case 2. Now suppose that $n \geq 1$. We suppose that $\deg(d)$ is odd, so $\varepsilon = \frac{1}{2}$ and $|z| = q^{n-\frac{1}{2}}$. Let $\omega = \omega(d)$ denote the leading coefficient of d. Note that $\omega \in \mathbb{F}_q$, so $\omega^q = \omega$, and $\omega^{q-1} = 1$.

Then we may write $z/T^n = \frac{1}{2}\omega^{\frac{1}{2}}T^{-\frac{1}{2}}(1+\zeta)$. In particular, $|z/T^n| < 1$, so substituting this into Proposition 3.2.2 gives

$$\begin{aligned} t(z) &= (\bar{\pi}z/T^n)^{-q^n} \cdot (1-(z/T^n)^{q-1})^{-q^n} \cdot (1+\zeta) \\ &= (\bar{\pi})^{-q^n} \cdot (\frac{1}{2}\omega^{\frac{1}{2}} \cdot T^{-\frac{1}{2}})^{-q^n} \cdot (1+\zeta), \quad \text{so} \\ t(z)^{q-1} &= (\bar{\pi})^{-q^n(q-1)} \cdot \omega^{-(q-1)/2} \cdot T^{q^n(q-1)/2} \cdot (1+\zeta), \quad \text{and} \\ |t(z)^{q-1}| &= q^{-q^n(q+1)/2} < q^{-q} \quad (\text{as } q \geq 2, n \geq 1). \end{aligned}$$

Here we have used

$$|\bar{\pi}| = q^{q/(q-1)}.$$

Substituting this expression for $t(z)$ into Proposition 3.2.3(1), we get

$$\begin{aligned} j(z) &= -t(z)^{-(q-1)} \cdot (1 - T^q t(z)^{q-1} + \zeta)^{q+1} \\ &= -(\bar{\pi})^{q^n(q-1)} \cdot \omega^{(q-1)/2} \cdot T^{-q^n(q-1)/2} \cdot (1+\zeta) \\ &= \omega^{(q-1)/2} \cdot T^{q^{n+1}} \cdot T^{-q^n(q-1)/2} \cdot (1+\zeta) \quad (\text{using } \bar{\pi}^{q-1} = -T^q(1+\zeta)) \\ &= \omega^{(q-1)/2} \cdot T^{q^n(q+1)/2} \cdot (1+\zeta), \quad \text{and so} \\ |j(z)| &= q^{q^n(q+1)/2} \\ &= (q^{\sqrt{q}(q+1)/2})^{|z|} \\ &= B_q^{|z|} \end{aligned}$$

as required.

Case 3. Lastly, we suppose $n \geq 1$ and $\deg(d)$ is even. Then $\varepsilon = 0$ and $|z| = q^n$. Here $\omega = \omega(d)$ is not a square in $\mathbb{F}_q$, so $\omega^{(q-1)/2} = -1$. We have $z/T^n = \frac{1}{2}\omega^{\frac{1}{2}}(1+\zeta)$, so

$$\begin{aligned} t(z) &= (\bar{\pi}z/T^n)^{-q^n} \cdot (1-(z/T^n)^{q-1})^{-q^n} \cdot (1+\zeta) \\ &= (\frac{1}{2}\bar{\pi}\omega^{\frac{1}{2}})^{-q^n} \cdot (1-(-1))^{-q^n} \cdot (1+\zeta) \\ &= \omega^{\frac{1}{2}} \cdot (\bar{\pi})^{-q^n} \cdot (1+\zeta), \quad \text{so} \\ t(z)^{q-1} &= T^{-q^{n+1}}(1+\zeta), \quad \text{and} \\ |t(z)^{q-1}| &= q^{-q^{n+1}} < q^{-q}. \quad \text{Now} \\ j(z) &= -t(z)^{-(q-1)}(1 - T^q t(z)^{q-1} + \zeta)^{q+1}, \quad \text{whence} \\ |j(z)| &= q^{q^{n+1}} \\ &= B_q^{|z|}, \end{aligned}$$

as required.

□

Corollary 3.2.6 *Let $\mathcal{O}$ be an order in K, and let $\mathfrak{a} \subset \mathcal{O}$ be an invertible ideal. Then $|j(\mathfrak{a})| \leq |j(\mathcal{O})|$, with equality if and only if $\mathfrak{a}$ is principal.*

Proof. Write $\mathcal{O} = A[\sqrt{d}]$. Then the representatives $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ of the ideal classes in $\mathrm{Pic}(\mathcal{O})$, with $h = \#\mathrm{Pic}(\mathcal{O})$ and $\mathfrak{a}_1 = \mathcal{O}$, correspond to elements $z_i = (-b_i + \sqrt{d_i})/2a_i \in \mathcal{D}_K$, with $z_1 = \sqrt{d_1} = \sqrt{d}$. Now

$$A[\sqrt{d_i}] = \mathrm{End}(\Lambda_{z_i}) = \mathrm{End}(j(\mathfrak{a}_i)) = \mathcal{O} = A[\sqrt{d}]$$

for every i, so we see that d and d_i differ only by the square of a unit, hence can be assumed to be equal. Now we have $|z_1| = |\sqrt{d}| > |\sqrt{d}/2a_i| = |z_i|$ for all $i \neq 1$ and the result follows from Theorem 3.3. (Note that if $|a_i| = 1$, then $a_i = 1$ and $b_i = 0$, so $i = 1$.)

□

It follows in particular that $j(\mathcal{O})$ is larger than any of its other conjugates.

3.3 CM heights

Definition 3.3.1 *Let ϕ be a CM Drinfeld module, with End(ϕ) $= A[\sqrt{d}]$ and j-invariant $j = j(\phi)$. Then we define the* CM height *of ϕ to be*

$$H_{CM}(\phi) = H_{CM}(j) = |d|.$$

If $x = (x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbf{C})$ then we define

$$H_{CM}(x) = \max\{H_{CM}(x_1), \ldots, H_{CM}(x_n)\}.$$

This height is not to be confused with the term occuring in Proposition 1.1.2(3), in fact all the Drinfeld modules here have generic characteristic. The CM height is so-named because it forms a true counting function on the CM points of $\mathbb{A}^1(\mathbf{C})$ (and thus also of $\mathbb{A}^n(\mathbf{C})$).

Proposition 3.3.2 *For every $\varepsilon > 0$ we have*

$$\#\{j \in \mathbf{C} \mid j \text{ is CM and } H_{CM}(j) \leq t\} = O(t^{3/2+\varepsilon}).$$

Proof. For every order $\mathcal{O}_d = A[\sqrt{d}]$, there are exactly $\#\mathrm{Pic}(\mathcal{O}_d)$ isomorphism classes of Drinfeld modules ϕ with $\mathrm{End}(\phi) = \mathcal{O}_d$, namely those corresponding to the ideal classes $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_d)$. So we have

$$\begin{aligned}
\#\{j \in \mathbf{C} \mid j \text{ is CM and } H_{CM}(j) \leq t\} &= \sum_{|d| \leq t} \#\mathrm{Pic}(\mathcal{O}_d) \\
&\leq \sum_{|d| \leq t} B_\varepsilon |d|^{1/2+\varepsilon} \qquad \text{from (3.3)} \\
&= B_\varepsilon \sum_{n=0}^{\lfloor \log(t) \rfloor} \sum_{|d| = q^n} |d|^{1/2+\varepsilon} \\
&= B_\varepsilon \sum_{n=0}^{\lfloor \log(t) \rfloor} q^{n+1} (q^n)^{1/2+\varepsilon}
\end{aligned}$$

$$\begin{aligned} &= qB_\varepsilon \sum_{n=0}^{\lfloor \log(t) \rfloor} (q^{3/2+\varepsilon})^n \\ &= qB_\varepsilon \frac{q^{(3/2+\varepsilon)(\lfloor \log(t) \rfloor + 1)} - 1}{q^{3/2+\varepsilon} - 1} \\ &= O(t^{3/2+\varepsilon}). \end{aligned}$$

□

Now that we may view the CM height as a height function, one may ask how this compares to the usual (i.e. arithmetic) height in $\mathbb{P}^1$. We recall the definition of the height (see for example [37, Part B] or [40, Chapter 3]).

Definition 3.3.3 *Let $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n(\bar{k})$. Let F be a finite extension of k containing $x_0, \ldots, x_n$, and normalize the absolute values $|\cdot|_v$ corresponding to the places $v \in \mathbb{P}_F$ in such a way that the product formula*

$$\prod_{v \in \mathbb{P}_F} |x|_v = 1, \ \forall x \in F$$

holds. Then we define the arithmetic height *of x by*

$$h(x) = \frac{1}{[F:k]} \sum_{v \in \mathbb{P}_F} \log(\max\{|x_0|_v, \ldots, |x_n|_v\}).$$

The height $h(x)$ is independent of the choice of F. If $x = (x_1, \ldots, x_n) \in \mathbb{A}^n(\bar{k})$, then we let $x' = (x_1 : \ldots : x_n : 1) \in \mathbb{P}^n(\bar{k})$ and set $h(x) = h(x')$.

Let $j \in \mathbf{C} = \mathbb{A}^1(\mathbf{C})$ be a CM point. Then $j \in k^{sep}$, so we may compare its CM height with its arithmetic height.

Proposition 3.3.4 *Let $j \in k^{sep}$ be a CM point, with $End(j) = \mathcal{O} = A[\sqrt{d}]$ and $H_{CM}(j) = |d|$. Then $h(j) \leq H_{CM}(j)^{1/2} + C_q$, where*

$$C_q = \begin{cases} q & \text{if } \deg(d) \text{ is even} \\ \sqrt{q}(q+1)/2 & \text{if } \deg(d) \text{ is odd.} \end{cases}$$

Proof. Let $K = \mathcal{O} \otimes_A k$ denote the CM field, and choose $F = K(j)$ as a field of definition for j, and fix an embedding $F \hookrightarrow \mathbf{C}$. We recall from Theorem 1.6 that j is integral over A, so that $|j|_v \leq 1$ for any place v of F that does not lie over the (unique) place ∞ of K. On the other hand, the place ∞ splits completely in F/K, so for any place $v|\infty$ of F we have $|j|_v = |\sigma_v(j)|$, where $\sigma_v : K \hookrightarrow F$ is the embedding of K into F corresponding to the place v, and $|\cdot|$ denotes the usual (chosen) absolute value of $\mathbf{C}$. This gives us

$$h(j) \quad = \quad \frac{1}{[F:K]} \sum_{v \in \mathbb{P}_F} \log(\max\{|j|_v, 1\})$$

$$\begin{aligned}
&= \frac{1}{[F:K]} \sum_{v|\infty} \log(\max\{|j|_v, 1\}) \qquad (j \text{ is integral}) \\
&= \frac{1}{[F:K]} \sum_{\sigma \in \mathrm{Gal}(F/K)} \log(\max\{|\sigma(j)|, 1\}) \\
&= \frac{1}{[F:K]} \sum_{[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})} \log(\max\{|j(\mathfrak{a})|, 1\}) \\
&\leq \log|j(\mathcal{O})| \qquad \text{(from Corollary 3.2.6)} \\
&\leq |z| + \log(B_q) \qquad \text{(from Theorem 3.3)} \\
&= |d|^{1/2} + C_q.
\end{aligned}$$

The result follows.

□

The results of this section are analogous to those of §B.2, but notice that in Proposition 3.3.4 we can explicitely state the constants involved. This is because we have a better estimate for $|j|$ here than in characteristic 0. (But with some hard work, one can attain even better estimates in characteristic 0, see [14]).

3.4 CM points on curves

We are now ready to prove our first main result: the André-Oort conjecture for the product of two Drinfeld modular curves. Our approach is very similar to that of Edixhoven in [19], in fact it is a characteristic p rendition of §C.6. However, the analogue of the Generalized Riemann Hypothesis holds true in function fields (Theorem 3.1(5)), so our result is unconditional.

Theorem 3.4 *Assume that q is odd. Let d and m be given positive integers, and g a given non-negative integer. Then there exists an effectively computable constant $B = B(d, m, g)$ such that the following holds. Let X be an irreducible algebraic curve in $\mathbb{A}^2$ of degree d, defined over a finite extension F of k of degree $[F:k] = m$ and genus $g(F) = g$. Then X is a modular curve $Y_0'(N)$ for some $N \in A$ if and only if X contains a CM point of arithmetic height at least B.*

Proof. Let the curve $X \subset \mathbb{A}^2$ be as in the theorem. Firstly, it is clear that the modular curves $Y_0'(N)$ contain CM points of arbitrary height. We want to prove the converse. Let $x = (x_1, x_2) \in X(\mathbf{C})$ be a CM point. From Proposition 3.3.4 follows that it suffices to show that X is modular if x has a large *CM height*. If X is a horizontal or a vertical line, and the fixed coordinate is a CM point (x_1 or x_2) in $\mathbb{A}^1$, and X is modular. So we may assume that both projections $p_i : X \to \mathbb{A}^1$ are dominant. We want to use Theorem 2.2, so we must show that X is fixed by a suitable Hecke operator.

We first assume that F/k is separable. Now we replace F by its Galois closure F', and we claim that the degree and genus of F' are still bounded in terms of m and g. Indeed, write $F = k(w)$, where w is a primitive element. Denote by $w_1, \ldots, w_m$ all the conjugates of w in k^{sep}. Then the fields $F_i = k(w_i)$ are

all isomorphic to F, and the Galois closure F' is the composite $F' = F_1 \cdots F_m$. Hence $[F' : k] \leq m^m$ and the genus of F' is bounded in terms of m and g using the Castelnuovo inequality (see [65, Theorem III.10.3]), which we will state here for convenience.

Proposition 3.4.1 (Castelnuovo Inequality) *Let F_1 and F_2 be two function fields, and let $F = F_1F_2$ be their compositum. Let $n_i = [F : F_i]$ and $g(F_i)$ be the genus of F_i. Then the genus of F is bounded by*

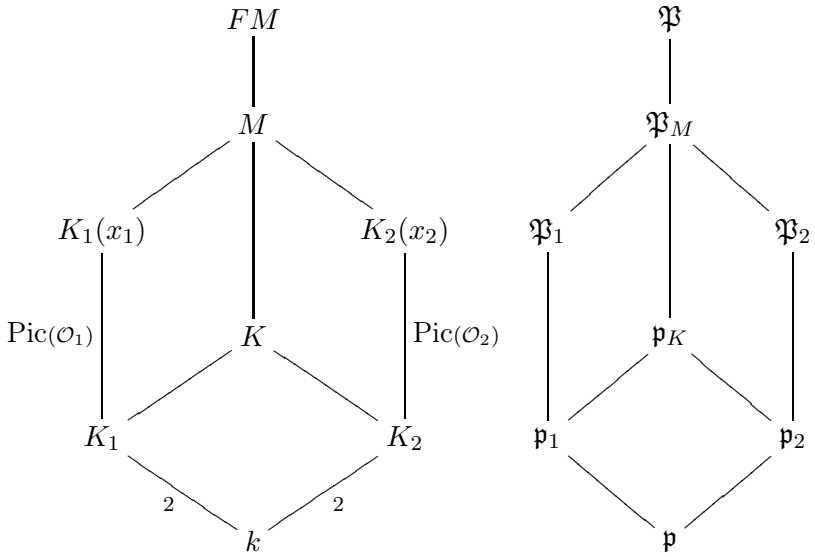
$$g(F) \leq n_1 g(F_1) + n_2 g(F_2) + (n_1 - 1)(n_2 - 1).$$

It follows that the genus of F' is bounded (crudely) by

$$g(F') < m^m g + m^{m+1},$$

which proves the claim. Hence we may assume that F/k is Galois.

Let $\mathcal{O}_i = \mathrm{End}(x_i)$ be orders of conductors f_i in the imaginary quadratic fields K_i, for $i = 1, 2$, and let $K = K_1K_2$ and $M = K(x_1, x_2)$. Let $\mathfrak{p}$ be a prime of even degree in k which splits completely in FK (and thus in K_1, K_2 and F) and does not divide f_1f_2. Let $\mathfrak{P}$ be a prime of FM lying over $\mathfrak{p}$, and denote by $\mathfrak{P}_M$, $\mathfrak{P}_i$, $\mathfrak{p}_K$ and $\mathfrak{p}_i$ its restriction to the fields M, $K_i(x_i)$, K and K_i, respectively. This is all summarized in the following diagram.



From Theorem 1.6 we see that all these extensions are Galois, $\mathrm{Gal}(K_i(x_i)/K_i) \cong \mathrm{Pic}(\mathcal{O}_i)$ and $\mathfrak{p}$ is unrammified in FM/k. Let $\sigma = (\mathfrak{P}, FM/k)$ be the Frobenius element, and let $\sigma_i = (\mathfrak{P}_i, K_i(x_i)/k) = \sigma|_{K_i(x_i)}$. As $\mathfrak{p}$ splits in K_i we see that in fact $\sigma_i = (\mathfrak{P}_i, K_i(x_i)/K_i)$. Now it follows again from Theorem 1.6 that we have isogenies $x_i \to x_i^\sigma$ with kernels isomorphic to $A/\mathfrak{p}$ as A-modules, so $(x_1, x_2) \in T_{\mathbb{A}^2,\mathfrak{p}}(x_1, x_2)^\sigma$. In other words, $(x_1, x_2) \in X \cap T_{\mathbb{A}^2,\mathfrak{p}}(X^\sigma) = X \cap T_{\mathbb{A}^2,\mathfrak{p}}(X)$, as σ acts trivially on F, the field of definition of X and $T_{\mathbb{A}^2,\mathfrak{p}}(X)$.

On the one hand, from Proposition 2.1.6 follows that $\deg(X \cap T_{\mathbb{A}^2,\mathfrak{p}}(X)) \leq d^2(|\mathfrak{p}|+1)^2$. On the other hand, the whole $\mathrm{Gal}(FM/F)$-orbit of the point (x_1, x_2)

lies in this intersection, giving us at least $\#\mathrm{Pic}(\mathcal{O}_i)/m$ points in the intersection (for $i = 1$ and $i = 2$). We must show that $\#\mathrm{Pic}(\mathcal{O}_i) > md^2(|\mathfrak{p}|+1)^2$, as then the intersection will be improper, giving $X \subset T_{\mathbb{A}^2,\mathfrak{p}}(X)$, as X is irreducible. Then the result will follow from Theorem 2.2, if $|\mathfrak{p}| \geq \max(13, d)$ (recall that $\mathfrak{p}$ was chosen of even degree).

Let $\mathcal{O}_i = A[f_i\sqrt{D_i}]$, where $D_i \in A$ is square-free. Then $H_{CM}(x_i) = |D_i f_i^2|$. We denote by g_i the genus of the CM field K_i, where we recall that

$$g_i = \begin{cases} (\deg(D_i) - 1)/2 & \text{if } \deg(D_i) \text{ is odd} \\ (\deg(D_i) - 2)/2 & \text{if } \deg(D_i) \text{ is even.} \end{cases}$$

Then for every $\varepsilon > 0$, (3.2) gives us

$$\#\mathrm{Pic}(\mathcal{O}_i) \geq C_\varepsilon (q^{g_i}|f_i|)^{1-\varepsilon}, \tag{3.6}$$

where $C_\varepsilon > 0$ is an absolutely computable constant, depending on ε.

