UiT
THE ARCTIC UNIVERSITY OF NORWAY

Faculty of Science and Technology
Department of Mathematics and Statistics

The Four Faces of Hyperelliptic curves

Marcus L. Boyne

Master’s thesis in Mathematics May 2020

Abstract

In this thesis we will look at elliptic and hyperelliptic curves. There are three abelian groups that are isomorphic to hyperelliptic curves. The Jacobian of hyperelliptic curves, the ideal class group and the form class group, will all be defined and given abelian group structure. We will give an algorithm for point addition and point doubling done exclusively in the jacobian of the curve. We will end the thesis with proving that there exists an isomorphism between the form class group and the ideal class group.

Acknowledgement

I am very grateful to Ragnar Soleng for all the help and guidance through the work on this thesis. I would also like to thank Helge Johansen for all the help with administrative issues regarding my studies.

Finally I would like to thank Madelene Niska for all her support.

Table of Contents

List of Notation

P, Q, R Usually points on the curve

k Field

$\overline{k}$ Algebraically closed field

C Hyper elliptic curve

$k[C]$ Coordinate ring of C over k

$\langle\rangle$ ideal generated by the polynomial inside

$k(C)$ Field of fraction of C over k

D Divisor

$\mathbf{D^0}$ Group of all divisors of degree 0

$\overline{k}(C)^*$ The function field of C over $\overline{k}$

$\mathbf{P}$ Group of all principal divisors

$\mathbf{J}$ The Jacobian of a curve

$J(k)$ Divisor class group

$\mathcal{F}$ The group of fractional ideals

$\mathcal{P}$ the group of principal ideals

$Cl(\mathcal{O})$ Ideal class group

$Cl(F)$ Form class group

$SL_2(Z)$ Form class group

1 Introduction

Hyperelliptic curves are, among other things, used for public key cryptography, digital signatures and pseudo random number generation. There are currently only standards using hyperelliptic curves of genus 1, which are called elliptic curves. The advantage of elliptic curve cryptography (ECC) becomes evident when higher level of security is required. If a 80 bit symmetric key security level is needed, using the most popular public key crypto system RSA, a 1024 bit key length is required, while only 160 bit keys are required using ECC. If a 256 bit symmetric key security level is required, 15360 bit keys are required if using RSA, while only a 512 bit keys are required in ECC.

Microsoft Research published an article that suggests that the ECC is going to be weaker against attacks from quantum computers than RSA. [4] This does not mean that hyperelliptic curve cryptography is not going to be interesting in the post quantum world. National Institute of Standards and Technology (NIST) is currently (may 2020) in a process of deciding on an post quantum cryptographic scheme. Among the contestants is Supersingular Isogeny Key Encapsulation (SIKE), which uses supersingular isogeny Diffie–Hellman key exchange (SIDH) to exchange keys before using a symmetric key scheme to encrypt the actual information.

As Menezes wrote in 1996:

> ”Elliptic curves have been extensively studied over hundred years, and there is a vast literature on the topic...
> ...On the other hand, the theory of hyperelliptic curves has not received much attention by the research community.” [1, p. 2]

This is still true 24 years later. Finding literature on the topic has proven to be difficult, which makes it hard to specialize in hyperelliptic curves.

In this thesis we will look at hyperelliptic curves and its four faces and then prove that two of them are isomorphic. First, we will look at elliptic curves, which are special cases of hyperelliptic curves. We will also prove that there exists an isomorphism between the points on an elliptic curve and the jacobian of the curve. Secondly, we will look at the jacobian of hyperelliptic curves, which is a quotient group where the elements are finite formal sums. This group is most commonly used for representing points on the hyperelliptic curve. The group operation in the jacobian, as defined by Menezes [1], performs the group operation in the ideal class group. We will present an algorithm which performs the group operation strictly in the jacobian. By an example, we are going to show how to use Hensel's lemma to improve the efficiency of the algorithm. This is not the first time this algorithm is described. Thirdly, we will describe the ideal class group, in which the elements are ideals. This is the group most commonly used for computational reasons. Fourthly, we describe the form class group, in which the elements are binary quadratic forms. The group operation will not be defined in this chapter, as we will define it through the ideal class group. Finally, we will prove that there exists an isomorphism between the ideal class group and the form class group.

2 Hyperelliptic curves

In this section we are introducing elliptic and hyperelliptic curves. Algebraic curves are affine or projective varieties of dimension one. They correspond to irreducible polynomials. For hyperelliptic and elliptic curves there is a single point at the line at infinity, which we denote by ∞. Our treatment of hyperelliptic curves will mostly follow ”An elementary introduction to hyperelliptic curves” [1]

Definition 2.1. Let k be a field and let $\overline{k}$ be the algebraic closure of k. A *hyperelliptic curve* C of *genus* g over k $(g \geq 1)$ is given by a polynomial on the form

$$C: \; y^2 + h(x)y - f(x) \in k[x, y]$$

where $h(x) \in k[x]$ is a polynomial of degree at most g, $f(x) \in k[x]$ is a polynomial of degree $2g+1$, and there are no solutions $(x, y) \in \overline{k} \times \overline{k}$ which simultaneously satisfy the equation $y^2 + h(x)y = f(x)$ and the partial derivative equations $2y + h(x) = 0$ and $h'(x)y - f'(x) = 0$

Rational points are all points $P = (a, b)$ such that a and b are in k and solve the equation $y^2 + h(x)y = f(x)$, together with the point at infinity ∞. All points except the point at infinity are called finite points. If $P = (a, b)$ is a finite point, then the opposite point of P is the point $\tilde{P} = (a, -b - h(a))$. If $P = \tilde{P}$, then we call P a special point.

Definition 2.2. An *elliptic curve* is an hyperelliptic curve of genus 1

3 Elliptic Curves

In this section we are going to prove that there exists a group isomorphism between the points on an elliptic curve, $E(k)$, and the jacobian of the curve, $J(E)$.

$$E(k) \leftrightarrow J(E)$$

In order to prove this, we are using several propositions and the Riemann-Roch theorem.

Proposition 3.1. *Let C be a smooth curve and let $f \in \overline{K}(C)^*$, where $\overline{K}(C)$ is the function field of C over $\overline{k}$.*
(a) $div(f) = 0$ if, and only if, $f \in \overline{k}^*$
(b) $deg(div(f)) = 0$
[5, p. 28]

Proposition 3.2. *Let W be a canonical divisor, then $deg(W) = 2g - 2$ and $l(W) \geq g$.*
[2, p. 107]

Theorem 3.3 (Riemann-Roch)**.** *Let W be a canonical divisor on C, then for any divisor D,*

$$l(D) = deg(D) + 1 - g + l(W - D).$$

[2, p. 108]

Corollary 3.3.1. *If $deg(D) \geq 2g - 1$, then $l(D) = deg(D) + 1 - g$ [2, p. 109]*

Proposition 3.4. *The map:*

$$f : P \mapsto P - \infty$$

is an isomorphism from the group of points on an elliptic curve, $E(k)$, to the jacobian $J(E)$

Proof. We must prove that the map f is an homomorphism, and that it is injective and surjective.

To prove that the map is an homomorphism, let $P, Q, R \in E(k)$ be points on the elliptic curve and $P - \infty, Q - \infty, R - \infty \in J(E)$ be divisors in the jacobian, such that

$$f(P) = P - \infty$$

$$f(Q) = Q - \infty$$

$$f(R) = R - \infty$$

Assume that $P + Q = R \in E(k)$
If $f(P) + f(Q) \sim f(R)$, we have proved that f is an homomorphism.

$$f(P) + f(Q) = P - \infty + Q - \infty = P + Q - 2\infty \in J(E))$$

In other words if $P + Q - 2\infty \sim R - \infty$, our proof is complete.