It remains to show that there exist primes $\mathfrak{p}$ which have the desired properties. For this we use the Čebotarev Theorem. Let

$$\pi_{FK}(t) = \#\{\mathfrak{p} \in A \mid \text{prime, split in } FK, \text{ and } |\mathfrak{p}| = q^t\}.$$

Suppose the CM fields K_1 and K_2 are not equal, so $[K : k] = 4$ (the case $K = K_1 = K_2$ is the same, with a few constants changed). Let L be the algebraic closure of $\mathbb{F}_q$ in FK, let $n_c = [L : \mathbb{F}_q]$ be the constant extension degree and $n_g = [FK : Lk]$ be the geometric extension degree. If $n_c \nmid t$ then $\pi_{FK}(t) = 0$. If $n_c | t$ then Theorem 1.5 gives us

$$|\pi_{FK}(t) - \frac{1}{n_g} q^t/t| < 4(g(FK) + 2)q^{t/2}.$$

Here $g(FK)$ is the genus of FK, which can be bounded with the Castelnuovo inequality to give $g(FK) \leq 2m(g_1+g_2)+4g+4m-3$. We also have $n_g n_c \leq 4m$.

Now we want both $\pi_{FK}(t) > \deg(f_1 f_2) = \log|f_1 f_2|$ (so that we have a split prime $\mathfrak{p}$ not dividing $f_1 f_2$) and $\#\mathrm{Pic}(\mathcal{O}_i) > md^2(q^t+1)^2$ (so that $X \subset T_{\mathbb{A}^2,\mathfrak{p}}(X)$).

Summarising, we need a simultaneous solution $t \in 2\mathbb{N}$ to the inequalities

$$\frac{1}{4m} q^t/t - 4(2m(g_1 + g_2 + 2) + 4g - 1)q^{t/2} > \log|f_1 f_2| \tag{3.7}$$

$$C_\varepsilon (q^{g_i}|f_i|)^{1-\varepsilon} > md^2(q^t + 1)^2 \tag{3.8}$$

for some $\varepsilon > 0$ and at least one of $i = 1$ or $i = 2$ (and of course $n_c | t$).

These inequalities hold for t sufficiently large (more precisely, we want $q^t \geq \max(13, d)$) if $H_{CM}(x_1, x_2) = \max(|D_1 f_1^2|, |D_2 f_2^2|)$ is larger than some computable constant B_1, which depends on d, m and g.

Lastly, we point out that if F/k is not separable, we first replace F by F_s, the separable closure of k in F, then extend the Frobenius element $\sigma \in (\mathfrak{P}, F_s M/k) \in \mathrm{Gal}(F_s M/F_s K)$ to $\mathrm{Aut}(FM/FK)$. This automorphism still has the desired properties.

□

We can easily generalize this to curves in the product of n Drinfeld modular curves. In fact, from Theorem 3.4 and Propositions 1.3.4 and 1.3.10 follows:

Corollary 3.4.2 *Let $X_1, \ldots, X_n$ be Drinfeld modular curves. Let $Z = X_1 \times \cdots \times X_n$, and let $X \subset Z$ be an irreducible algebraic curve. Then the following are equivalent:*

1. *X contains infinitely many CM points*
2. *X contains at least one CM point of height larger than some effectively computable constant which depends only on Z, $\deg(X)$ and the field of definition of X.*
3. *There exists a non-empty subset $S \subset \{1, \ldots, n\}$ for which we may write*

$$Z \cong Z_S \times Z'_S = \Big(\prod_{i \in S} X_i\Big) \times \Big(\prod_{i \notin S} X_i\Big).$$

Then

$$X = X' \times \Big(\prod_{i \notin S} \{x_i\}\Big),$$

where the $x_i \in X_i$ are CM points and X' is a Hecke correspondence on Z_S.

3.5 CM points on varieties

In this section we prove our second main result: the André-Oort conjecture for subvarieties of the product of n Drinfeld modular curves. The characteristic 0 analogue of this result has been proved by Edixhoven [21], but he must assume the Generalized Riemann Hypothesis for imaginary quadratic fields. The treatment here is based closely on his method.

Theorem 3.5 *Suppose q is odd. Let $X \subset \mathbb{A}^n$ be an irreducible variety, containing a Zariski-dense subset S of CM points. Then X is a modular variety.*

Proof. As CM points are defined over k^{sep}, so is X. Hence there exists a finite Galois extension F of k such that X is defined over F.

Set $d = \dim(X)$. We will use induction on d. From Theorem 3.4 and Corollary 3.4.2 we know that the result already holds for $d = 1$. We now suppose $d \geq 2$, $n \geq 3$ and that the result is already known for dimensions less than d. In fact, it follows from Proposition 1.3.8 that we may assume X to be a hypersurface, i.e. $d = n - 1$.

If there is some projection $p_i : X \to \mathbb{A}^1$ which is not dominant, then X is of the form $\mathbb{A}^{n-1} \times \{x_i\}$, for a CM point x_i, and hence is modular. So now we may assume that every projection $p_i : X \to \mathbb{A}^1$ is dominant.

For a given constant $B > 0$ we may assume that every point $x = (x_1, \ldots, x_n) \in S$ satisfies $H_{CM}(x_i) > B$ for all $i = 1, \ldots, n$, as the set

$$\{x \in X \mid H_{CM}(x_i) \leq B \text{ for some } i = 1, \ldots, n\}$$

is contained in a proper closed subvariety of X.

Step 1. Choose a point $x = (x_1, \ldots, x_n) \in S$. Suppose that we have primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_{d-1}$ satisfying the following conditions:

1. Each $\mathfrak{p}_j$ splits completely in every $\mathcal{O}_i = \mathrm{End}(x_i)$ for $i = 1, \ldots, n$ and in F.
2. $|\mathfrak{p}_1| \geq \max\{13, \deg X\}$
3. $|\mathfrak{p}_{j+1}| \geq (\deg X)^{2^j} \prod_{m=1}^{j} (2|\mathfrak{p}_m| + 2)^{n2^{j-m}}$ for $j = 1, \ldots, d-2$
4. We have $\#\mathrm{Pic}(\mathcal{O}_i) > [F : k](\deg X)^{2^{d-1}} \prod_{m=1}^{d-1} (2|\mathfrak{p}_m| + 2)^{n2^{d-m-1}}$ for each $i = 1, \ldots, n$, for which it suffices to assume

$$\#\mathrm{Pic}(\mathcal{O}_i) > [F : k]|\mathfrak{p}_{d-1}|^2 (2|\mathfrak{p}_{d-1}| + 2)^n. \tag{3.9}$$

Then, as in the proof of Theorem 3.4 it follows that

$$\mathrm{Gal}(F^{sep}/F) \cdot x \subset X \cap T_{\mathbb{A}^n, \mathfrak{p}_1}(X).$$

Let X_1 be an F-irreducible component of $X \cap T_{\mathfrak{p}_1}(X)$ containing x. Now either $\dim(X_1) = \dim(X)$, in which case $X_1 \subset T_{\mathfrak{p}_1}(X_1)$ and X_1 is modular (Theorem 2.3), or $\dim(X_1) < \dim(X)$. In the latter case we repeat the procedure: We let X_2 be an F-irreducible component of $X_1 \cap T_{\mathfrak{p}_2}(X_1)$ containing x, and so on. We thus produce a sequence $X_1, X_2, \ldots$ of F-irreducible subvarieties of X of strictly decreasing dimension. But, as the X_j are defined over F, the full $\mathrm{Gal}(F^{sep}/F)$-orbit of x is contained in each X_j. Moreover, after at most $d-1$ steps we arrive at $\dim(X_j) \leq 1$, and

$$\begin{aligned} \deg X_j &\leq (\deg X)^{2^j} \prod_{m=1}^{j} (2|\mathfrak{p}_m| + 2)^{n2^{j-m}} \quad \text{(using Proposition 2.1.6)} \\ &< \#\mathrm{Pic}(\mathcal{O}_i)/[F : k] \leq \#\mathrm{Gal}(F^{sep}/F) \cdot x \quad (\text{as } j \leq d-1). \end{aligned}$$

Hence X_j must have dimension at least 1. In summary, this process must terminate, after at most $d-1$ steps, with some X_j of dimension at least 1, satisfying $X_j \subset T_{\mathfrak{p}_{j+1}}(X_j)$. Hence X_j is modular.

By varying $x \in S$, we see that we have covered X by a Zariski-dense family of modular subvarieties X_x for $x \in S$. We now show that the X_x's are in fact pure modular. Suppose not. Recall that each X_x is F-irreducible, so if it's not pure then it contains the $\mathrm{Gal}(F^{sep}/F)$-orbit of a modular variety of the form

$$Y_x \times \{y_x\},$$

where y_x is a CM point (in fact a projection of x) and Y_x a pure modular variety. But as the $\mathrm{Gal}(F^{sep}/F)$-orbit of the point y_x is larger than the degree of X_x, by construction, this would mean that the number of (geometrically) irreducible components of X_x of maximal dimension is larger than $\deg(X_x)$, which is impossible. So each X_x is in fact pure modular. Now each X_x contains a Zariski-dense family of pure modular curves, hence so does X.

Step 2. We want to show that X is modular, using the fact that X is covered by a Zariski-dense family of pure modular curves. For ease of notation we will denote this family by S and the pure modular curves by $s \in S$.

Choose a CM point $x_1 \in \mathbb{A}^1(\mathbf{C})$ and consider the intersection

$$X_1 = X \cap (\{x_1\} \times \mathbb{A}^{n-1}).$$

As each curve $s \in S$ is pure modular, it intersects X_1 in at least one CM point. We denote by X' the Zariski closure of these points:

$$X' = \overline{\cup_{s \in S}(s \cap X_1)}^{Zar}.$$

Now if $\dim(X') = \dim(X)$, then $X \subset \{x_1\} \times \mathbb{A}^{n-1}$, which is impossible: we had assumed in the beginning that all projections $p_i : X \to \mathbb{A}^1$ are dominant. Hence $\dim(X') < \dim(X)$. Then it follows from the induction hypothesis that all the (geometrically) irreducible components of X' are modular. Write $X' = X'_1 \cup \cdots \cup X'_r$ as the union of r irreducible components. Then the points of $s \cap X_1$ distribute amongst these components. By restricting S to a Zariski-dense subfamily, and renumbering the components of X', we may assume that X'_1 contains at least $1/r$ of the points of $s \cap X_1$ for every $s \in S$.

If, up to permutation of coordinates, X'_1 is of the form $\{y\} \times \mathbb{A}^m$ for some $m < n-1$ and y a CM point in $\mathbb{A}^{n-1-m}$, then it follows that X is of the form (again up to permutation of coordinates) $Y \times \mathbb{A}^{n-2}$, where Y is an irreducible curve in $\mathbb{A}^2$. But then Y contains infinitely many CM points, hence is modular. In this case we see that X is modular.

So we may now assume that X'_1 is not of the above form, so that at least one modular curve appears as a factor of X'_1. Then there exists some pair of coordinates $1 < i < j$ such that

$$p_{i,j}(X'_1) = Y'_0(m),$$

for some *fixed* $m \in A$ (see Proposition 1.3.4).

We now consider the curves $s' = p_{\{1,i,j\}}(s) \subset \mathbb{A}^3$ for each $s \in S$, and digress briefly to give another description of these curves.

Let $y = (y_1, y_2, y_3)$ be a generic point on s'. Then each y_i corresponds to an isomorphism class of lattices L_i in k^2. For every prime $\mathfrak{p} \in A$, we consider the $\mathfrak{p}$-part of these lattices, i.e. we consider $L_{i,\mathfrak{p}} = L_i \otimes_A A_{\mathfrak{p}}$ for $i = 1, 2, 3$, where $A_{\mathfrak{p}}$ denotes the valuation ring of the completion $k_{\mathfrak{p}}$ of k at $\mathfrak{p}$. Then the $L_{i,\mathfrak{p}}$'s correspond to vertices on the Bruhat-Tits tree $\mathcal{T}_{\mathfrak{p}}$ of $\mathrm{PGL}_2(k_{\mathfrak{p}})$. We recall that two vertices v_1 and v_2 of $\mathcal{T}_{\mathfrak{p}}$ are joined by an edge if $L_1/L_2 \cong A/\mathfrak{p}A$ for suitable representatives L_i of v_i. The tree $\mathcal{T}_{\mathfrak{p}}$ is regular of degree $|\mathfrak{p}| + 1$.

Now to any triple (v_1, v_2, v_3) of vertices in $\mathcal{T}_{\mathfrak{p}}$ we may associate a unique vertex v_c called the *center* of (v_1, v_2, v_3), which has the property that the three paths linking v_c to the vertices v_1, v_2 and v_3 are disjoint (unless at least two vertices v_i and v_j coincide, in which case $v_c := v_i = v_j$). Let $n_{1,\mathfrak{p}}, n_{2,\mathfrak{p}}, n_{3,\mathfrak{p}} \in \mathbb{N} \cup \{0\}$ denote the lengths of these three paths, and set $N_i = \prod_{\mathfrak{p} \in A} \mathfrak{p}^{n_{i,\mathfrak{p}}}$ for $i = 1, 2, 3$. Then the pure modular curve $s' \subset \mathbb{A}^3$ is uniquely determined by the triple $(N_1, N_2, N_3) \in A^3$. Furthermore, let L_c be the lattice corresponding to

the center $L_{c,\mathfrak{p}}$ of $(L_{1,\mathfrak{p}}, L_{2,\mathfrak{p}}, L_{3,\mathfrak{p}})$ for every $\mathfrak{p} \in A$. Then L_c corresponds to a point $y_c \in \mathbf{C}$ which is linked to each y_i by a cyclic isogeny of degree N_i, and we have $p_{i,j}(s') = Y_0'(N_iN_j)$ for each $\{i,j\} \subset \{1,2,3\}$, $i \neq j$.

Now we return to our proof of Theorem 3.5, where we have a family S of pure modular curves, and a pair of coordinates $1 < i < j$ such that at least $1/r$ of the points of the form $(x_1, x_i, x_j) \in p_{1,i,j}(s)$, for the x_1 fixed above, satisfy $(x_i, x_j) \in Y_0'(m)$, for some $m \in A$ *independent of* $s \in S$. Let $s \in S$ be characterized by the triplet $(N_{s,1}, N_{s,i}, N_{s,j}) \in A^3$ as above, and assume, by restricting S to a Zariski-dense subfamily and permuting coordinates, that we always have $|N_{s,i}| \leq |N_{s,j}|$. Fix $s \in S$ and fix also x_i such that we have a point $(x_1, x_i, x_j) \in p_{1,i,j}(s)$. We want to find many points x_j with this property. Let x_c be the center of (x_1, x_i, x_j) in the above sense, which is determined by x_1, x_i and $N_{s,1}$, and hence is independent of x_j. Now the number of cyclic degree N_j isogenies leading out from x_c, and disjoint from the paths leading out to x_1 and x_i, is given by $\prod_{\mathfrak{p}\in A}(|\mathfrak{p}|-1)|\mathfrak{p}|^{n_{s,j,\mathfrak{p}}-1} \geq \phi(N_{s,j})$. However, as (x_1, x_i, x_j) is a CM point, some of these isogenies might have the same target, corresponding to non-trivial endomorphisms $\alpha \in \mathrm{End}(x_c)$ of norm $N_{K/k}(\alpha) = N_{s,j}^2$. But the number of such endomorphisms is at most $\prod_{\mathfrak{p}|N_{s,j}}(2n_{s,j,\mathfrak{p}}+1)$ (in the spirit of Proposition 2.2.2), so the number of distict values of x_j satisfying (x_1, x_i, x_j) tends to infinity as $N_{s,j}$ increases.

But $1/r$ of these points also satisfy $(x_i, x_j) \in Y_0'(m)$, of which there can be at most $\psi(m)$, for fixed x_i. So we have shown that $N_{s,j}$, and thus also $N_{s,i}$, is bounded as s ranges through S.

It follows that there are only finitely many possibilities for $p_{i,j}(s) = Y_0'(N_{s,i}N_{s,j})$. By replacing S with a Zariski-dense subfamily, we may assume there is only one: $p_{i,j}(s) = Y_0'(N_0)$ for all $s \in S$. Now, after a permutation $(i,j) \mapsto (n-1, n)$ of coordinates, we see that

$$\begin{aligned} S &\subset \mathbb{A}^{n-2} \times Y_0'(N_0), \quad \text{and so} \\ X = \overline{S}^{Zar} &\subset \mathbb{A}^{n-2} \times Y_0'(N_0). \end{aligned}$$

But X is a hypersurface, so we have in fact $X = \mathbb{A}^{n-2} \times Y_0'(N_0)$, which is modular. This is what we set out to prove.

Step 3. It remains to show that we can find primes $\mathfrak{p}_j$ with the desired properties. Recall that $x = (x_1, \ldots, x_n)$ and each $\mathcal{O}_i = \mathrm{End}(x_i)$ is an order of conductor f_i in the imaginary quadratic field K_i of genus g_i.

Set $|\mathfrak{p}_j| = q^{t_j}$ for $j = 1, \ldots, d-1$. Firstly, we need (3.9), which, combined with the lower bound for the class number (3.2), gives

$$C_\varepsilon (q^{g_i}|f_i|)^{1-\varepsilon} > [F:k] q^{2t_{d-1}} (2q^{t_{d-1}}+2)^n. \tag{3.10}$$

Secondly, the $\mathfrak{p}_j$'s must be well spaced out, i.e. we need

$$q^{t_{j+1}} \geq (\deg X)^{2^j} \prod_{m=1}^{j} (2q^{t_m}+2)^{n2^{j-m}}. \tag{3.11}$$

Thirdly, each $\mathfrak{p}_j$ must split completely in FK, where $K = K_1 \cdots K_n$, and not divide $f_1 \cdots f_n$. Here the Čebotarev Theorem (Theorem 1.5) says

$$|\pi_{LK}(t_j) - \frac{1}{n_g} q^{t_j}/t_j| < 4(g(FK)+2)q^{t_j/2} \quad \text{and } n_c | t_j,$$

where n_g denotes the geometric extension degree of FK/k, n_c denotes the constant extension degree, and $g(FK)$ is the genus of FK. We have $n_g n_c = [FK : k] \leq 2^n [F : k]$ and we may bound $g(FK)$ from above via the Castelnuovo Inequality (Proposition 3.4.1) to obtain $g(FK) \leq C_1(g_1 + \cdots + g_n) + C_2$ for some computable constants C_1 and C_2 depending on the field F.

We need $\pi_{FK}(t_j) > \log |f_1 \cdots f_n|$, so that at least one of these split primes does not divide any of the conductors. In summary, we need $d-1$ simultaneous solutions $t_1, \ldots, t_{d-1} \in 2\mathbb{N}$, $n_c | t_j$ and $q^{t_1} \geq \max(13, \deg X)$ to (3.10), (3.11) and

$$\frac{1}{2^n [F : k]} q^{t_j}/t_j - 4(C_1(g_1 + \cdots + g_n) + C_2 + 2)q^{t_j/2} > \log |f_1 \cdots f_n|. \quad (3.12)$$

If we choose the constant B sufficiently large then, as $B < H_{CM}(x_i) \leq q^{2g_i+1}|f_i|^2$ for all $i = 1, \ldots, n$, such a set of solutions $(t_1, \ldots, t_{d-1})$ exists. Quod erat demonstrandum.

□

From Proposition 1.3.10 now follows

Corollary 3.5.1 *Let $X_1, \ldots, X_n$ be Drinfeld modular curves. Let $Z = X_1 \times \cdots \times X_n$, and let $X \subset Z$ be an irreducible algebraic variety. Then the following are equivalent:*

1. *X contains a Zariski-dense set of CM points*
2. *There exists a partition $\{1, \ldots, n\} = S_0 \coprod \cdots \coprod S_g$ for which we may write*

$$Z \cong \prod_{i=0}^{g} Z_i = \prod_{i=0}^{g} \Big(\prod_{j \in S_i} X_j \Big).$$

Then

$$X = \Big(\prod_{j \in S_0} \{x_j\} \Big) \times \prod_{i=1}^{g} X_i'$$

where the $x_j \in X_j$ (for $j \in S_0$) are CM points and each X_i' is a Hecke correspondence in Z_i (for $i = 1, \ldots, g$).

3.6 Concluding remarks

So we have settled the André-Oort conjecture for products of Drinfeld modular curves, at least in the case of rank 2 Drinfeld A-modules, where $A = \mathbb{F}_q[T]$ and q is odd. What remains to be done?

Firstly, we expect our results to hold in characteristic 2 as well, but many technical little details will have to be replaced by similar details (e.g. the quadratic extensions K/k will be Artin-Schreier extensions instead of Kummer extensions). The next step might be to consider rank 2 Drinfeld $\mathcal{A}$-modules, for $\mathcal{A} = \Gamma(\mathcal{X} \smallsetminus \infty, \mathcal{O}_{\mathcal{X}})$, the ring of functions regular away from a chosen point ∞ on some irreducible projective curve $\mathcal{X}$ over $\mathbb{F}_q$. In this case, however, one no longer has a j-invariant, instead we must deal directly with points on the curve $M^2_{\mathcal{A}}(\mathbf{C}_\infty)$, which parametrizes isomorphism classes of rank 2 Drinfeld $\mathcal{A}$-modules over $\mathbf{C}_\infty$. It should still be possible to derive versions of Theorems 3.4 and 3.5 using an approach similar to the one presented here.

A more difficult generalization will be to look at moduli spaces of (tuples of) rank r Drinfeld modules, for $r > 2$. Here we have to leave the familiar waters of analogy with elliptic curves, and confront creatures that seem half-way between elliptic curves and abelian varieties. At this point, I will not venture any conjecture as to which subvarieties of $M^r_{\mathcal{A}}$ contain Zariski-dense sets of CM points, but I suspect that an approach via Hecke operators should throw some light on the matter.

Furthermore, one may start studying moduli spaces of T-modules. Here, however, we do not yet have enough tools at our disposal. For example, as far as I know the theory of T-modules with complex multiplication has not yet been worked out, so we already run into difficulties before we can even define CM points.

Lastly, there may be other characteristic p analogues of Shimura varieties and Conjecture 0.1, for example via Richard Pink's theory of Hodge structures in characteristic p [55].

As a closing remark, we point out one aspect of Drinfeld modular curves that is conspiciously absent from this thesis: The absolute value $|\cdot|$ of the field $\mathbf{C}$ is non-Archimedian, so we may reduce modulo $|\cdot|$. Reducing the Drinfeld upper half-plane Ω in this way leads to the Bruhat-Tits tree and other useful tools which are very popular in the literature. But I haven't used this at all. The reason is that all my techniques come from $\mathbb{C}$, where such a reduction does not exist. Therefore it is reasonable to expect that one may find more elegant and powerful proofs of the results in this thesis using reduction modulo $|\cdot|$. It may be interesting to try this approach, or to adapt André's transcendence proof for Theorem 0.3 to characteristic p.

Appendix A

Some results from group theory

In this appendix we collect some miscellaneous results from group theory, which are needed in Chapter 2. The results are presented roughly in the order in which they are used. We do not strive for any further generality than is needed.

A.1 Notation

Below, R always denotes a commutative ring with identity, and F denotes a field. We write $G_1 < G_2$ if G_1 is a subgroup of G_2, and $G_1 \lhd G_2$ if G_1 is a normal subgroup of G_2.

We recall that $A = \mathbb{F}_q[T]$, $k = \mathbb{F}_q(T)$ and $k_\infty = \mathbb{F}_q((1/T))$.

$\mathrm{GL}_2(R)$ denotes the group of invertible 2×2 matrices with entries in R.

$\mathrm{SL}_2(R)$ denotes the subgroup of $\mathrm{GL}_2(R)$ of matrices with determinant 1.

$Z(R^*) \cong R^*$ denotes the center of $\mathrm{GL}_2(R)$, i.e. the group of scalar matrices $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, for $a \in R^*$.

$\mathrm{PGL}_2(R) = \mathrm{GL}_2(R)/Z(R^*)$ and $\mathrm{PSL}_2(R) = \mathrm{SL}_2(R)/\{x \in Z(R^*) \mid x^2 = 1\}$.

We will write elements of $\mathrm{PSL}_2(R)$ and $\mathrm{PGL}_2(R)$ as 2×2 matrices, keeping in mind that two matrices define the same element if they differ by a scalar.

A.2 Subgroups of $\mathbf{PGL}_2(R)$ and $\mathbf{PSL}_2(R)$

We start with a very classical result of Dickson, see [39, §II.8, especially Hauptsatz 8.27 and Satz 8.28].

Theorem A.1 (Dickson) *Let $q = p^f$, where p is a prime number. Then the subgroups of $PSL_2(\mathbb{F}_q)$ are precisely the following.*

1. *Elementary abelian p-groups;*
2. *Cyclic groups of order n, where $n|(q \pm 1)/k$, and $k = \gcd(p-1, 2)$;*
3. *Dihedral groups of order $2n$, with n as above;*
4. *The alternating group A_4 if $p > 2$ or $p = 2$ and f is even;*

5. *The symmetric group S_4 if $16|q^2-1$;*
6. *The alternating group A_5 if $5|q^2-1$;*
7. *Semi-direct products of abelians groups of order p^m with cyclic groups of order t, where $t|p^m-1$ and $t|q-1$.*
8. *$PSL_2(\mathbb{F}_{q^m})$ where $m|f$;*
9. *$PGL_2(\mathbb{F}_{q^m})$ where $2m|f$.*

Corollary A.2.1 *If $q \geq 13$, then every proper subgroup of $PSL_2(\mathbb{F}_q)$ has index at least $q+1$.*

Proof. This follows from computing the orders of the subgroups listed in Theorem A.1. We point out that in case (6) above A_5 has order 60, so $[\mathrm{PSL}_2(\mathbb{F}_{11}) : A_5] = 11$, which is why we must assume $q \geq 13$. Case (7) above, for $p^m = q$ and $t = q-1$, gives a Borel subgroup of index $q+1$. □

Next, we investigate $\mathrm{PGL}_2(k_\infty)$.

Lemma A.2.2 $k_\infty^*/k_\infty^{*2} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Proof. Let $x \in k_\infty = \mathbb{F}_q((1/T))$, and write $x = T^{-n}(a_0 + a_1T^{-1} + \cdots)$, with $a_0 \neq 0$. Then x is a square in k_∞ if and only if n is even and a_0 is a square in $\mathbb{F}_q$, so we get an isomorphism

$$\begin{array}{rcl} k_\infty^*/k_\infty^{*2} & \xrightarrow{\sim} & \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_q^*/\mathbb{F}_q^{*2} \cong (\mathbb{Z}/2\mathbb{Z})^2 \\ x & \longmapsto & (n \bmod 2,\ a_0 \bmod \mathbb{F}_q^{*2}). \end{array}$$

□

Proposition A.2.3 *Every non-trivial normal subgroup of $PGL_2(k_\infty)$ contains $PSL_2(k_\infty)$. In particular, $PGL_2(k_\infty)$ has no non-trivial discrete normal subgroups.*

Proof. Let $H \triangleleft \mathrm{PGL}_2(k_\infty)$ be a normal subgroup. Then $H \cap \mathrm{PSL}_2(k_\infty)$ is a normal subgroup of $\mathrm{PSL}_2(k_\infty)$, which is simple. Hence either $\mathrm{PSL}_2(k_\infty) \subset H$, in which case H is not discrete, or $H \cap \mathrm{PSL}_2(k_\infty) = \{1\}$. In the latter case, we get an embedding $H \hookrightarrow \mathrm{PGL}_2(k_\infty)/\mathrm{PSL}_2(k_\infty) \cong k_\infty^*/k_\infty^{*2} \cong (\mathbb{Z}/2\mathbb{Z})^2$. So it remains to show that $\mathrm{PGL}_2(k_\infty)$ has no normal subgroups isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$.

Firstly, every element $\alpha \in \mathrm{PGL}_2(k_\infty)$ of order 2 is of the form $\alpha = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$. Now suppose $H = \langle \alpha \rangle \cong \mathbb{Z}/2\mathbb{Z}$ is normal in $\mathrm{PGL}_2(k_\infty)$. Then

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a+c & -2a+b-c \\ c & -a-c \end{pmatrix} \in H,$$

which is impossible.

Next suppose $H = \langle \alpha_1, \alpha_2 \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$ is normal in $\mathrm{PGL}_2(k_\infty)$, and write

$$\alpha_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}.$$

Then $\alpha_1\alpha_2 = \alpha_2\alpha_1$, giving $a_1b_2 = a_2b_1$, $a_1c_2 = a_2c_1$ and $b_1c_2 = b_2c_1$. As H is normal, we must have (after renaming the elements of H, if necessary)

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ c_1 & -a_1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 + c_1 & -2a_1 + b_1 - c_1 \\ c_1 & -a_1 - c_1 \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ c_2 & -a_2 \end{pmatrix},$$

from which follow $c_1 = c_2 \Rightarrow a_1 = a_2$ and $b_1 = b_2$. But then $a_1 = c_1 = 0$, which is impossible.

□

Proposition A.2.4 *Let F be an infinite field such that F^*/F^{*2} is finite. Let H be a subgroup of finite index in $G = PGL_2(F)$. Then H contains $PSL_2(F)$ and is normal in G.*

Proof. G acts on the cosets G/H, giving a representation $\rho : G \to \mathrm{Aut}(G/H) \cong S_n$, where $n = (G : H)$. Let $K = \ker(\rho)$, then K lies in H, is a normal subgroup of G and ρ induces an embedding $G/K \hookrightarrow S_n$, hence $(G : K) \leq n!$.

Suppose that $K \cap \mathrm{PSL}_2(F) = \{1\}$. Then we would have an embedding $K \hookrightarrow \mathrm{PGL}_2(F)/\mathrm{PSL}_2(F) \cong F^*/F^{*2}$, which is impossible, as K is infinite. Hence K has non-trivial intersection with $\mathrm{PSL}_2(F)$, which is simple, hence K contains $\mathrm{PSL}_2(F)$.

To show that H is in fact normal (which we won't need), it suffices to point out that the groups lying between $\mathrm{PSL}_2(F)$ and $\mathrm{PGL}_2(F)$ are all of the form $H_C = \{\alpha \in \mathrm{PGL}_2(F) \mid \det(\alpha) \in C\}$ for some subgroup C of F^*/F^{*2}. These are all normal in G.

□

Corollary A.2.5 *Let $H < PGL_2(F)$ be a subgroup of finite index, and suppose H is simple. Then $H = PSL_2(F)$*

Proof. As H has finite index, it contains $\mathrm{PSL}_2(F)$, by Proposition A.2.4. The group $\mathrm{PSL}_2(F)$ is normal in $\mathrm{PGL}_2(F)$, hence also in H. But if H is simple then this must imply that $H = \mathrm{PSL}_2(F)$.

□

Corollary A.2.6 *Let $PSL_2(F) < H < PGL_2(F)$ and suppose $f : H \hookrightarrow PGL_2(F)$ is a monomorphism whose image has finite index in $PGL_2(F)$. Then $f(PSL_2(F)) = PSL_2(F)$, i.e. f restricts to an automorphism of $PSL_2(F)$.*

Proof. The image $K = f(\mathrm{PSL}_2(F))$ has finite index in $f(H)$, hence also in $\mathrm{PGL}_2(F)$, and is simple. From the above corollary follows that $K = \mathrm{PSL}_2(F)$.

□

We only need the above results for $F = k_\infty$.

A.3 Miscellanous

Proposition A.3.1 *Let R be a Euclidian ring. Then the group $PSL_2(R)$ is generated by the elements of the form $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\alpha_x = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ with $x \in R$.*

Proof. Let $G = \langle T, \alpha_x \mid x \in R \rangle$. Then G contains all the elements of the form

$$\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & q \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix}, \begin{pmatrix} q & -1 \\ 1 & 0 \end{pmatrix},$$

for all $q \in R$. Let $\alpha \in \mathrm{PSL}_2(R)$, then multiplying by the above elements performs elementary row and column operations on α. As R is Euclidian, we can find a sequence of row and column operations to reduce α to the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, which is clearly contained in G. Hence $G = \mathrm{PSL}_2(R)$. □

Proposition A.3.2 *Let G_1 be a subgroup of the topological group G_2, and let $H < G_1$ be a subgroup of finite index. Denote by $\overline{H}$ and $\overline{G_1}$ the (topological) closure of H and G_1, respectively, in G_2. Then $[\overline{G_1} : \overline{H}] \leq [G_1 : H]$.*

Proof. If $G_1 = \gamma_1 H \cup \cdots \cup \gamma_n H$, then $\overline{G_1} = \gamma_1 \overline{H} \cup \cdots \cup \gamma_n \overline{H}$. □

Proposition A.3.3 (Goursat's Lemma) *Let G_1 and G_2 be groups, and let H be a subgroup of $G_1 \times G_2$ such that the two projections $pr_i : H \to G_i$ are surjective. Then $K_1 = \ker(pr_1)$ can be considered as a normal subgroup of G_2, and K_2 as a normal subgroup of G_1. Then H is the inverse image of the graph of an isomorphism $\rho : G_1/K_2 \xrightarrow{\sim} G_2/K_1$.*

Proof. This result is well-known orally, but for lack of a suitable reference we prove it here.

$$\begin{aligned} \ker(pr_1) &= \{(g_1, g_2) \in H \mid g_1 = 1\} \\ &\cong \{g_2 \in G_2 \mid (1, g_2) \in H\} = K_1 \triangleleft G_2, \end{aligned}$$

and similarly $\ker(pr_2) \cong K_2 \triangleleft G_1$.

We define a map

$$\begin{aligned} \rho : G_1/K_2 &\longrightarrow G_2/K_1 \\ g_1 &\longmapsto g_2 \text{ with } (g_1, g_2) \in H. \end{aligned}$$

This map is well-defined: suppose $g_2' \in G_2$ is another element with $(g_1, g_2') \in H$, then $(1, g_2 {g_2'}^{-1}) \in H$, so $g_2 {g_2'}^{-1} \in K_1$, and g_2 and g_2' define the same element of G_2/K_1.

One checks easily that ρ is actually an isomorphism. Its graph is $\{(g_1, \rho(g_1)) \mid g_1 \in G_1/K_2\}$, whose preimage in $G_1 \times G_2$ is H. □

Proposition A.3.4 *Let F be a field. Then every automorphism of $PSL_2(F)$ is of the form $g \mapsto h g^\sigma h^{-1}$, where $h \in PGL_2(F)$ and $\sigma \in Aut(F)$.*

Proof. It follows from [38, Theorem 4] that every automorphism of $\mathrm{PSL}_2(F)$ is induced by an automorphism of $\mathrm{SL}_2(F)$. Then [38, Theorem 2] says that every automorphism of $\mathrm{SL}_2(F)$ is either of the form

$$g \mapsto \chi(g) h g^\sigma h^{-1},$$

where $h \in \mathrm{GL}_2(F)$, $\chi : \mathrm{SL}_2(F) \to F^*$ is a homomorphism and $\sigma \in \mathrm{Aut}(F)$, or of the form

$$g \mapsto \chi(g) h ({}^t g^{-1})^\sigma h^{-1},$$

where ${}^t g$ denotes the transpose of g. (Note that F is commutative, so automorphisms and anti-automorphisms of F are the same thing. Hua actually considered the more general case where F is a skew field).

As we are only interested in $\mathrm{PSL}_2(F)$ we may ignore the $\chi(g)$. It remains to verify that the map $g \mapsto {}^t g^{-1}$ is also an inner automorphism. Indeed,

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = {}^t \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}.$$

□

Lemma A.3.5 *Let A and B be infinite subgroups of a group G, and suppose that A has finite index in G. Then $A \cap B$ has finite index in B.*

Proof. Let $(G : A) = n$, then $G = \bigcup_{i=1}^n \alpha_i A$ for some $\alpha_1, \ldots, \alpha_n \in G$. Renumber the α's in such a way that $(\alpha_i A) \cap B \neq \emptyset$ iff $i \leq m$, for some $1 \leq m \leq n$. Choose some $\beta_i \in (\alpha_i A) \cap B$ for each $i = 1, \ldots, m$. Then

$$B = \bigcup_{i=1}^m (\alpha_i A) \cap B = \bigcup_{i=1}^m (\beta_i A) \cap B = \bigcup_{i=1}^m \beta_i (A \cap B)$$

and it follows that $(B : A \cap B) \leq m \leq n = (G : A)$.

□

Lemma A.3.6 *Let $A = \mathbb{F}_q[T]$, and denote by A^+ the additive group of A. Let $A_0^+ \subset A^+$ be a subgroup of finite index. Then the elements of A_0^+ generate all of $k = \mathbb{F}_q(T)$ as a field over $\mathbb{F}_q$.*

Proof. Choose representatives $P_1, \ldots, P_n$ of A^+/A_0^+. It suffices to prove that these representatives can be generated by elements of A_0^+. Now amongst any $n+1$ distinct elements $Q_1, \ldots, Q_{n+1}$ of A_0^+ there exists a pair $Q_i \neq Q_j$ such that $P_1 Q_i \equiv P_1 Q_j \bmod A_0^+$. Then $0 \neq P_1(Q_i - Q_j) \in A_0^+$, so we can get P_1 by dividing by $(Q_i - Q_j)$. Same for $P_2, \ldots, P_n$.