If L is the line that goes through the points P and Q, the line will intersect the curve in a third point, $(-R)$. This line has divisor

$$div(L) = P + Q + (-R)$$

If M is the line that goes through the points $(-R)$ and R, it will intersect a third point in infinity. The line M has divisor

$$div(M) = R + (-R) + \infty$$

$$P + Q - R - \infty = div\left(\frac{L}{M}\right)$$

This proves that f is an homomorphism.

Now assume $P - \infty \sim Q - \infty$.
If we can prove that $P = Q$, we have proved that f is injective. Since P is a point, then $div(f) + Q = P$ and $P > 0$. The function f is in the vector space $L(Q)$, because $div(f) + Q \geq 0$.

Proposition 3.2 states that if W is a canonical divisor, then the degree is $deg(W) = 2g - 2$. If $deg(D) \geq 2g - 1$, then

$$deg(W) - deg(D) \leq 2g - 2 - (2g - 1)$$

$$deg(W - D) \leq -1$$

This implicates that $l(W - D) = 0$.

If we further assume, in addition to this, that $deg(D) \geq 2g-1$, then the Riemann-Roch theorem 3.3 reduces to

$$l(D) = deg(D)$$

Since Q is a point on the elliptic curve, then $deg(Q) = 1$, which is $\geq 2g - 1$. The reduced form of the Riemann-Roch theorem now applies, and therefore the dimension of the vector space $l(Q) = 1$, and $k \subseteq L(Q)$. This implicates that $L(Q) = k$. This means that f must be a constant function, which further implicates that $P = Q$. This completes the injection proof.

In order to prove that f is a surjection, it is assumed that D is a divisor of degree 0. Let $D' = D + \infty$, then $deg(D') = 1$. Corollary 3.3.1 states that if $deg(D) \geq 2g - 1$, then $l(D) = deg(D) + 1 - g$. Elliptic curves have genus 1, which implicates that $l(D') = deg(D')$. By the definition of $L(D)$, there exists a function $f \in \overline{K}(C)^*$, such that $div(f) + D' \geq 0$. Proposition 3.1 states that $deg(div(f)) = 0$. This leads to $deg(div(f)+D') = 1$. Since $div(f)+D'$ is positive and the degree is 1, it must be a point, $div(f) + D' = P$, on the elliptic curve. This means that $D' - \infty = D$ is equivalent to $P - \infty$

This concludes our proof.

□

4 Jacobian of Curves

The coordinate ring of C over k, is defined to be $k[C] = k[x, y]/ \left\langle y^2 + h(x)y - f(x) \right\rangle$, where $\left\langle y^2 + h(x)y - f(x) \right\rangle$ denotes the ideal in $k[x, y]$, generated by the polynomial $y^2+h(x)y-f(x)$. Elements in the coordinate ring $k[C]$, are called polynomial functions in C. The field of fraction of $k[C]$, is called the function field of C over k. The field of fraction is denoted by $k(C)$, and its elements are called rational functions. There exists a rational function u, such that $u(P) = 0$, and for each polynomial function t there exists an integer d and a rational function s, such that $s(P) \neq 0, \infty$, and $t = u^d s$. d is defined to be the order of t, and is denoted by $\operatorname{ord}_P(t) = d$. u is called the uniformizing parameter for the point P, and the integer d does not depend on the choice of u. Let $r = t/h$ be a rational function, where t and h are polynomial functions, then the order of r on the point $P \in C$ is defined to be $\operatorname{ord}_P(r) = \operatorname{ord}_P(t) - \operatorname{ord}_P(h)$.