□

Appendix B

Heights of CM points on complex affine curves

This chapter appeared as an article in the *Ramanujan Journal* [8].

Abstract In this note we show that, assuming the generalized Riemann hypothesis for quadratic imaginary fields, an irreducible algebraic curve in $\mathbb{C}^n$ is modular if and only if it contains a CM point of sufficiently large height. This is an effective version of a theorem of Edixhoven.

Keywords complex multiplication, elliptic curves, modular curves, heights

B.1 Introduction

Yves André [3] proved that a curve in $\mathbb{C}^2$ is modular if and only if it has infinitely many CM points. Here a curve in $\mathbb{C}^2$ is said to be modular if it is the image of a modular curve $Y_0(N)$, under the map sending a pair (E_1, E_2) of isogenous elliptic curves to the point $(j(E_1), j(E_2))$ - this is not to be confused with modularity in the Shimura-Taniyama sense! For simplicity, we denote the image of $Y_0(N)$ in $\mathbb{C}^2$ by $Y_0'(N)$. This settled a special case of the André-Oort conjecture (see [2] and [20] for more details). Earlier, Bas Edixhoven [19] proved the same result under the assumption that the generalized Riemann hypothesis (GRH) holds for quadratic imaginary fields. The purpose of this note is to refine Edixhoven's result to obtain the following theorem:

Theorem B.1 *Assume GRH for quadratic imaginary fields. Let $d_1, \ldots, d_n, m$ be given positive integers. Then there exists an effectively computable constant $B = B(d_1, \ldots, d_n, m)$ such that the following holds. Let X be an irreducible algebraic curve in $\mathbb{C}^n$ defined over a number field of degree m over $\mathbb{Q}$, such that the degrees of the standard projections $X \to \mathbb{C}$ are $d_1, \ldots, d_n$, respectively. Then X is a modular curve Y_Γ if and only if X contains a CM point of height greater than B.*

Here a point $(x_1, \ldots, x_n) \in \mathbb{C}^n$ is CM if each x_i is the j-invariant of an elliptic curve with complex multiplication. Let $\mathfrak{H}$ denote the Poincaré upper

half-plane. The modular curves Y_Γ are given by $\{(j(\sigma_1(\tau)), \ldots, j(\sigma_n(\tau))) \mid \tau \in \mathfrak{H}\}$ for some[1] $(\sigma_1, \ldots, \sigma_n) \in GL_2(\mathbb{Q})^n$. Let $\Gamma := \cap_{i=1}^n \sigma_i^{-1} SL_2(\mathbb{Z})\sigma_i$, then we note that the curve Y_Γ is also given by $\Gamma \backslash \mathfrak{H}$, hence the notation.

The advantage of this result is that firstly we can treat curves in $\mathbb{C}^n$ rather than curves in $\mathbb{C}^2$ (this was actually already known to André and Edixhoven, and is in fact mentioned in [2]), and secondly, in order to show a curve is modular it suffices to find a CM point of sufficient height, rather than finding infinitely many CM points.

The reader is assumed familiar with the basics of elliptic curves over $\mathbb{C}$, but we recall some basic results on complex multiplication that will be needed in this paper. These results can be found for example in [41].

Let K be a quadratic imaginary field, and $L \subset K$ a lattice, then the set $\mathcal{O} := \{\lambda \in \mathbb{C} \mid \lambda L \subset L\}$ is called the order of L, and is in fact an order of K (i.e. a subring of finite index f of the ring of integers $\mathcal{O}_K$. f is called the conductor of $\mathcal{O}$). Every lattice $L \subset \mathbb{C}$ is homothetic to a lattice $\langle 1, \tau \rangle$, where τ lies in the fundamental domain $\mathcal{D} := \{z \in \mathfrak{H} \mid |z| \geq 1,\ -1/2 \leq \Re(z) \leq 1/2\}$. If τ lies in a quadratic imaginary field, then the order of $\langle 1, \tau \rangle$ is $\mathbb{Z}[D/2 + \sqrt{D}/2]$, where $D = \mathrm{Discr}(\tau)$, i.e. if $AX^2 + BX + C = 0$ is a minimal equation for τ in relatively prime integer coefficients, then $D = B^2 - 4AC$. Let $\mathcal{O}$ be an order in K, then an ideal $\mathfrak{a} \subset \mathcal{O}$ is called a proper $\mathcal{O}$-ideal if the order of $\mathfrak{a}$ (as a lattice) is $\mathcal{O}$. The group of proper $\mathcal{O}$-ideals modulo scalars is called the generalized ideal class group of $\mathcal{O}$, and denoted by $\mathrm{Pic}(\mathcal{O})$. This coincides with the usual class group if $\mathcal{O} = \mathcal{O}_K$.

We recall some results on the class numbers of quadratic imaginary fields. Let $\mathcal{O}_n$ be the order of discriminant $-n$ (i.e. write $n = df^2$, with f maximal with respect to the condition that $d \equiv 0$ or $1 \pmod 4$, then $\mathcal{O}_n$ is the order of conductor f in the quadratic imaginary field $\mathbb{Q}(\sqrt{-d})$). Note that such an order need not exist for each n, (e.g. $n = 2, 3, 6, 7, \ldots$). We define

$$h(-n) := \begin{cases} \#\mathrm{Pic}(\mathcal{O}_n) & \text{if } \mathcal{O}_n \text{ exists} \\ 0 & \text{otherwise.} \end{cases}$$

Theorem B.2 *Let n be such that $\mathcal{O}_n$ exists.*

1. $\log(h(-n)) \approx \frac{1}{2}\log(n)$. *The constants involved here are only effective if we assume GRH for quadratic imaginary fields.*
2. *For every $\epsilon > 0$ there exists an effecively computable constant C_ϵ such that $h(-n) \leq C_\epsilon n^{1/2+\epsilon}$.*

Here $f(x) \approx g(x)$ means that $\lim_{x\to\infty} f(x)/g(x) = 1$.

Proof Write $n = df^2$, as above. Then (1) is Siegel's theorem, which is well-known for $h(-d)$ (see [42]), and is easily extended to $h(-df^2)$ using the formula (see [41] or [52])

$$h(-df^2) = h(-d)w^{-1} f \prod_{p|f} (1 - p^{-1}\chi(p)),$$

[1]Throughout this chapter, one should replace $\mathrm{GL}_2(\mathbb{Q})$ by $\mathrm{GL}_2^+(\mathbb{Q})$.

where $w = 3$ if $d = 3$ and $f \geq 2$, $w = 2$ if $d = 4$ and $f \geq 2$ and $w = 1$ otherwise, and $\chi(p)$ is the Dirichelet character of p.

To show (2) we use the result, found in [52],

$$h(-d) \leq \pi^{-1} \log(d)\sqrt{d},$$

from which follows

$$\begin{aligned} h(-df^2) &\leq \pi^{-1} \log(d)\sqrt{d} f \prod_{p|f} (1 + \frac{1}{p}) \\ &\leq C_\epsilon (df^2)^{1/2+\epsilon}. \ \square \end{aligned}$$

Now let $E = \mathbb{C}/L$ be a CM elliptic curve, then $\mathcal{O} = \mathrm{End}(E)$ is an order in some quadratic imaginary field K, called the CM field of E, and $j(E)$ is an algebraic integer. Moreover, $K(j(E))$ is an abelian Galois extension of K, and $\mathrm{Gal}(K(j(E))/K) \cong \mathrm{Pic}(\mathcal{O})$. This isomorphism is canonical, so the conjugates of $j(E)$ are precisely the numbers of the form $j(\mathfrak{a}) := j(\mathbb{C}/\mathfrak{a})$, for proper $\mathcal{O}$-ideals $\mathfrak{a} \subset \mathcal{O}$. In particular, one of the conjugates is $j(\mathcal{O}) = j(D/2 + \sqrt{D}/2)$, which is in fact real.

Lastly, we define the absolute logarithmic height $h(x)$ of $x \in \bar{\mathbb{Q}}$, following [37]. Let k be a number field containing x. Then

$$h(x) := \frac{1}{[k : \mathbb{Q}]} \sum_{v \in M_k} \log(\max\{1, \|x\|_v\}),$$

where M_k is the set of places of k (the set of Archimedian places will be denoted by M_k^∞) and $\| \cdot \|_v$ is the normalized absolute value (satisfying the product formula) corresponding to the place v.

B.2 CM Heights

Let $x \in \mathbb{C}$ and define $H_{CM}(x) := |\mathrm{Discr}(\mathrm{End}(x))|$, i.e. the absolute value of the discriminant of the endomorphism ring of an elliptic curve of j-invariant x. We also define $H_{CM}(x) := \max\{H_{CM}(x_1), \ldots, H_{CM}(x_n)\}$ for $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$. We can view H_{CM} as a kind of height function on the CM points in $\mathbb{C}$ (or $\mathbb{C}^n$), and call it the CM height, as the number of CM points of bounded CM height is finite. We list below some of its properties.

Proposition B.2.1 *Let $x \in \mathbb{C}$.*

1. *x is CM if and only if $H_{CM}(x) > 1$.*
2. *H_{CM} is Galois invariant.*
3. *$\#\{x \in \mathbb{C} \mid 1 < H_{CM}(x) < n\} = O(n^{3/2+\epsilon})$, for all $\epsilon > 0$.*
4. *If x is CM then $\log[\mathbb{Q}(x) : \mathbb{Q}] = (1/2 + o(1)) \log H_{CM}(x)$.*
5. *Let h be the usual absolute logarithmic height on $\bar{\mathbb{Q}}$. Then there exists an effectively computable constant C such that if x is CM, $h(x) \leq \pi H_{CM}(x)^{1/2} + C$.*

Proof (1) and (2) are clear. Let x be a CM point, $\mathcal{O} = \mathrm{End}(x)$, $\mathrm{Discr}(\mathcal{O}) = -d$ and let K be its CM field. Then $[\mathbb{Q}(x) : \mathbb{Q}] = c[K(x) : K] = c\#\mathrm{Pic}(\mathcal{O})$, where $c = 1$ or 2, and now (4) follows from Theorem B.2. Further, x is a conjugate of $j(-d/2 + \sqrt{-d}/2)$, and as there are $\#\mathrm{Pic}(\mathcal{O})$ elements in this conjugacy class, it follows that there are $\#\mathrm{Pic}(\mathcal{O})$ points of CM height d. Thus we have

$$\begin{aligned} \#\{x \in \mathbb{C} \mid 1 < H_{CM}(x) < n\} &= \sum_{d=2}^{n-1} h(-d) \\ &= O(\sum_{d=2}^{n-1} d^{1/2+\epsilon}) \\ &= O(n^{3/2+\epsilon}), \end{aligned}$$

which proves (3).

To show (5) we need the following lemma.

Lemma B.2.2 *There exists an effectively computable constant C_1 such that if $\mathcal{O}$ is an order in a quadratic imaginary field with $|Discr(\mathcal{O})| \geq C_1$, then $|j(\mathcal{O})| \geq |j(\mathfrak{a})|$ for all proper $\mathcal{O}$-ideals $\mathfrak{a}$.*

Proof Let $D = \mathrm{Discr}(\mathcal{O})$ and let $\tau = D/2 + \sqrt{D}/2$, then $j(\mathcal{O}) = j(\tau)$. Let $\mathfrak{a} \subset \mathcal{O}$ be a proper $\mathcal{O}$-ideal. As a lattice, $\mathfrak{a}$ is homothetic to $\langle 1, \tau' \rangle$ for some $\tau' \in \mathcal{D}$. As the order of $\langle 1, \tau' \rangle$ is $\mathcal{O}$ it follows that $\mathrm{Discr}(\tau') = \mathrm{Discr}(\mathcal{O}) = \mathrm{Discr}(\tau) = D$. Let $A'x^2 + B'x + C' = 0$ be the minimal equation of τ', then $\Im(\tau') = \sqrt{-D}/2A' \leq \sqrt{-D}/2 = \Im(\tau)$. Note that if $A' = 1$ then $\tau' = -B'/2 + \sqrt{D}/2$ with $B' \equiv D \pmod 2$, giving $j(\tau') = j(\tau)$.

The q-expansion of the j-invariant is

$$j(\tau) = 1/q + 744 + \sum_{m=1}^{\infty} c_m q^m \qquad \text{where } q = \exp(2\pi i \tau).$$

As $|q| = \exp(-2\pi\Im(\tau))$ we see that for $\Im(\tau)$ sufficiently large we get $|j(\tau)| \approx |1/q| = \exp(2\pi\Im(\tau))$. Hence we can find a constant C_1 such that $|j(\mathfrak{a})| = |j(\tau')| \leq |j(\tau)| = |j(\mathcal{O})|$ for $\Im(\tau) \geq C_1$. Here we choose C_1 sufficiently large that $\Im(\tau) \mapsto |j(\tau)|$ is increasing for fixed $\Re(\tau)$. □

We now complete the proof of Proposition B.2.1. Let x be a CM point and let $k = \mathbb{Q}(x)$. Let $h(x)$ denote the absolute logarithmic height of x. As x is an algebraic integer it follows that

$$\begin{aligned} h(x) &= \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k^\infty} \log(\max\{1, ||x||_v\}) \\ &= \frac{1}{[k:\mathbb{Q}]} \sum_{\sigma : k \hookrightarrow \mathbb{C}} \log(\max\{1, |\sigma(x)|\}). \end{aligned}$$

Let $D = -H_{CM}(x)$. Then one of the conjugates of x is $j(D/2 + \sqrt{D}/2) \approx \exp(\pi\sqrt{|D|})$ (which is real), and from the lemma follows that all the other

conjugates have smaller absolute values (if $D \geq C_1$). Thus we get $h(x) \leq \pi H_{CM}(x)^{1/2} + C$. $\square$

B.3 Edixhoven's Result for $\mathbb{C}^2$

In [19] Edixhoven essentially proves the following result (he stated it in a slightly weaker form, but the following version does follow from his proof).

Theorem B.3 (Edixhoven) *Assume GRH for quadratic imaginary fields. Let d_1, d_2, m be given positive integers. Then there exists an effectively computable constant $B = B(d_1, d_2, m)$ such that the following holds. Let X be an irreducible algebraic curve in $\mathbb{C}^2$ defined over a number field of degree m over $\mathbb{Q}$, such that the degrees of the standard projections $X \to \mathbb{C}$ are d_1, d_2, respectively. Then $X = Y_0'(N)$ for some N if and only if X contains a CM point $(x_1, x_2) \in X$ with $H_{CM}(x_1, x_2) > B$.*

Proof outline Let X' be the union of the conjugates of X, so that X' is defined over $\mathbb{Q}$. Edixhoven first shows ([19, Proposition 3.1]) that for almost all CM points $(x_1, x_2) \in X'$ the CM fields of x_1 and x_2 coincide. He does this by showing that if the CM fields differ then

$$\log_2 \#\mathrm{Pic}(\mathrm{End}(x_i)) \leq \log_2(2md_i) + \#\{2 \neq p | \mathrm{Discr}(\mathrm{End}(x_i))\} + 10.$$

Then Siegel's theorem (which is effective, as we're assuming GRH) gives us an upper bound on $\mathrm{Discr}(\mathrm{End}(x_i)) = H_{CM}(x_i)$ depending on d_i and m.

He then goes on to show that if p is a prime which splits in an order $\mathcal{O} = \mathrm{End}(x_1) \cap \mathrm{End}(x_2)$, where $(x_1, x_2) \in X'$ is a CM point for which the CM fields coincide, and if $6d_1d_2(p+1)^2 < \#\mathrm{Pic}(\mathcal{O})$, then $X' \subset (T_p \times T_p)X'$, where $(T_p \times T_p)$ is a certain Hecke correspondence on $\mathbb{C}^2$. Now if $p_1, \ldots, p_t$ are sufficiently many such small split primes (i.e. if t is greater than some constant depending on $\min(d_1, d_2)$ and on m) then $X \subset (T_n \times T_n)X$, where $n = p_1 \ldots p_t$. It then follows ([19, Theorem 6.1]) that X is a modular curve.

The last hurdle is to show that there exist sufficiently many such small split primes. For this he uses an effective version of the Chebotarev Theorem (which requires GRH to be sharp enough), which gives us our primes, provided $\mathrm{Discr}(\mathcal{O}) = \mathrm{lcm}\{H_{CM}(x_1), H_{CM}(x_2)\}$ is sufficiently large.

So we see that the only two times Edixhoven used an infinity of CM points he really only needed one CM point of sufficiently large CM height. $\square$

Combining this result with part 5 of Proposition B.2.1, we see that we already have Theorem B.1 for $n = 2$.

B.4 Extending to $\mathbb{C}^n$

We now turn our attention to modular curves in $\mathbb{C}^n$. We define the set

$$Y_0(N_1, \ldots, N_{n-1}) \qu:= \quad \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid \text{There exist cyclic isogenies}$$

$$x_i \to x_{i+1} \text{ of degree } N_i \text{ for all } i = 1, \ldots, n-1\},$$

which is easily seen to be algebraic, defined by the ideal

$$\langle \Phi_{N_1}(X_1, X_2), \Phi_{N_2}(X_2, X_3), \ldots, \Phi_{N_{n-1}}(X_{n-1}, X_n) \rangle \subset \mathbb{Q}[X_1, \ldots, X_n],$$

where Φ_N is the modular polynomial defining $Y_0'(N)$ in $\mathbb{C}^2$ (see [41, chapter 5]). This set is also clearly a curve, though it is not in general irreducible.

Proposition B.4.1 *The irreducible components of $Y_0(N_1, \ldots, N_{n-1})$ are of the form Y_Γ.*

Proof Recall that $j(\tau)$ and $j(\tau')$ are isogenous if and only if $\tau' = \sigma(\tau)$ with $\sigma \in GL_2(\mathbb{Q})$. Thus a point $(x_1, \ldots, x_n) \in Y_0(N_1, \ldots, N_{n-1})$ is of the form $(j(\sigma_1(\tau)), j(\sigma_2(\tau)), \ldots, j(\sigma_n(\tau)))$, for some $\tau \in \mathfrak{H}$ and $A := (\sigma_1, \ldots, \sigma_n) \in GL_2(\mathbb{Q})^n$. Let

$$Y(A) := \{(j(\sigma_1(\tau)), \ldots, j(\sigma_n(\tau))) \mid \tau \in \mathfrak{H}\}.$$

It is clear on the one hand that $Y(A)$ is an irreducible component of $Y_0(N_1, \ldots, N_{n-1})$ and on the other hand that every irreducible component is of this form.