A divisor D is a formal sum on the form $\sum_{P \in C} m_P P$, where $m_P \in \mathbb{Z}$, $P \in C(k)$, with only a finite number of the m_P being unequal to zero. The sum of two divisors is defined to be

$$\sum_{P \in C} m_p P + \sum_{P \in C} n_p P = \sum_{P \in C} (m_p + n_p) P.$$

The degree of a divisor is given by the sum $\sum_{P \in C} m_p$. The set of all divisors of degree 0 form an additive group, which will be denoted by $\mathbf{D^0}$.

A divisor of a rational function $r \in \overline{k}(C)^*$ is given by $div(r) = \sum_{P \in C} (\operatorname{ord}_P r) P$. These divisors are called principal divisors. All principal divisors have degree 0. The set of all principal divisors form a subgroup under the group $\mathbf{D^0}$, which will be denoted by $\mathbf{P}$

Definition 4.1. The Jacobian, $\mathbf{J}$ of a hyperelliptic curve, C is defined to be the quotient group $\mathbf{J} = \mathbf{D^0} \ / \ \mathbf{P}$

As the Jacobian is a quotient group, there are several divisors which are equivalent. This would be a problem seen from a cryptographic perspective. This is because two parties wouldn't necessarily end up with the same divisor after decryption. To make it useful for cryptography, there has to be a way of representing divisors uniquely.

Definition 4.2. A semi-reduced divisor is a divisor of the form

$$D = \sum_{P \in C} m_i P_i - \left(\sum m_i \right) \infty,$$

where each $m_i \geq 0$ and the P_i's are finite points, such that when $P_i \in \operatorname{supp}(D)$ then $\tilde{P_i} \notin \operatorname{supp}\ (D)$, unless $P_i = \tilde{P_i}$ in which case $m_i = 1$. Here $\operatorname{supp}(D)$ is defined to be the set $\operatorname{supp}(D) = \{P \in C \ | m_p \neq 0\}$

For each divisor $D \in \mathbf{D^0}$ there exist a semi-reduced divisor, which is equivalent to D.

Definition 4.3. Let D be a semi-reduced divisor. If $\sum m_i \leq g$, then D is called a reduced divisor.

For all divisors $D \in \mathbf{D^0}$ there exists a unique reduced divisor, which is equivalent to D. This means that there is a unique way to represent each coset in the Jacobian, $\mathbf{J}$. A divisor D is said to be defined over k if it is invariant for all automorphisms of $\overline{k}$ over k. The set of all such divisors form a subgroup under $\mathbf{J}$, and will be denoted by $J(k)$. $J(k)$ is a divisor class group and when k is i finite, then $J(k)$ is a finite abelian group.

When adding reduced divisors together, we are not guaranteed to get a reduced divisor, or even a semi-reduced divisor. Given a divisor D, the following algorithm will generate a semi-reduced divisor, which is equivalent to D.

Algorithm 4.1.

1. Partition the set of points in the support of D into three sets, $\{C_0, C_1, C_2\}$. Such that C_0 contains all special points. A point P is in C_1 if and only if $\tilde{P} \in C_2$ and $m_P \geq m_{\tilde{P}}$ or when $m_{\tilde{P}} = 0$. Then we can write D as,

$$D = \sum_{P \in C_0} m_p P + \sum_{P \in C_1} m_p P + \sum_{P \in C_2} m_p P - m\infty$$

2. Construct the following divisor

$$D_s = D - \sum_{P=(a,b) \in C_2} m_p \mathrm{div}(u-a) - \sum_{P=(a,b) \in C_0} \left\lfloor \frac{m_p}{2} \right\rfloor \mathrm{div}(u-a)$$

$$D_s = \sum_{P \in C_1} (m_P - m_{\tilde{P}})P + \sum_{P \in C_0} \left(m_p - 2\left\lfloor \frac{m_p}{2} \right\rfloor \right) P - m_1\infty$$

for some $m_1 \in \mathbb{Z}$.

Given a semi-reduced divisor D_s, such as the one generated in the algorithm 4.1, the following algorithm will generate a reduced divisor, which is equivalent to D_s

Algorithm 4.2.

1. If $|D_s| \leq g$, where g is the genus of the curve, then D_s is reduced.

2. Pick $g+1$ finite points in suppD_s, $P_1, P_2, ..., P_{g+1}$. Assume $P_i = (a_i, b_i)$ has multiplicity m_i. The points do not need to be distinct, but they can't have multiplicity bigger than $\mathrm{ord}_P(D_s)$.

3. There exists a unique polynomial $g_i(x) \in \overline{k}[x]$ such that $g(a_i) = b_i$, and $g_i^2 + hg_i - g \equiv 0 \; mod \; (x - a_i)^{m_i}$ for each $P_i = (a_i, b_i) \in C_1$. Use Hensel's lemma to generate these polynomial's.

4. Use chinese remainder theorem to generate $g(x) \equiv g_i(x) \bmod (x - a_i)^{m_i}$, for all i

5. Construct $\text{div}(g(x) - y)$

6. $D_s - \text{div}(g(x) - y) = D'$

7. Use algorithm 4.1 to generate a semi-reduced divisor on D'. Then go to step 1 with the semi-reduced divisor.

This algorithm will terminate in finite time.

Example:

Suppose that C is the hyperelliptic curve:

$$y^2 + h(x)y = x^5 + 5x^4 + 6x^2 + x + 3,$$

where $h(x) = x$, and is defined over the field $k = \mathbb{F}_7$, with genus $g = 2$.

Let's consider the divisor $D = 4(1,1) + 2(1,5) + (5,3) - 7\infty$. Using algorithm 4.1, we can find an equivalent semi reduced divisor.

1.
$$\begin{array}{rc} C_0: & \{\} \\ C_1: & \{(1,1),\ (5,3)\} \\ C_2: & \{(1,5)\} \end{array}$$

2.
$$D_s = (4-2)(1,1) + (5,3) - 3\infty$$
$$D_s = 2(1,1), +(5,3) - 3\infty$$

If we further apply algorithm 4.2 to D_s we can find the unique reduced divisor.

1.
$$|D_s| = \sum_{P \in C/\{\infty\}} m_p = 3 \geq 2$$

D_s is not a reduced divisor.

2. $P_1 = (1,1)$, $P_2 = (1,1)$, $P_3 = (5,3)$

3.

$$B(a_0) = b_0$$
$$B(1) = 1$$

The polynomial function $y - 1$ goes through the point $(1,1)$, but does not have a double root at the point. To get such a function we need Hensel's lemma.

Theorem 4.1 (Hensel's Lemma)**.** *Let k be a field and let $F(y) \in k[x][y]$. Let A be an irreducible polynomial in $k[x]$. Suppose $B \in k[x]$ is such that $F(B) \equiv 0 \, mod \, A^r$. If $F'(B) \not\equiv 0 \, mod \, A$, there is a unique $T \in k[x]$, such that $F(B + TA) \equiv 0 \, mod \, A^{r+1}$. In fact, $T \equiv -F'(B)^{-1}((F(B))/A) \, mod \, A$.*

Our problem states that we have a single root at a specified point, but we need a double root, so that $F(B) \equiv 0 \bmod A$ is given.

$$F(B) = B(x)^2 + B(x)h(x) - f(x) = 0$$

If $A(\alpha) = 0$ then $(\alpha, B(\alpha))$ is a point on the curve. This implies that $B(\alpha) = -B(\alpha) - h(x)$, which by definition makes $(\alpha, B(\alpha))$ a special point. But special points come with order one in any semi-reduced divisor. Thus we do not need to find a function with a double zero at $(\alpha, B(\alpha))$. Hence we may assume $2B(x) + h(x) \not\equiv 0 \bmod A$, which is equivalent with $F'(B) \not\equiv mod(A)$

Using Hensel's lemma we can produce a polynomial with a double root.