Let $\Gamma = \cap_{i=1}^n \sigma_i^{-1} SL_2(\mathbb{Z})\sigma_i$. We now show that $\Gamma \backslash \mathfrak{H} \to Y(A)$, induced by $\tau \mapsto (j(\sigma_1(\tau)), \ldots, j(\sigma_n(\tau)))$, is an isomorphism (hence the notation $Y_\Gamma := Y(A)$). The map $\mathfrak{H} \to Y(A)$ is clearly surjective. On the other hand, $\tau, \tau' \in \mathfrak{H}$ have the same image $\iff j(\sigma_i(\tau')) = j(\sigma_i(\tau))\ \forall i \iff \sigma_i(\tau') = \gamma_i(\sigma_i(\tau))$, $\gamma_i \in SL_2(\mathbb{Z})\ \forall i \iff \tau' = \gamma(\tau)$, $\gamma \in \Gamma$. This concludes the proof. □

Let $\pi_{ij} : \mathbb{C}^n \to \mathbb{C}^2$ denote the projection $(x_1, \ldots, x_n) \mapsto (x_i, x_j)$.

Proposition B.4.2 *Let X be an irreducible algebraic curve in $\mathbb{C}^n$, and fix some $1 \le i \le n$. Then the following are equivalent.*

1. *$X \subset Y_0(N_1, \ldots, N_{n-1})$ for some $(N_1, \ldots, N_{n-1}) \in \mathbb{Z}_{>0}^{n-1}$*
2. *$\pi_{ij}(X) = Y_0'(M_j)$, for some M_j, for all $j \neq i$.*

Proof (1) ⇒ (2). $\pi_{ij}(X)$ is an irreducible algebraic curve in $\mathbb{C}^2$ and consists of points of the form (x_i, x_j), where x_i and x_j are linked by an isogeny of degree at most $N_i N_{i+1} \cdots N_{j-1}$. Hence there exists some integer $M_j \le N_i N_{i+1} \cdots N_{j-1}$ such that infinitely many of these points lie on $Y_0'(M_j)$, which gives $\pi_{ij}(X) = Y_0'(M_j)$.

(2) ⇒ (1). Every point $(x_1, \ldots, x_n) \in X$ has the property that the x_i's are isogenous and that the isogenies involved have degree at most $\prod_{j \neq i} M_j$. Thus we must have $X \subset Y_0(N_1, \ldots, N_{n-1})$ for some $(N_1, \ldots, N_{n-1}) \in \mathbb{Z}_{>0}^{n-1}$. □

Theorem B.1 now follows easily. Pick B large enough that it works for each of the $\pi_{ij}(X)$'s. Now if $(x_1, \ldots, x_n)$ is a CM point of height larger than B, then we must have $h(x_i) > B$ for some i, and we just apply Proposition B.4.2 with

this i. $\square$

Similarly, combining Propositions B.4.1 and B.4.2 with André's result on curves in $\mathbb{C}^2$ we immediately get the following unconditional result.

Theorem B.4 *Let X be an irreducible algebraic curve in $\mathbb{C}^n$ such that none of the standard projections $X \to \mathbb{C}$ are constant. Then X is a modular curve Y_Γ if and only if X contains infinitely many CM points.*

Lastly, we point out that bounding the CM height (and thus the usual height) of the CM points on a variety is equivalent to bounding their number.

Theorem B.5 *Let X be an affine algebraic variety, defined over a number field k of degree m over $\mathbb{Q}$, containing a CM point x with $H_{CM}(x) = n$. Then X contains at least $h(-n)/m$ CM points.*

Proof Let X' be the union of all the conjugates of X, so X' is defined over $\mathbb{Q}$ and we can write X' as the union of at most m distinct conjugates X_i. Then X' contains all conjugates of x, of which there are at least $h(-n)$. Thus, one of the conjugates X_i will contain at least $h(-n)/m$ of these CM points. As this X_i is a conjugate of X, and conjugation preserves CM points, we in fact have at least $h(-n)/m$ CM points on X. $\square$.

Thus, if some affine variety X/k contains at most B_0 CM points, then we can find a constant B_1 (depending on B_0 and $[k : \mathbb{Q}]$) such that the CM points of X have CM heights bounded by B_1. For this we must choose B_1 such that $h(-B_1) \geq [k : \mathbb{Q}]B_0$. There exist effective lower bounds on $h(-n)$, for example using Goldfeld's theorem (see [51]), but they are not very sharp and rather hard to compute.

It would be nice to remove the assumption of GRH from the statement of Theorem B.1 using André's methods, but unfortunately, his constants seem to involve the actual coefficients of the curve, and not just the degrees.

Acknowledgments. Special thanks to Bas Edixhoven and Marc Hindry for their friendly help and useful comments.

Appendix C

Distinguished liftings and the André-Oort conjecture

This chapter is due to appear as an article in *Quaestiones Mathematica*. [9].

C.1 Introduction

Denote by $\overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, and by $\overline{\mathbb{F}}_p$ an algebraic closure of the finite field $\mathbb{F}_p$.

Let p be a prime number, and $\mathfrak{P}$ a place of $\overline{\mathbb{Q}}$ above p. Throughout the first five sections we will consider p and $\mathfrak{P}$ fixed. Now we can reduce mod $\mathfrak{P}$ those points of $\mathbb{A}^n(\overline{\mathbb{Q}})$ whose coordinates are algebraic integers, thus obtaining the points of $\mathbb{A}^n(\overline{\mathbb{F}}_p)$.

Conversely, every point in $\mathbb{A}^n(\overline{\mathbb{F}}_p)$ has many lifts to $\mathbb{A}^n(\overline{\mathbb{Q}})$. For some of these points $x \in \mathbb{A}^n(\overline{\mathbb{F}}_p)$ we will define a unique canonical lift x_0 of x to $\mathbb{A}^n(\overline{\mathbb{Q}})$. We then study the following lifting problem:

Let $X \subset \mathbb{A}^n_{\overline{\mathbb{F}}_p}$ be an irreducible affine algebraic variety defined over $\overline{\mathbb{F}}_p$, let $S \subset X(\overline{\mathbb{F}}_p)$ be a subset of points each of which possesses a canonical lift, and let $S_0 \subset \mathbb{A}^n(\overline{\mathbb{Q}})$ denote the set of canonical lifts of these points. Then an irreducible affine algebraic variety $X_0 \subset \mathbb{A}^n_{\overline{\mathbb{Q}}}$ defined over $\overline{\mathbb{Q}}$ and which reduces to X mod $\mathfrak{P}$ is called a distiguished lifting of X with respect to S if $S_0 \subset X_0(\overline{\mathbb{Q}})$. We sometimes also say that X_0 is a distinguished lifting of (X, S). We will use this notation throughout the paper, the subscript 0 can be understood as meaning "characteristic 0".

Here we require the lifting to be sufficiently "nice". In particular, it must have the following properties. Reduction mod $\mathfrak{P}$ must preserve the dimensions of closed subvarieties, so that, for example, S Zariski-dense in $X(\overline{\mathbb{F}}_p)$ implies S_0 Zariski-dense in $X_0(\overline{\mathbb{Q}})$. It must also preserve degrees, whenever defined. In this paper we deal in particular with affine curves and hypersurfaces, where the definition of degree is clear.

One can then study the existence and uniqueness of distinguished liftings. Some uniqueness results are immediate. For example, if S_0 is Zariski-dense in $X_0(\overline{\mathbb{Q}})$, or if X is a curve and $\#S > (\deg(X))^2$, then any distinguished lifting

X_0 of (X, S), if it exists, is unique. This follows because, if X_0' denotes another distinguished lifting, $S_0 \subset X_0'(\overline{\mathbb{Q}}) \cap X_0(\overline{\mathbb{Q}})$, and the intersection is improper.

We will describe below the notion of canonical lifts which we will use in this paper.

We start by viewing $\mathbb{A}^n$ as the moduli space of products of n elliptic curves. A point $(x_1, \ldots, x_n)$ in $\mathbb{A}^n(\overline{\mathbb{F}}_p)$ (respectively in $\mathbb{A}^n(\overline{\mathbb{Q}})$) then corresponds to the isomorphism class of a product of elliptic curves $E_1 \times \cdots \times E_n$ defined over $\overline{\mathbb{F}}_p$ (respectively $\overline{\mathbb{Q}}$) with $x_i = j(E_i)$ for $i = 1, \ldots, n$.

If the j-invariant of an elliptic curve over $\overline{\mathbb{Q}}$ is integral, then its $\overline{\mathbb{Q}}$-isomorphism class contains an elliptic curve with good reduction at $\mathfrak{P}$, and the reduction mod $\mathfrak{P}$ of this j-invariant then corresponds to the isomorphism class of the reduced curve.

An elliptic curve E over $\overline{\mathbb{F}}_p$ is said to be ordinary if $E[p] \cong \mathbb{Z}/p\mathbb{Z}$. Otherwise it is called supersingular, in which case $E[p] = 0$. There are only finitely many isomorphism classes of supersingular elliptic curves (remember that p is fixed), and in fact their j-invariants all lie in $\mathbb{F}_{p^2}$. A point $(x_1, \ldots, x_n)$ is called ordinary if each x_i is the j-invariant of an ordinary elliptic curve.

Now Deuring has shown (see [41, Chapter 13]), that an ordinary elliptic curve E over $\overline{\mathbb{F}}_p$ has a unique lift (called the canonical lift) to an elliptic curve E_0 defined over $\overline{\mathbb{Q}}$, such that $\mathrm{End}(E) \cong \mathrm{End}(E_0)$. In particular it follows that the canonical lift E_0 has complex multiplication (CM), and hence $j(E_0)$ is integral.

To sum up, let $(x_1, \ldots, x_n) \in \mathbb{A}^n(\overline{\mathbb{F}}_p)$ be an ordinary point, then we define its canonical lift to be $(x_1', \ldots, x_n') \in \mathbb{A}^n(\overline{\mathbb{Q}})$, where x_i' is Deuring's canonical lift of x_i. (By a slight abuse of notation we will often identify an elliptic curve with its j-invariant when this does not cause confusion.)

Of course, one can also define other notions of "canonical" lifts, or consider more general algebraic varieties, provided one has a working notion of reduction mod $\mathfrak{P}$, and study the corresponding distiguished lifting problems (see also Section 3).

We recall that if E is a CM elliptic curve, then $\mathrm{End}(E)$ is an order in the quadratic imaginary field $K = \mathrm{End}_{\mathbb{Q}}(E) := \mathrm{End}(E) \otimes \mathbb{Q}$, called the CM field of E. So we may write $\mathcal{O} = \mathrm{End}(E) = \mathbb{Z} + f\mathcal{O}_K$, where f is called the conductor of $\mathcal{O}$. If E is the canonical lift of its reduction mod $\mathfrak{P}$, then p splits in K and does not divide f, in which case we say that p splits in $\mathcal{O}$.

See [62] and [41] for references to elliptic curves and complex multiplication, respectively.

In Section 2 we see how far we can go with elementary methods. In section 3 we show how the study of distinguished liftings leads naturally to the André-Oort conjecture, and consider the generalisation from products of elliptic curves to abelian varieties. In section 4 we continue again with products of elliptic curves and show that modular varieties can be lifted. In section 5 we state some obstructions for non-modular varieties, these can be considered to be the main results of this paper. These results are then proved in the last two sections, where we obtain some results on the André-Oort conjecture itself, treating curves in section 6 and hypersurfaces in section 7.

C.2 Applying linear algebra

We first want to see under which conditions we can find distinguished liftings by elementary means. We expect this to be easier if the set S is small, and the field we lift into is large.

Let K be a number field with ring of integers $\mathcal{O}_K$ and residue field $\mathbb{F}_q$ at the prime $\mathfrak{p} = \mathfrak{P} \cap K$. Let S be a finite set of ordinary points in $X(\overline{\mathbb{F}}_p)$ and let $S_0 = \{x_1, \ldots, x_t\}$, with $x_k = (x_{k1}, \ldots, x_{kn}) \in \mathbb{A}^n(\overline{\mathbb{Q}})$ be the set of canonical lifts of the points of S. Let $L = K(x_1, \ldots, x_t)$ be a field of definition for the points in S_0. In this section we will construct, under suitable conditions, distinguished liftings of (X, S) into L.

Suppose X is defined in $\mathbb{A}^n_{\mathbb{F}_q}$ by the m polynomials

$$f_i(X_1, \ldots, X_n) = \sum_{(j_1,\ldots,j_n)\in J_i} \bar{a}^{(i)}_{j_1,\ldots,j_n} X_1^{j_1} X_2^{j_2} \cdots X_n^{j_n} \in \mathbb{F}_q[X_1, \ldots, X_n]$$

for $i = 1, \ldots, m$, where $J_i \subset \mathbb{Z}^n$ is the set of those indices for which $\bar{a}^{(i)}_{j_1,\ldots,j_n} \neq 0$.

Now consider the system of linear equations in $\overline{\mathbb{Q}}$,

$$\sum_{(j_1,\ldots,j_n)\in J_i} a^{(i)}_{j_1,\ldots,j_n} x_{k1}^{j_1} x_{k2}^{j_2} \cdots x_{kn}^{j_n} = 0 \qquad i = 1, \ldots, m; \quad k = 1, \ldots, t \tag{C.1}$$

where the $a^{(i)}_{j_1,\ldots,j_n}$ are the variables. These equations have a solution mod $\mathfrak{P}$ (namely $\{\bar{a}^{(i)}_{j_1,\ldots,j_n}\}$), and we want to determine under which conditions we can lift this solution to $\overline{\mathbb{Q}}$. Once we have such a solution $\{a^{(i)}_{j_1,\ldots,j_n}\}$, then the polynomials

$$F_i(X_1, \ldots, X_n) = \sum_{(j_1,\ldots,j_n)\in J_i} a^{(i)}_{j_1,\ldots,j_n} X_1^{j_1} X_2^{j_2} \cdots X_n^{j_n} \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$$

define a distinguished lifting X_0 of (X, S).

So we must now investigate lifting solutions of linear equations from characteristic p to characteristic 0. This would seem like a case for Hensel's Lemma, but as the equations are linear, we can solve this more directly (and in particular we don't need our field to be complete).

Fix i, $1 \leq i \leq m$, and let M_i be the $t \times \#J_i$ matrix of coefficients of the system of equations (C.1). Denote by $\overline{M_i}$ the reduction of M_i mod $\mathfrak{P}$. We claim that a solution to $\overline{M_i}$ (i.e. to the equation (C.1) with coefficients reduced mod $\mathfrak{P}$) can be lifted to a solution of M_i if $\operatorname{rank}(M_i) = \operatorname{rank}(\overline{M_i})$. To simplify our notation, we state this as a proposition.

Proposition C.2.1 *Let L be a number field with ring of integers $\mathcal{O}_L$, $\mathfrak{P}$ a prime in $\mathcal{O}_L$ and $\mathcal{O}_L/\mathfrak{P} = \mathbb{F}_q$. Let $M = (c_{ij})$ be an $m \times n$ matrix with coefficients in $\mathcal{O}_L$, and denote by $\overline{M}$ its reduction mod $\mathfrak{P}$. Let $X = {}^t(X_1, \ldots, X_n)$. Then every solution to $\overline{M}X = 0$ in $\mathbb{F}_q^n$ can be lifted to a solution of $MX = 0$ in L^n if and only if rank(M) = rank$(\overline{M})$.*

Proof. Suppose $\mathrm{rank}(M) = \mathrm{rank}(\overline{M}) = r$, and let $\overline{x} = {}^t(\overline{x_1}, \ldots, \overline{x_n})$ be a solution to $\overline{M}X = 0$. Then $\overline{M}X = 0$ is equivalent to a subsystem with r equations, whose $r \times n$ matrix of coefficients must have an invertible $r \times r$ submatrix, denoted by $\overline{M'}$. We may assume without loss of generality that $\overline{M'}$ consists of the first r columns of the first r rows of $\overline{M}$. Then ${}^t(\overline{x_1}, \ldots, \overline{x_r})$ is the unique solution to

$$\overline{M'} \begin{bmatrix} X_1 \\ \vdots \\ X_r \end{bmatrix} = \begin{bmatrix} \overline{c}_{r+1,1}\overline{x_{r+1}} & + \cdots + & \overline{c}_{n,1}\overline{x_n} \\ \vdots & & \vdots \\ \overline{c}_{r+1,r}\overline{x_{r+1}} & + \cdots + & \overline{c}_{n,r}\overline{x_n} \end{bmatrix}. \tag{C.2}$$

Let M' be the submatrix of M corresponding to $\overline{M'}$. As we always have $\mathrm{rank}(M') \geq \mathrm{rank}(\overline{M'})$, it follows that $\mathrm{rank}(M') = r$. Pick any lifting $(x_{r+1}, \ldots, x_n)$ of $(\overline{x_{r+1}}, \ldots, \overline{x_n})$. Then the system

$$M' \begin{bmatrix} X_1 \\ \vdots \\ X_r \end{bmatrix} = \begin{bmatrix} c_{r+1,1}x_{r+1} & + \cdots + & c_{n,1}x_n \\ \vdots & & \vdots \\ c_{r+1,r}x_{r+1} & + \cdots + & c_{n,r}x_n \end{bmatrix}.$$

has a unique solution $(x_1, \ldots, x_r)$, which must reduce to the unique solution of (C.2) mod $\mathfrak{P}$. Hence $x = {}^t(x_1, \ldots, x_n)$ is a solution to $MX = 0$ and reduces to $\overline{x}$ mod $\mathfrak{P}$.

Conversely, suppose that $\mathrm{rank}(M) > \mathrm{rank}(\overline{M})$. Then the solution space $\overline{V}$ of $\overline{M}X = 0$ has dimension strictly larger than the space V of solutions to $MX = 0$, so the reduction map $V \to \overline{V}$ cannot be surjective.

□

Now we can apply Propostion C.2.1 to the equations (C.1) and obtain a distinguished lifting of (X, S) into the number field L, provided that the ranks of the matrices M_i are stable under reduction mod $\mathfrak{P}$.

One feels that this last condition should be true for "most" sets S of ordinary points. For example, if S consists of only one point $S = \{(\overline{x_1}, \ldots, \overline{x_n})\}$, then this condition is satisfied if none of the $\overline{x_i}$'s is 0.

It remains to investigate when this lifting is "sufficiently nice", as required in the introduction.

It is clear that if X is defined by a single equation (i.e. the case of plane curves and hypersurfaces) then this lifting preserves degrees, as in fact we have not introduced any new monomials into the equations defining X_0. On the other hand, we require that reduction mod $\mathfrak{P}$ preserve the dimensions of subvarieties, in particular we want $\dim(X) = \dim(X_0)$. This is far from automatic, and in general one only has $\dim(X) \geq \dim(X_0)$. Indeed, as we have seen with Proposition C.2.1, this can already break down for linear varieties. We will not solve this problem in general, but only note that at least if X is a complete intersection (e.g. a hypersurface) then we will have $\dim(X) = \dim(X_0)$, because then $\dim(X) = n - m \leq \dim(X_0) \leq \dim(X)$. So for complete intersections X at least, provided the matrices M_i satisfy the rank conditions above, a distinguished lifting of (X, S) into the field L does exist.

We briefly mention that, in a more technical language, one would require $\mathcal{X} = \mathrm{Spec}(R[X_1, \ldots, X_n]/\langle F_1, \ldots, F_m\rangle)$ to be flat as a scheme over $\mathrm{Spec}(R)$, where R is the localisation of $\mathcal{O}_K$ at $\mathfrak{p}$. Then X is the special fibre and X_0 the generic fibre of $\mathcal{X}$, and we get $\dim(X) = \dim(X_0)$, amongst other things. See [32, III.9] for more details, and [37, A.9] for a brief account of reduction mod p in scheme-theoretic language.

So far, our arithmetic definition of canonical lifts has not yet entered the picture, and the above results apply for an arbitrary notion of "canonical lift". So we expect things to become more interesting when S is infinite or the field we lift into is smaller than L. Indeed, the purpose of this article is to show how arithmetical phenomena lead to lifts of modular varieties into the field $\mathbb{Q}$ on the one hand, and to obstructions to lifts of non-modular varieties into small fields on the other hand.

C.3 The André-Oort conjecture

What happens if the set S is large? Suppose that S is Zariski-dense in the irreducible algebraic variety $X \subset \mathbb{A}^n_{\overline{\mathbb{F}}_p}$. If (X, S) has a distingushed lifting $X_0 \subset \mathbb{A}^n_{\overline{\mathbb{Q}}}$, then X_0 will have a Zariski-dense set of CM points, i.e. points whose coordinates are j-invariants of CM elliptic curves. But the André-Oort conjecture states that this is only possible if X_0 is modular.

Before giving a more precise statement of this conjecture, we shall first place ourselves in a more general situation.

Let A be an abelian variety of dimension g defined over $\overline{\mathbb{F}}_p$. We say that A is ordinary if $A[p] \cong (\mathbb{Z}/p\mathbb{Z})^g$. In that case there exists a lift A_0 of A to $\overline{\mathbb{Q}}$, called the Serre-Tate canonical lift, which has the property that $\mathrm{End}(A_0) \cong \mathrm{End}(A)$ (see [44] or [54]). If $g = 1$ then this is just Deuring's lift.

An abelian variety A is said to have complex multiplication if $\mathrm{End}_{\mathbb{Q}}(A)$ contains a commutative semi-simple $\mathbb{Q}$-algebra R with $[R : \mathbb{Q}] = 2\dim(A)$ (so in some sense $\mathrm{End}_{\mathbb{Q}}(A)$ is as large as possible). In particular, any abelian variety A over $\overline{\mathbb{F}}_p$ has CM (first proved by Tate) and so the Serre-Tate canonical lift of an ordinary A also has CM.

Let $\mathcal{A}$ be some moduli space of abelian varieties, so the points of $\mathcal{A} \otimes \overline{\mathbb{F}}_p$ (respectively $\mathcal{A} \otimes \overline{\mathbb{Q}}$) correspond to isomorphism classes of abelian varieties over $\overline{\mathbb{F}}_p$ (respectively $\overline{\mathbb{Q}}$). Then for an ordinary point $x \in \mathcal{A}(\overline{\mathbb{F}}_p)$ we let $x_0 \in \mathcal{A}(\overline{\mathbb{Q}})$ correspond to the Serre-Tate canonical lift of (an abelian variety corresponding to) x, and call it the canonical lift of x.

Now for subvarieties $X \subset \mathcal{A}$ which behave well under reduction mod $\mathfrak{P}$ we can also define distinguished liftings as in Section 1. In fact, if we let $\mathcal{A} = \mathbb{A}^g$, the moduli space of products of g elliptic curves, then we are back at our original notion.

Conjecture C.1 (André-Oort) *Let X be a subvariety of a moduli space $\mathcal{A}$ of abelian varieties over $\mathbb{C}$, and suppose $X(\mathbb{C})$ contains a Zariski-dense set of CM points. Then X is a Shimura subvariety of $\mathcal{A}$.*

For a precise technical definition of Shimura subvarieties, also known as subvarieties of Hodge type, we refer the reader to [47]. For $\mathcal{A}_g \otimes \mathbb{C}$, the moduli space of principally polarised complex abelian varieties of dimension g, the Shimura subvarieties are easy to describe. Let $\mathfrak{H}_g$ denote Siegel's upper half space, on which the symplectic group $\mathrm{Sp}_{2g}(\mathbb{R})$ acts transitively. Then we can write $\mathcal{A}_g(\mathbb{C}) \cong \mathrm{Sp}_{2g}(\mathbb{Z}) \backslash \mathfrak{H}_g$ (see [43]). Now a subvariety $S \subset \mathcal{A}_g \otimes \mathbb{C}$ is called a Shimura subvariety if and only if there exists an algebraic subgroup G of Sp_{2g}, defined over $\mathbb{Q}$, such that $S(\mathbb{C})$ is an irreducible component of the image in $\mathcal{A}_g$ of the $G(\mathbb{R})$-orbit of a CM point in $\mathfrak{H}_g$. So a CM point is a Shimura subvariety of dimension zero.

It follows easily from the fact that $G(\mathbb{Q})$ is dense in $G(\mathbb{R})$ that the CM points are dense in $S(\mathbb{C})$ for the analytic topology, hence also for the Zariski topology, as was first pointed out by Mumford [50]. As CM points are defined over $\overline{\mathbb{Q}}$ it follows that S is also defined over $\overline{\mathbb{Q}}$. So it makes sense to talk about the Shimura subvarieties of $\mathcal{A} \otimes \overline{\mathbb{Q}}$.

If $X \subset \mathcal{A} \otimes \overline{\mathbb{F}}_p$ then we call it a Shimura subvariety if it is the reduction mod $\mathfrak{P}$ of a Shimura subvariety of $\mathcal{A} \otimes \overline{\mathbb{Q}}$.

There is a more general statement in terms of abstract Shimura varieties, in fact Conjecture C.1 was first stated (as a problem) for curves in a general Shimura variety by André [1, X.4] in 1989 and (independently) in roughly the above form by Oort ([54], see also [47]) in 1994. For a good reference for abelian varieties, see [37].

One partial result is the following theorem of Moonen [47, 49]:

Theorem C.2 (Moonen) *Let $\mathcal{A}_g$ be the moduli space of principally polarised abelian varieties of dimension g. Let $X \subset \mathcal{A}_g \otimes \overline{\mathbb{Q}}$ be a subvariety containing a Zariski-dense set of CM points, each of which is the Serre-Tate canonical lift of its reduction mod $\mathfrak{p}$, where $\mathfrak{p}$ is a prime lying above the fixed rational prime p. Then X is a Shimura subvariety of $\mathcal{A}_g$.*

We remark that Moonen originally stated this for $\mathcal{A} = \mathcal{A}_{g,1,n}$, the moduli space of principally polarised abelian varieties with level n structure, $n \geq 3$, but as Edixhoven has pointed out (e.g. in [21]), we can safely ignore any level structures.

Other partial results have been found by André, Belhaj-Dahmane, Edixhoven and Yafaev [2, 3, 6, 19, 20, 21, 22, 71, 72].

Luckily we don't need the full strength of Conjecture C.1, we just need Theorem C.2, as our CM points are already Serre-Tate canonical lifts for some fixed prime, by construction. So we get our first obstruction result:

Corollary C.3.1 *Let $\mathcal{A}_g$ be the moduli space of principally polarised abelian varieties of dimension g. Let $X \subset \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ be a subvariety, and $S \subset X(\overline{\mathbb{F}}_p)$ a Zariski-dense set of ordinary points. Then X has a distinguished lifting $X_0 \subset \mathcal{A}_g \otimes \overline{\mathbb{Q}}$ with respect to S only if X is Shimura subvariety.*

C.4 Lifting modular varieties

We now return to the special case where $\mathcal{A} = \mathbb{A}^n$, the moduli space of products of elliptic curves. As products of elliptic curves are principally polarised abelian varieties, the case where S is Zariski-dense in $X(\overline{\mathbb{F}}_p)$ is included in Corollary C.3.1. Note that, strictly speaking, $\mathcal{A} = \mathbb{A}^n/S_n$ (S_n is the group of permutations on n letters) is the "true" moduli space of products of n elliptic curves, as permuting the coordinates preserves the isomorphism class. However, the notions of CM points and Shimura subvarieties are preserved by the canonical map $\mathbb{A}^n \to \mathbb{A}^n/S_n$.

The Shimura subvarieties of $\mathbb{A}^n_{\mathbb{C}}$, which we refer to as modular varieties, can be described, up to permutation of coordinates, as products of CM points, affine lines $\mathbb{A}^1_{\mathbb{C}}$ and modular curves in $\mathbb{A}^r_{\mathbb{C}}$.

A modular curve in $\mathbb{A}^r_{\mathbb{C}}$ is the image of the upper halfplane $\mathfrak{H}$ under the map $\tau \mapsto (j(g_1(\tau)), \ldots, j(g_r(\tau)))$, for some $(g_1, \ldots, g_r) \in GL_2^+(\mathbb{Q})^r$. In particular, the modular curves in $\mathbb{A}^2$ are the images $Y_0'(N)$ of the modular curves $Y_0(N)$, under the map sending the pair of isogenous elliptic curves (E_1, E_2) to the point $(j(E_1), j(E_2))$.

We now give another characterisation of modular curves in $\mathbb{A}^n_{\mathbb{C}}$, which we will need below. Define

$$\begin{aligned} Y_0(N_1, \ldots, N_{n-1}) &= \{(x_1, \ldots, x_n) \mid \text{there exist cyclic isogenies} \\ &\qquad x_i \to x_{i+1} \text{ of degree } N_i \text{ for } i = 1, \ldots, n-1\}. \end{aligned}$$

$Y_0(N_1, \ldots, N_{n-1})$ is algebraic, given by the ideal

$$\langle \Phi_{N_1}(X_1, X_2), \Phi_{N_2}(X_2, X_3), \ldots, \Phi_{N_{n-1}}(X_{n-1}, X_n) \rangle \subset \mathbb{Q}[X_1, \ldots, X_n],$$

where Φ_N is the polynomial defining the curve $Y_0'(N)$. It is known (see e.g. [8]), that a curve $X \subset \mathbb{A}^n_{\mathbb{C}}$ is modular if and only if it is an irreducible component of $Y_0(N_1, \ldots, N_{n-1})$, where each N_i satisfies $\pi_{i,i+1}(X) = Y_0'(N_i)$, and $\pi_{i,j}$ is the projection onto the ith and jth coordinates.

$Y_0(N_1, \ldots, N_{n-1})$ can also be described as the moduli space of tuples $(E, C_1, C_2, \ldots, C_{n-1})$, where E is an elliptic curve and the C_i's are nested subgroups of E satisfying $C_{i+1}/C_i \cong \mathbb{Z}/N_i\mathbb{Z}$ for $i = 1, \ldots, n-1$. The equivalence is given by $x_1 = j(E)$ and $x_i = j(E/C_{i-1})$ for $i = 2, \ldots, n$.

Next we want to describe the irreducible components of $Y_0(N_1, \ldots, N_{n-1})$. Let $G_1 \subset \cdots \subset G_{n-1}$ be subgroups of $(\mathbb{R}/\mathbb{Z})^2$ satisfying $G_{i+1}/G_i \cong \mathbb{Z}/N_i\mathbb{Z}$ for $i = 1, \ldots, n-1$, and define the subset

$$\begin{aligned} Y_0(G_1, \ldots, G_{n-1}) &= \{(j(E), j(E/C_1), \ldots, j(E/C_{n-1})) \mid \text{there exists an} \\ &\qquad \text{isomorphism of abstract groups } \phi : E(\mathbb{C}) \to (\mathbb{R}/\mathbb{Z})^2 \\ &\qquad \text{such that } \phi(C_i) = G_i \text{ for } i = 1, \ldots, n-1\} \\ &\subset Y_0(N_1, \ldots, N_{n-1}). \end{aligned}$$

We claim that these are precisely the irreducible components. To prove this we must show that $Y_0(G_1, \ldots, G_{n-1})$ is irreducible. Consider the map

$$\begin{aligned} \Theta : \mathfrak{H} &\longrightarrow Y_0(G_1, \ldots, G_{n-1}) \\ \tau &\longmapsto (j(E_\tau), j(E_\tau/G_1(\tau)), \ldots, j(E_\tau/G_{n-1}(\tau))), \end{aligned}$$

where $E_\tau = \mathbb{C}/\langle 1, \tau\rangle \cong (\mathbb{R}/\mathbb{Z})^2$ and $G_i(\tau)$ is just the preimage of $G_i \subset (\mathbb{R}/\mathbb{Z})^2$ under this isomorphism. Θ is surjective, and if we let

$$\Gamma = \{\sigma \in SL_2(\mathbb{Z}) \mid j(E_\tau/G_i(\tau)) = j(E_\tau/G_i(\sigma(\tau))) \ \ \forall \tau \in \mathfrak{H}, i = 1, \ldots, n-1\}$$

then Θ induces an isomorphism of Riemann surfaces $Y_0(G_1, \ldots, G_{n-1}) \cong \Gamma \backslash \mathfrak{H}$. In particular, $Y_0(G_1, \ldots, G_{n-1})$ is irreducible.

Now we can show that distinguished liftings of modular varieties always exist.

Proposition C.4.1 *Let $X \subset \mathbb{A}^n_{\overline{\mathbb{F}}_p}$ be the reduction mod $\mathfrak{P}$ of a modular variety $X_0 \subset \mathbb{A}^n_{\overline{\mathbb{Q}}}$, suppose X is irreducible and $S \subset X(\overline{\mathbb{F}}_p)$ any set of ordinary points. Then X_0 is a distinguished lifting of (X, S).*

Proof. We will show that if $(x_1, \ldots, x_n) \in X(\overline{\mathbb{F}}_p)$ is an ordinary point, then its canonical lift $(x_1', \ldots, x_n')$ lies in $X_0(\overline{\mathbb{Q}})$. As modular varieties in $\mathbb{A}^n$ are products of CM points, affine lines and modular curves, and the assertion is trivial for CM points and affine lines, it suffices to prove the assertion for modular curves.

Let $X_0 = Y_0(G_1, \ldots, G_{n-1}) \subset Y_0(N_1, \ldots, N_{n-1})$, and suppose the point $(x_1', \ldots, x_n')$ corresponds to the tuple $(E, C_1, \ldots, C_{n-1})$. We note that p does not divide any N_i, for otherwise the reduction mod $\mathfrak{P}$ of $\pi_{i,i+1}(X_0) = Y_0'(N_i)$ would be reducible, whereas X is irreducible. So the subgroups C_i all belong to the p-primary part of the torsion group of E, which is isomorphic to the p-primary part of the torsion group of $\overline{E}$, the reduction mod $\mathfrak{P}$. It follows that the canonical lift of an ordinary point $(\overline{E}, \overline{C}_1, \ldots, \overline{C}_{n-1}) \in \overline{Y}_0(G_1, \ldots, G_{n-1})(\overline{\mathbb{F}}_p)$ lies in $Y_0(G_1, \ldots, G_{n-1})(\overline{\mathbb{Q}})$.

□

Hence for the case where $\mathcal{A} = \mathbb{A}^n$, we can replace "only if" in Corollary C.3.1 by "if and only if". For other moduli spaces $\mathcal{A}$ one can do the same thing for Shimura subvarieties that can be characterised purely by level structure, but it is not clear that this holds for arbitrary Shimura subvarieties.

C.5 Obstructions

From now on we're interested in finding obstructions to distinguished liftings. Corollary C.3.1 gives us an obstruction if S is Zariski-dense and X non-modular. Now we try to find obstructions (notably the condition that X is non-modular) for finite S. We have seen in Section 2 that a distinguished lifting will often exist if we allow liftings into large fields, so our strategy will be to bound the degree of the lifting field.

Suppose X is a curve. Intuitively, given a finite set S_0 of points in $\mathbb{A}^n(\overline{\mathbb{Q}})$, one can always construct a curve X_0 containing S_0. But this curve might have a large degree, or be defined over a large field, unless the points in S_0 belong "naturally" to a simple curve. The philosophy of the André-Oort conjecture is that the only curves which contain CM points in a natural way are modular curves. In fact André has proved that the only curves in $\mathbb{A}^n_{\mathbb{C}}$ containing infinitely

many CM points are precisely the modular curves (see [2], [3] and [19]). One can also obtain effective results, giving upper bounds for the heights of CM points on non-modular curves, as we shall see in the next sections.

Using these ideas we shall obtain the following results in the next sections, which form the heart of this paper. But first, we introduce some notation and conventions:

The CM height is defined as $H_{CM}(x) := |\mathrm{Discr}(\mathrm{End}(x))|$ for an ordinary point $x \in \overline{\mathbb{F}}_p$ or a CM point $x \in \overline{\mathbb{Q}}$, and $H_{CM}(x_1, \ldots, x_n) := \max\{H_{CM}(x_1), \ldots, H_{CM}(x_n)\}$. Note that the usual arithmetic height of $x \in \overline{\mathbb{Q}}$ is bounded in terms of the CM height ([8], see also [14]).

UTPC means "up to permutation of coordinates", i.e. that said statement is true modulo a possible permutation of the coordinates of the point(s) involved.

GRH stands for the generalised Riemann hypothesis for quadratic imaginary fields.

If L/K is a Galois extension and $\mathfrak{p}$ a prime of L, then we denote by $(\mathfrak{p}, L/K)$ the Frobenius element in $\mathrm{Gal}(L/K)$ corresponding to $\mathfrak{p}$.

Theorem C.3 *Assume GRH. Then there exists an effectively computable function $B_1 : \mathbb{N}^3 \to \mathbb{N}$, satisfying $B_1(n, d, h) \to \infty$ as $h \to \infty$ for any fixed n, d, such that the following holds. Let X be an irreducible algebraic curve in $\mathbb{A}^n_{\overline{\mathbb{F}}_p}$, for which none of the standard projections $X \to \mathbb{A}^1$ is constant, and $x \in X(\overline{\mathbb{F}}_p)$ an ordinary point. Suppose that X is not modular, but has a distinguished lifting X_0 into a number field k with respect to $S = \{x\}$. Then $[k : \mathbb{Q}] \geq B_1(n, \deg(X), H_{CM}(x))$.*

Theorem C.4 *Assume GRH.Then there exists an effectively computable function $B_2 : \mathbb{N}^3 \to \mathbb{N}$ such that the following holds. Let X be an irreducible algebraic hypersurface in $\mathbb{A}^n_{\overline{\mathbb{F}}_p}$ of degree d, and let $(x'_1, \ldots, x'_n) \in X(\overline{\mathbb{F}}_p)$ be an ordinary point with canonical lift $(x_1, \ldots, x_n)$. Suppose that X has a distinguished lifting X_0 to a number field k w.r.t. $S = \{(x'_1, \ldots, x'_n)\}$ and that the following conditions hold UTPC:*

$$
\begin{aligned}
&H_{CM}(x_1, x_2) \geq B_2(2, d, [k(x_3, \ldots, x_n) : \mathbb{Q}]) \\
&H_{CM}(x_3) \geq B_2(3, d, [k(x_4, \ldots, x_n) : \mathbb{Q}]) \\
&\ldots \\
&H_{CM}(x_n) \geq B_2(n, d, [k : \mathbb{Q}])
\end{aligned}
$$

Then X_0 is modular.

Without GRH we can only prove weaker results. We can get the following.

Theorem C.5 *There exists an effectively computable function $B_3 : \mathbb{N}^4 \to \mathbb{N}$ such that the following holds. Let X be an irreducible algebraic curve in $\mathbb{A}^2_{\overline{\mathbb{F}}_p}$ of bidegree (d_1, d_2), with d_1 and d_2 positive. Let $(x'_1, x'_2) \in X(\overline{\mathbb{F}}_p)$ be an ordinary point and (x_1, x_2) its canonical lift. Let K be the compositum of the CM fields $End_{\mathbb{Q}}(x_1)$ and $End_{\mathbb{Q}}(x_2)$. Suppose that $p \geq \max\{d_1, 13\}$, that X has a distinguished lifting X_0 defined over a number field k w.r.t. $S = \{(x'_1, x'_2)\}$ and that the following conditions hold:*

1. $K \subset k \subsetneq K(x_1, x_2)$
2. $k|K$ *is Galois, and for* $\mathfrak{p}$ *a prime of* k *lying above* p *we have* $(\mathfrak{p}, k/K) = 1$.
3. $H_{CM}(x_1, x_2) \geq B_3(d_1, d_2, [k : \mathbb{Q}], p)$.

Then X_0 *is a modular curve.*

Theorem C.6 *There exist effectively computable functions* $B_4 : \mathbb{N}^3 \to \mathbb{N}$ *and* $B_5 : \mathbb{N}^2 \to \mathbb{N}$ *such that the following holds. Let* X *be an irreducible algebraic hypersurface in* $\mathbb{A}^n_{\overline{\mathbb{F}}_p}$ *of degree* d*, and let* $(x'_1, \ldots, x'_n) \in X(\overline{\mathbb{F}}_p)$ *be an ordinary point with canonical lift* $(x_1, \ldots, x_n) \in \mathbb{A}^n(\overline{\mathbb{Q}})$*. Let* K *denote the compositum of the CM fields* $End_{\mathbb{Q}}(x_i)$*. Suppose that* X *has a distinguished lifting* X_0 *defined over a number field* k *w.r.t.* $S = \{(x'_1, \ldots, x'_n)\}$*, and that the following conditions hold UTPC.*

- $p \geq \max\{d, 13\}$
- *Let* $\mathfrak{p}$ *be a prime of* $K(x_3, \ldots, x_n)$ *lying above* p*. Then* $(\mathfrak{p}, K(x_3, \ldots, x_n)/K) = 1$.
- $K \subset k \subset K(x_n) \subset K(x_n, \ldots, x_3) \subset K(x_1, x_2)$
- $H_{CM}(x_1), H_{CM}(x_2) > B_4(d, [K(x_n, \ldots, x_3) : \mathbb{Q}], p)$
  $H_{CM}(x_3) > B_4(d, [K(x_n, \ldots, x_4) : \mathbb{Q}], p)$
  $\cdots$
  $H_{CM}(x_{n-1}) > B_4(d, [K(x_n) : \mathbb{Q}], p)$
- $[K(x_n) : k] > B_5(d, n)$
  $[K(x_n, x_{n-1}) : K(x_n)] > B_5(d, n)$
  $\cdots$
  $[K(x_n, \ldots, x_3) : K(x_n, \ldots, x_4)] > B_5(d, n)$

Then X_0 *is modular.*

Remarks. The hypothesis of Theorem C.4 is stronger than it appears. $B_2(n, d, m)$ grows with m, the degree of the field extension involved, while $\log[\mathbb{Q}(x) : \mathbb{Q}] \approx (\frac{1}{2} + o(1)) \log H_{CM}(x)$ for a CM point x (see [8]), so in effect the hypothesis requires

$$H_{CM}(x_1, x_2) > H_{CM}(x_3) > H_{CM}(x_4) > \cdots > H_{CM}(x_n)$$

with fairly large gaps between the heights.

On the other hand, every modular hypersurface (being of the form $\{x_1\} \times \mathbb{A}^{n-1}$ or $Y'_0(N) \times \mathbb{A}^{n-2}$, UTPC) has CM points with this property.

Concerning Theorem C.5, we point out that, again as $[\mathbb{Q}(x_1, x_2) : \mathbb{Q}]$ grows with $H_{CM}(x_1, x_2)$, the field k must be much smaller than $K(x_1, x_2)$ in order for the condition $H_{CM}(x_1, x_2) > B_3(d_1, d_2, [k : \mathbb{Q}], p)$ to hold.

C.6 CM points on curves

In this section we shall study CM points on affine curves defined over $\overline{\mathbb{Q}}$ and prove Theorems C.3 and C.5.

We now give an outline of Edixhoven's approach to the André-Oort conjecture. It is based on the following characterisation of the modular curves.

Let T_m denote the correspondence on $\mathbb{A}^n$ which to each point $(x_1, \ldots, x_n)$ assigns the set

$$\{(y_1, \ldots, y_n) \mid \text{There exist cyclic isogenies } y_i \to x_i \text{ of degree } m, \text{ for each } i\},$$

so T_m maps subsets of $\mathbb{A}^n$ to subsets of $\mathbb{A}^n$. For m square free (as it will be in our case) this is just the direct product of n copies of the usual Hecke operator, also denoted T_m, which assigns to every elliptic curve E the set of quotients of E by various subgroups of order m. See for example [63, Chapter 1]. Then we have (see [19])

Theorem C.7 (Edixhoven) *Let X be an irreducible algebraic curve in $\mathbb{A}^2_{\mathbb{C}}$ of bidegree (d_1, d_2), with d_1 and d_2 positive. Suppose we have $X \subset T_m(X)$ for some square free integer $m > 1$ composed of primes $p \geq \max(13, d_1)$. Then $X = Y_0'(N)$ for some N.*

There exist various generalisations of this, characterising subvarieties of Hodge type in terms of their being fixed by Hecke operators, see for example [71].

Now Edixhoven's strategy is to find enough points on $X \cap T_m(X)$ to make this intersection improper. One way of going about this is the following.

Let $x \in \overline{\mathbb{Q}}$ be a CM point that is the canonical lift of its reduction mod $\mathfrak{P}$. We say that x is canonical at p. According to [41, Chapter 13] this is equivalent to the condition that p splits in the CM field K of x and that p does not divide the conductor f of the order $\mathrm{End}(x)$ in K. According to the theory of complex multiplication (see for example [41, Chapter 10]) this is in turn equivalent to the condition that there is an isogeny of degree p (and hence cyclic) between $\sigma_{\mathfrak{p}}(x)$ and x, where $\mathfrak{p} = \mathfrak{P} \cap K$ and $\sigma_{\mathfrak{p}} = (\mathfrak{p}, K(x)/K) \in \mathrm{Gal}(K(x)/K)$ is the Artin symbol corresponding to $\mathfrak{p}$.

If $x \in X(\overline{\mathbb{Q}})$ is a CM point on X, which is canonical at p (i.e. all the coordinates of x are canonical at p), then we see that we find a Galois element $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma_p(x) \in T_p(\{x\})$. If σ_p fixes X (and hence $T_p(X)$), then we get $x \in X \cap T_p(X)$. So if we have enough points canonical at p, then the intersection is improper and we can conclude from Theorem C.7 that X must be modular. In particular, this shows Theorem C.2 for curves X defined over $\mathbb{Q}$.

For an abelian variety A of dimension g it is still true that if A is canonical at p then there is an isogeny $A \to A^\sigma$ with kernel isomorphic to $(\mathbb{Z}/p\mathbb{Z})^g$, for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so the above argument should yield another proof of Theorem C.2. But there are difficulties, for example we need a version of Theorem C.7 for abelian varieties, and the σ's must fix X.

In general, given a Zariski-dense set S of CM points on a variety X, there need not exist any prime p at which all (or even infinitely many) of the points S are canonical. So what is needed is a method of constructing new CM points on X, with convenient properties, given the set S. This seems to be very difficult. The only method that has yielded results so far (to the author's knowledge) is to take the Galois conjugates of S.

It is now clear why we have such restrictions on the field of definition k of X in the next Theorem below. On the one hand, our σ_p must fix k, as described above, and on the other hand, a given CM point has fewer conjugates on X if the degree of k is large. In fact it is precisely this last principle that gives us our bounds on the lifting field in section 5.

Theorem C.8 *There exists an effectively computable function $B_3 : \mathbb{N}^4 \to \mathbb{N}$ such that the following holds. Let X be an irreducible algebraic curve in $\mathbb{A}^2_{\overline{\mathbb{Q}}}$ of bidegree (d_1, d_2) with d_1 and d_2 positive, defined over a number field k. Suppose X contains a CM point (x_1, x_2). Denote by K the compositum of the CM fields $End_{\mathbb{Q}}(x_1)$ and $End_{\mathbb{Q}}(x_2)$, and suppose that the following properties hold:*

1. *There exists a prime $p \geq \max(d_1, 13)$ at which (x_1, x_2) is canonical.*
2. *$K \subset k \subsetneq K(x_1, x_2)$*
3. *$k|K$ is Galois, and for $\mathfrak{p}$ a prime of k lying above p we have $(\mathfrak{p}, k/K) = 1$.*
4. *$H_{CM}(x_1, x_2) \geq B_3(d_1, d_2, [k : \mathbb{Q}], p)$.*

Then X is modular.

Proof. Let $K_i = \mathrm{End}_{\mathbb{Q}}(x_i)$ denote the CM field of x_i, so that $K = K_1K_2$. Write $L_i = K_i(x_i)$ and $L = L_1L_2 = K(x_1, x_2)$. Let $\mathfrak{P}$ be a prime of L lying above $\mathfrak{p}$, and set $\mathfrak{P}_i = \mathfrak{P} \cap L_i$ and $\mathfrak{p}_i = \mathfrak{P} \cap K_i$.

We first show that p is unramified in L. As x_i is canonical at p it follows that p is split in K_i and that p does not divide the conductors of the orders $\mathrm{End}(x_i)$. The Main Theorem of complex multiplication tells us that L_i is the ring class field of K_i with respect to $\mathrm{End}(x_i)$ (see [17]), hence p is unramified in L_i and thus also in L.

Let $\sigma = (\mathfrak{P}, L/\mathbb{Q}), \sigma_i = \sigma|_{L_i} = (\mathfrak{P}_i, L_i/\mathbb{Q})$ and $\sigma_i' = (\mathfrak{P}_i, L_i/K_i) = (\mathfrak{p}_i, L_i/K_i)$ (the Artin symbol, as L_i/K_i is abelian). We show next that $\sigma_i = \sigma_i'$. Let $\mathcal{O}_{L_i}$ denote the ring of integers of L_i. Then, by definition, σ_i is the unique element of $\mathrm{Gal}(L_i/\mathbb{Q})$ satisfying

$$\sigma_i(\alpha) \equiv \alpha^p \bmod \mathfrak{P}_i \quad \forall \alpha \in \mathcal{O}_{L_i}. \tag{C.3}$$

But as p splits in K_i we have $N(\mathfrak{p}_i) = p$ and so σ_i' also satisfies (C.3). Hence $\sigma_i = \sigma_i'$. In particular, $\sigma|_K = 1$.

Let $\mathcal{O}_i = \mathrm{End}(x_i)$ and $\mathfrak{p}_i' = \mathfrak{p}_i \cap \mathcal{O}_i$. Then $\mathcal{O}_i/\mathfrak{p}_i' \cong \mathbb{Z}/p\mathbb{Z}$. By the Main Theorem of complex multiplication we see that $\mathfrak{p}_1'$ and $\mathfrak{p}_2'$ induce cyclic isogenies $x_1 \to \sigma_1^{-1}(x_1)$ and $x_2 \to \sigma_2^{-1}(x_2)$ of degree p. Thus $\sigma^{-1}(x_1, x_2) \in$

$T_p(\{(x_1,x_2)\}) \subset T_p(X)$. But $\sigma|_k = (\mathfrak{p}, k/K) = 1$, so σ fixes X and $T_p(X)$, hence we get $(x_1,x_2) \in T_p(X^\sigma) \cap X = T_p(X) \cap X$.

Furthermore, we see that the entire Galois orbit of (x_1,x_2) must lie in this intersection. We may assume with loss of generality that $[L_1 : K_1] \geq [L_2 : K_2]$. Then we have at least $\#\mathrm{Gal}(L/k) = \#\mathrm{Gal}(L/K)/\#\mathrm{Gal}(k/K) \geq 2[L_1 : K_1]/[k : \mathbb{Q}] = 2\#\mathrm{Pic}(\mathcal{O}_1)/[k : \mathbb{Q}]$ points in the intersection.

On the other hand, the intersection index is $X \cdot T_p(X) = 2d_1d_2(p+1)^2$ (see [19]). So if $\#\mathrm{Pic}(\mathcal{O}_1) > [k : \mathbb{Q}]d_1d_2(p+1)^2$ then the intersection is improper, implying that $X \subset T_p(X)$, as X is irreducible. Then it will follow from Theorem C.7 that X is modular.

Now $H_{CM}(x_1,x_2) = \max\{|\mathrm{Discr}(\mathcal{O}_1)|, |\mathrm{Discr}(\mathcal{O}_2)|\}$, and by the theorem of Goldfeld, Gross and Zagier (see [51]) there exist effective lower bounds on $\#\mathrm{Pic}(\mathcal{O}_i)$ in terms of $\mathrm{Discr}(\mathcal{O}_i)$. Hence if $H_{CM}(x_1,x_2)$ is sufficiently large, so is $\#\mathrm{Pic}(\mathcal{O}_1) = \max\{\#\mathrm{Pic}(\mathcal{O}_1), \#\mathrm{Pic}(\mathcal{O}_2)\}$ and we're done. □

Now Theorem C.5 is nothing more than a reformulation of Theorem C.8.

We note that if we have several CM points, each satisfying (1), (2) and (3) for the same prime p, then we can get away with smaller CM heights. More precisely, let $\{(x_1,y_2),\ldots,(x_t,y_t)\} \subset X(\overline{\mathbb{Q}})$ be CM points satisfying (1), (2) and (3) for the same prime p, and suppose that their Galois orbits are distinct. Then condition (4) can be replaced by

$$\sum_{i=1}^{t} \max\{\#\mathrm{Pic}(\mathrm{End}(x_i)), \#\mathrm{Pic}(\mathrm{End}(y_i))\} > [k : \mathbb{Q}]d_1d_2(p+1)^2. \tag{C.4}$$

In particular, the result holds if we have more than $[k : \mathbb{Q}]d_1d_2(p+1)^2$ CM points on X satisfying (1), (2) and (3).

We can compute an explicit version of condition (4). The theorem of Goldfeld, Gross and Zagier states (see [51]) that the class number $h(-d)$ of the quadratic imaginary field K of discriminant $-d$ satisfies $h(-d) \geq C^{-1}\vartheta(d)\log(d)$, where $\vartheta(d) = \prod(1 - \lfloor 2\sqrt{p}\rfloor/(p+1))$ and the product is taken over all primes p dividing d except the largest. One can take $C = 55$ for d prime to 5077, or $C = 7000$ in general. For an order $\mathcal{O}$ of conductor f in K we have (see e.g. [41, chapter 8])

$$\begin{aligned} \#\mathrm{Pic}(\mathcal{O}) &= h(-d)\frac{f}{[\mathcal{O}_K^* : \mathcal{O}^*]}\prod_{p|f}(1-\chi(p)p^{-1}) \\ &\geq \frac{1}{3}h(-d)\phi(f), \end{aligned} \tag{C.5}$$

where $\phi(f)$ is the Euler-ϕ function. So if we write $H_{CM}(x_1,x_2) = df^2$, with f maximal with respect to the condition that $d \equiv 0$ or $1 \bmod 4$, then we see that condition (4) is equivalent to

$$\vartheta(d)\log(d)\phi(f) > 3C[k : \mathbb{Q}]d_1d_2(p+1)^2. \tag{C.6}$$

The above arguments follow closely the methods in [19], except that we have bypassed the step showing that the CM fields K_1 and K_2 coincide for almost all

CM points (= for points of sufficient height). One can also extend this result to curves in $\mathbb{A}^n$ as follows. Let $\pi_{ij} : \mathbb{A}^n \to \mathbb{A}^2$ denote projection onto the ith and jth coordinates. Then we have

Proposition C.6.1 (see [8]) *A curve X in $\mathbb{A}^n$ is modular if and only if for some fixed i we have $\pi_{ij}(X) = Y_0'(N_{ij})$ for some integer N_{ij} for every $j \neq i$.*

Now if $(x_1, \ldots, x_n)$ is a CM point on X, choose i such that $H_{CM}(x_1, \ldots, x_n) = H_{CM}(x_i)$, and apply Theorem C.8 to each $\pi_{ij}(X)$. One may use a different prime for each projection.

We note that the existence of a suitable prime p above is not at all obvious. The Čebotarev density theorem tells us that there exist plenty of primes satisfying conditions (1) and (3), but as the function B_3 grows with p we see that for condition (4) to hold, p must be relatively small. To find small suitable primes one needs an effective version of the Čebotarev theorem, which requires GRH. In addition, (C.6) is not sharp enough even for this effective version of the Čebotarev theorem, so one has to replace Goldfeld's theorem by Siegel's theorem, which states that $\log(h(-d)) = (1/2 + o(1)) \log(d)$, but is only effective if we assume GRH.

In [8] we showed the following theorem, although again the hard work was done in [19].

Theorem C.9 *Assume GRH. Then there exists an effectively computable function $B_6 : \mathbb{N}^3 \to \mathbb{N}$ such that the following holds. Let X be an irreducible algebraic curve in $\mathbb{A}^n$ defined over a number field k, and suppose each standard projection $X \to \mathbb{A}^1$ is non-constant and has degree less than d. Then X is modular if and only if $X(\mathbb{C})$ contains a CM point of height at least $B_6(n, d, [k : \mathbb{Q}])$.*

This is just a reformulation of Theorem C.3, though we point out that in these formulations the functions B_1 and B_6 are inverses of each other (for fixed n and d, of course).

Proof outline. We only consider the case $n = 2$, the extension to general n being outlined above. Let X' be the union of the conjugates of X, so that X' is defined over $\mathbb{Q}$ (but in general no longer irreducible over $\overline{\mathbb{Q}}$). Let $x = (x_1, x_2)$ be a CM point on X', and p a prime at which x is canonical. Suppose that

$$\#\mathrm{Pic}(\mathrm{End}(x_1)) > d_1 d_2 (p+1)^2, \tag{C.7}$$

then as before we get $X' \subset T_p(X')$, where we point out that $T_p(X')$ is defined over $\mathbb{Q}$ and X' is still irreducible over $\mathbb{Q}$. However, as X' is not irreducible over $\mathbb{C}$, we cannot yet apply Theorem C.7.

Denote by W the set of irreducible components of X'. Then T_p defines a correspondence on W, also denoted by T_p. This correspondence is symmetric in the sense that $a \in T_p(\{b\}) \Rightarrow b \in T_p(\{a\})$, and surjective in the sense that $T_p(\{a\})$ is non-empty for every $a \in W$. So if we have two distinct primes p and q, such that T_p and T_q give the same correspondence on W, then $a \in T_p T_q(\{a\}) =$

$T_{pq}(\{a\})$ for all $a \in W$. Hence we would have $X \subset T_m(X)$, with $m = pq$, and we can apply Theorem C.7. There are

$$S(n) = 2^{n(n+1)/2} \tag{C.8}$$

symmetric correspondences on a set of n elements (not all of which are surjective). Let $t = [k : \mathbb{Q}] \geq \#W$. It follows that if we have at least $2^{t(t+1)/2}$ primes p satisfying (C.7), then X is modular.

Again, let $\mathcal{O}_i = \mathrm{End}(x_i)$ and assume $\#\mathrm{Pic}(\mathcal{O}_1) \geq \#\mathrm{Pic}(\mathcal{O}_2)$. From Siegel's theorem we get $\mathrm{Pic}(\mathcal{O}_1) \gg \mathrm{Discr}(\mathcal{O}_1)^{1/2-\epsilon}$, combining this with (C.7) we see that we want at least $2^{t(t+1)/2}$ primes p splitting in $\mathcal{O}_1$ and $\mathcal{O}_2$, and satisfying $\max(d_1, 13) \leq p \ll \mathrm{Discr}(\mathcal{O}_1)^{1/4-\epsilon}$, up to constants depending on ϵ and $d_1 d_2$.

In [61] there appears a version of the Čebotarev theorem, assuming GRH, that gives us our primes, see [19]. In fact, we can find at least $C_\epsilon \mathrm{Discr}(\mathcal{O}_1)^{1/4-\epsilon}$ suitable primes, for $\mathrm{Discr}(\mathcal{O}_1)$ sufficiently large. Combined with (C.8), this proves our theorem with

$$B_1(2, \deg(X), H_{CM}(x)) \gg \sqrt{\log\left(C_\epsilon H_{CM}(x)^{1/4-\epsilon}\right)}.$$

□

C.7 CM points on hypersurfaces

In this last section we shall prove some results on CM points on hypersurfaces, which are really just reformulations of Theorems C.4 and C.6.

Theorem C.10 *Assume GRH. Then there exists an effectively computable function $B_2 : \mathbb{N}^3 \to \mathbb{N}$ such that the following holds. Let X be an irreducible hypersurface in $\mathbb{A}^n_{\overline{\mathbb{Q}}}$ of degree not greater than d and defined over a number field k. Then X is modular if and only if, UTPC, X has a CM point $x = (x_1, \ldots, x_n)$ with the following properties:*

$$\begin{aligned}
&H_{CM}(x_1), H_{CM}(x_2) \geq B_2(2, d, [k(x_3, \ldots, x_n) : \mathbb{Q}]) \\
&H_{CM}(x_3) \geq B_2(3, d, [k(x_4, \ldots, x_n) : \mathbb{Q}]) \\
&\ldots \\
&H_{CM}(x_n) \geq B_2(n, d, [k : \mathbb{Q}]).
\end{aligned}$$

Proof. First, suppose that one of the standard projections $X \to \mathbb{A}^1$ is constant. Then (UTPC) $X = \{x_1\} \times \mathbb{A}^{n-1}$, which is modular. So we may assume that none of these projections are constant.

We use induction on n. For $n = 2$ we simply have a CM point x of large height on a plane curve. This case was already treated in Theorem C.9. So we assume $n \geq 3$.

If $H_{CM}(x_n)$ is sufficiently large (w.r.t. d and $[k : \mathbb{Q}]$), then $[k(x_n) : k]$ will also be large, so that $X(\mathbb{C})$ contains many conjugates of the point x with distinct

x_n-coordinates. Pick one and consider the intersection $X \cap (\mathbb{A}^{n-1} \times \{x_n\})$. The intersection is non-empty, thus has dimension at least $n-2$. If the dimension is $n-1$ then we have $X = \mathbb{A}^{n-1} \times \{x_n\}$, and we're done. So we suppose the dimension is $n-2$.

Let C' be an irreducible component of the intersection containing x. Write $C' = C \times \{x_n\}$, where C is an irreducible hypersurface in $\mathbb{A}^{n-1}$ defined over the number field $k(x_n)$, and containing the CM point $(x_1, \ldots, x_{n-1})$. By the induction hypothesis it follows that C is modular. As we can do this for each conjugate of x we can find sufficiently many (for our purposes below) disjoint modular subvarieties C' of X. We distinguish two cases.

Case 1. Suppose that one of the C''s is of the form (UTPC) $C' = \mathbb{A}^{n-2} \times \{x_{n-1}\} \times \{x_n\}$. It then follows that $X = \mathbb{A}^{n-2} \times Z$, where Z is a curve in $\mathbb{A}^2$, defined over k and containing the CM point (x_{n-1}, x_n), which has CM height at least $\min\{B_2(n, d, [k : \mathbb{Q}]), B_2(n-1, d, [k(x_n) : \mathbb{Q}])\} \geq B_2(2, d, [k : \mathbb{Q}])$. Thus Z is modular and so is X.

Case 2. Suppose all the C''s are of the form (UTPC) $C' = Y_0'(N) \times \mathbb{A}^{n-3} \times \{x_n\}$, for various N's. As the N's are bounded from above in terms of d, we can find one N (and one particular permutation of the coordinates) which occurs often enough (by suitably defining the function B_2) to make the intersection $X \cap (Y_0'(N) \times \mathbb{A}^{n-2})$, containing all these C''s, improper. Then $X = Y_0'(N) \times \mathbb{A}^{n-2}$ is modular.

□

Remarks. Unfortunately, a Zariski-dense set of points need not have a point with this property, so this does not imply the André-Oort conjecture. We note that, assuming GRH, the André-Oort conjecture has already been proved for subvarieties of $\mathbb{A}^n$ by Edixhoven [21].

Every modular hypersurface does in fact have points with this property, so we can interpret Theorem C.10 as a characterisation of modular hypersurfaces.

Why just hypersurfaces? One can pull the whole argument through for subvarieties of higher codimension, and get a result which requires a similar - but stricter - height condition on the CM point. Unfortunately, this is all theory of the empty set, as many modular varieties of higher codimension do not have any CM points actually satisfying that height condition.

If we keep track of fields of definitions and existence of certain primes, then we can get a similar result without GRH.

Theorem C.11 *There exist effectively computable functions $B_4 : \mathbb{N}^3 \to \mathbb{N}$ and $B_5 : \mathbb{N}^2 \to \mathbb{N}$ such that the following holds. Let X be an irreducible algebraic hypersurface in $\mathbb{A}^n_{\overline{\mathbb{Q}}}$, of degree not greater than d, and defined over a number field k. Suppose that $X(\overline{\mathbb{Q}})$ contains a CM point $x = (x_1, \ldots, x_n)$. Let K denote the compositum of the CM fields $End_{\mathbb{Q}}(x_1), \ldots, End_{\mathbb{Q}}(x_n)$. Suppose that the following conditions are satisfied (UTPC):*

- *There exists a prime $p \geq \max\{13, d\}$ which splits in each $End(x_i)$.*
- *Let $\mathfrak{p}$ be a prime of $K(x_3, \ldots, x_n)$ lying above p. Then $(\mathfrak{p}, K(x_3, \ldots, x_n)/K) = 1$.*

- $K \subset k \subset K(x_n) \subset K(x_n, \ldots, x_3) \subset K(x_1, x_2)$
- $H_{CM}(x_1), H_{CM}(x_2) > B_4(d, [K(x_n, \ldots, x_3) : \mathbb{Q}], p)$
  $H_{CM}(x_3) > B_4(d, [K(x_n, \ldots, x_4) : \mathbb{Q}], p)$
  $\ldots$
  $H_{CM}(x_{n-1}) > B_4(d, [K(x_n) : \mathbb{Q}], p)$
- $[K(x_n) : k] > B_5(d, n)$
  $[K(x_n, x_{n-1}) : K(x_n)] > B_5(d, n)$
  $\ldots$
  $[K(x_n, \ldots, x_3) : K(x_n, \ldots, x_4)] > B_5(d, n)$

Then X is modular.

Proof Outline. Similar as for Theorem C.10. The number $B_5(d, n)$ ensures that the point x has enough conjugates with distinct x_n coordinates, a fact which does not follow effectively from $H_{CM}(x)$ large without assuming GRH. As before one checks that this reduces to Theorem C.8 for $n = 2$, and that the step reducing the dimension (i.e. the induction step) preserves the list of properties.

□

Acknowledgments The author would like to thank Bas Edixhoven for pointing out an error in a previous version of the manuscript and Marc Hindry for his patient help and useful suggestions.

Bibliography

[1] Y.André, "G-functions and geometry", *Aspects of Mathematics*, **E13**, Vieweg Verlag, 1989.

[2] Y.André, "Distribution des points CM sur les sous-variétés des variétés de modules de variétés abéliennes", Jussieu prépublication **120**, 1997

[3] Y.André, "Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire", *J. reine angew. Math.* **505** (1998), 203-208.

[4] E.Artin and J.Tate, "Class Field theory", W.A.Benjamin, 1968.

[5] S.Bae, "On the modular equation for Drinfeld modules of rank 2", *J. Number Theory* **42** (1992), 123-133.

[6] B.Belhaj-Dahmane, "Jacobiennes à mulitplication complexe", Thesis, Université de Paris 6, 2001.

[7] S.Bosch, U.Güntzer and R.Remmert, "Non-Archimedean Analyis", Springer-Verlag, 1984.

[8] F.Breuer, "Heights of CM points on complex affine curves", *The Ramanujan Journal.* **5.3** (2001), 311-317.

[9] F.Breuer, "Distinguished liftings and the André-Oort conjecture", To appear in: *Quaestiones Math.*

[10] M.L.Brown, "Singular moduli and supersingular moduli of Drinfeld modules", *Invent. Math.* **110** (1992), 419-439.

[11] L.Carlitz, "A class of polynomials", *Trans. Amer. Math. Soc.* **43** (1938), 167-182.

[12] J.W.S.Cassels, "Global fields", in: "Algebraic Number Theory" (J.W.S.Cassels and A.Fröhlich, eds), Academic Press, 1967.

[13] P.B.Cohen and G.Wüstholz, "Application of the André-Oort conjecture to some questions in transcendence". in: "A Panorama of Number Theory" (G.Wüstholz, ed.), Cambridge University Press, 2001.

[14] P.Colmez, "Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe", *Compos. Math.* **111** (1998), 359-368.

[15] C.Cornut, "Mazurs's Conjecture on higher Heegner points", *Invent. Math.* **148** (2002), 495-523.

[16] C.Cornut, "Non-trivialité des points de Heegner", *C.R.Acad.Sci.Paris, Ser. A* **334.12** (2002), 1039-1042.

[17] D.A.Cox, "Primes of the form $p = x^2 + ny^2$: Fermat, class field theory and complex multiplication", John Wiley & Sons, Inc., 1989.

[18] V.L.Drinfeld, "Elliptic modules (Russian)", *Math.Sbornik* **94** (1974), 594-627. Translated in *Math. USSR. S.* **23** (1974), 561-592.

[19] S.J.Edixhoven, "Special points on the product of two modular curves", *Compos. Math.* **114** (1998), 315-328.

[20] S.J.Edixhoven, "On the André-Oort conjecture for Hilbert modular surfaces", in: "Moduli of Abelian Varieties", *Progress in Mathematics*, Birkhäuser Verlag, Basel, 2001.

[21] S.J.Edixhoven, "On the André-Oort conjecture for products of modular curves", in preparation.

[22] S.J.Edixhoven and A.Yafaev, "Subvarieties of Shimura varieties", to appear in *Annals of Math.*.

[23] M.Fried and M.Jarden, "Field Arithmetic", Springer-Verlag, 1986.

[24] W.Fulton, "Intersection Theory", Springer-Verlag, 1984.

[25] E.-U. Gekeler, "Drinfeld-Moduln und modulare Formen über rationalen Funktionen-köpern", *Bonner Math. Schriften* **119** (1980).

[26] E.-U. Gekeler, "Zur Arithmetik von Drinfeld-Moduln", *Math. Annalen* **256** (1982), 549-560.

[27] E.-U. Gekeler, "Modulare Einheiten für Funktionen-körper", *J. Reine Angew. Math.* **348** (1984), 94-115.

[28] E.-U. Gekeler, "Über Drinfeld'sche Modulkurven vom Hecke-typ", *Compositio Math.* **57** (1986), 219-236.

[29] E.-U. Gekeler, "Drinfeld Modular Curves", *Lecture Notes in Mathematics* **1231**, Springer-Verlag, 1986.

[30] E.-U. Gekeler, "On the coefficients of Drinfeld modular forms", *Invent. Math.* **93** (1988), 667-700.

[31] D.Goss, "Basic Structures of Function Field Arithmetic", Springer-Verlag, 1996.

[32] R.Hartshorne, "Algebraic geometry", *Graduate Texts in Mathematics* **52**, Springer-Verlag, 1977.

[33] D.Hayes, "Explicit class field theory in global function fields", in: "Studies in algebra and number theory" (G.C.Rota, ed.), Academic Press, New York, 1979.

[34] D.Hayes, "A Brief introduction to Drinfeld modules", in: The Arithmetic of Function Fields (eds. D.Goss et al), de Gruyter, New York-Berlin, 1992.

[35] M.Hindry, "Points de torsion sur les sous-variétés de variétés abéliennes", *C.R.Acad.Sci.Paris, Ser.A* **304.12** (1987), 311-314.

[36] M.Hindry, "Autour d'une conjecture de Serge Lang", *Invent. Math.* **94** (1988), 575-603.

[37] M.Hindry, J.H.Silverman, "Diophantine Geometry: An Introduction", *Graduate Texts in Mathematics* **201**, Springer-Verlag, 2000.

[38] L.K.Hua, appendix to: J.Dieudonné, "On the automorphisms of the classical groups", *Memoirs Amer.Math.Soc.* **2** (1951), 1-95.

[39] B.Huppert, "Endliche Gruppen I", Springer-Verlag, 1967

[40] S.Lang, "Fundamentals of Diophantine Geometry", Springer-Verlag, 1983.

[41] S.Lang, "Elliptic Functions", 2nd Edition, *Graduate Texts in Mathematics* **112**, Springer-Verlag, 1987.

[42] S.Lang, "Algebraic Number Theory", 2nd Edition, *Graduate Texts in Mathematics* **110**, Springer-Verlang, 1994.

[43] H.Lange, Ch.Birkenhake, "Complex abelian varieties", *Grundlehren der mathematischen Wissenschaften* **302**, Springer-Verlag, 1992.

[44] J.Lubin, J-P.Serre & J.Tate, "Elliptic curves and formal groups", in: *Lect. Notes, AMS Summer Inst. Algebraic Geometry*, Woods Hole, July 1964.

[45] B.Mazur, "Modular curves and arithmetic", Proceedings of the International Congress of Mathematicians, Warszawa, 1983.

[46] J.S.Milne, "Class field theory", lecture notes available at `http://www.math.lsa.umich.edu/jmilne`

[47] B.Moonen, "Special points and linearity properties of Shimura varieties", thesis, Universiteit Utrecht, 1995.

[48] B.Moonen, "Linearity properties of Shimura varieties I", *J. Alg. Geom.* **7** (1998), 639-567.

[49] B.Moonen, "Linearity properties of Shimura varieties II", *Compos. Math.* **114** (1998), 3-35.

[50] D.Mumford, "A note on Shimura's paper 'Discontinuous groups and abelian varieties' ", *Math. Ann.* **181** (1969), 345-351.

[51] J.Oesterlé, "Nombre de classes des corps quadratiques imaginaires", *Astérisque* **121-122** (1985), 309-323.

[52] J.Oesterlé, "Le problème de Gauss sur le nombre de classes", *Ens. Math.* **34** (1988), 43-67.

[53] F.Oort, "Some questions in algebraic geometry", manuscript, 1995, available at `http://www.math.uu.nl/people/oort/`

[54] F.Oort, "Canonical liftings and dense sets of CM points", *Sympos. Math.*, **XXXVII**, (1997), Cambridge Univ. Press, 228-234.

[55] R.Pink, "Hodge structures over function fields", Preprint 1997.

[56] M.Raynaud, "Courbes sur une variété abélienne et points de torsion", *Invent. Math.* **71** (1983), 207-233.

[57] M.Raynaud, "Sous-variété d'une variété abélienne et points de torsion." in: "Arithmetic and Geometry" (dedicated to Shafarevic) Vol 1, pp327-352. Birkhäuser Verlag, Boston, 1983.

[58] S.Roman, "Field Theory", *Graduate Texts in Mathematics* **158**, Springer-Verlag, 1995.

[59] M.Rosen, "Number Theory in Function Fields", *Graduate Texts in Mathematics* **210**, Springer-Verlag, 2002.

[60] M.Saïdi, "Moduli schemes of Drinfeld modules" in *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, 17–31, World Sci. Publishing, River Edge, NJ, 1997.

[61] J-P.Serre, "Quelques applications du théorème de densité de Chebotarev", *Publ.Math.IHES* **54** (1981), 123-202.

[62] J.H.Silverman, "The arithmetic of elliptic curves", *Graduate Texts in Mathematics* **106**, Springer-Verlag, 1986.

[63] J.H.Silverman, "Advanced topics in the arithmetic of elliptic curves", *Graduate Texts in Mathematics***151**, Springer-Verlag, 1994.

[64] G.Van Steen, "Some rigid geometry", in *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, 17–31, World Sci. Publishing, River Edge, NJ, 1997.

[65] H.Stichtenoth, "Algebraic Function Fields and Codes", Springer-Verlag, 1993.

[66] J.Tate, "Global class field theory", in: "Algebraic Number Theory" (J.W.S.Cassels and A.Fröhlich, eds), Academic Press, 1967.

[67] M.van der Put, "The structure of Ω and its quotients $\Gamma\backslash\Omega$", in *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, 17–31, World Sci. Publishing, River Edge, NJ, 1997.

[68] M.van der Put and J. Top, "Analytic compactification and modular forms", in *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, 17–31, World Sci. Publishing, River Edge, NJ, 1997.

[69] J.T.-Y.Wang and J.Yu, "On class number relations over function fields", *J. Number Theory* **69** (1998), 181-196.

[70] J.Wolfart, "Werte hypergeometrischer Funktionen", *Invent. Math* **92** (1988), 187-216.

[71] A.Yafaev, "Sous-variétés des variétés de Shimura", thesis, Université de Rennes, 2000.

[72] A.Yafaev, "Special points on products of two Shimura curves" *Manuscripta Math.*, **104**, (2001), 163-171.

[73] J.-K. Yu, "A class number relation over function fields", *J. Number Theory* **54.2** (1995), 318-340.