$$F(y) = y^2 + h(x)y - f(x)$$
$$F(B) = B^2 + xB - f(x) \equiv 0 \bmod A$$

Thus

$$-(x-1)(x^4 + 6x^3 + 6x^2 + 5x + 5) \equiv 0 \bmod A$$

Let $A = (x - 1)$ and $C = -(x^4 + 6x^3 + 6x^2 + 5x + 5)$. Hensel's Lemma tells us that $F(B + TA) \equiv 0 \bmod A^2$ where $T \equiv -F'(B)^{-1} \, (F(A)/A) \bmod A$

$$\begin{aligned}
T(2B + x) &\equiv -F(B)/A \bmod A \\
T(2B + x) &\equiv -C \bmod A \\
T(2 * 1 + 6) &\equiv -C \bmod (x-1) \\
T &\equiv -5C \bmod (x-1) \\
T &\equiv (5x^4 + 2x^3 + 2x^2 + 4x + 4) \bmod (x+6) \\
T &\equiv 3 \bmod (x+6)
\end{aligned}$$

$$B + T(x)A = 1 + 3(x + 6)$$

which is the new unique polynomial $B = 1 + 3(x + 6)$

$$B(a_1) = (b_1)$$
$$B(5) = 3$$

The polynomial function $y - 3$ has a simple zero at the point $(5, 3)$. This gives us the system of polynomial congruence equations,

$$B(x) \equiv 3x - 2 \bmod (x - 1)^2$$
$$B(x) \equiv 3 \bmod (x - 5)$$

To solve a system of polynomial congruence equations, we need the Chinese remainder theorem.

Theorem 4.2 (Chinese remainder Theorem)**.** *Let $A_1, A_2, ..., A_i$, $B_1, B_2, ..., B_i$ $\in k[X]$, where $A_1, A_2, ..., A_i$ are relative coprime.Then the system of polynomial congruences*

$$\begin{gathered} B(x) \equiv B_1 \; mod \, A_1 \\ B(x) \equiv B_2 \; mod \, A_2 \\ \vdots \\ B(x) \equiv B_i \; mod \, A_i \end{gathered}$$

have a unique solution modulo $M = m_1 m_2 ... m_i$, and the solution is given by

$$B = B_1 M_1 \mu_1 + B_2 M_2 \mu_2 + ... + B_i M_i \mu_i$$

where $M_i = M/A_i$ and μ_i is the inverse of $M_i \; mod \, A_i$

Using the Chinese remainder theorem results in:

$$(x - 5)\mu_1 \equiv 1 \bmod (x - 1)^2$$
$$(x - 1)^2 \mu_2 \equiv 1 \bmod (x - 5)$$

$$(x - 1)^2 = x^2 - 2x + 1 = (x - 5)(x + 3) + 2$$

multiplying by 4 which is the inverse of 2

$$1 = 4(x - 1)^2 - 4(x + 3)(x - 5)$$

which gives us $\mu_1 = -4(x + 3)$ and $\mu_2 = 4$.

$$\begin{aligned} &B \equiv (3x - 2)(x - 5)(-4(x + 3)) + 3(x - 1)^2 4 \bmod (x - 1)^2 (x - 5) \\ &B \equiv -40x^2 + 272x - 168 \bmod (x - 1)^2 (x - 5) \\ &B \equiv 2x^2 + 6x \bmod (x - 1)^2 (x - 5) \end{aligned}$$

4. $div(B(x) - y) = div(2x^2 - x - y)$

$$B(x)^2 + h(x)B(x) - f(x) = (x - 1)^3(x - 5)^2$$

so $div(2x^2 - x - y) = 3(1, 1) + 2(5, 3) - 5\infty$

5.

$$\begin{aligned} D_s &\sim 2(1, 1) + (5, 3) - 3\infty - 3(1, 1) - 2(5, 3) + 5\infty \\ &\sim -(1, 1) - (5, 3) + 2\infty \\ &\sim (1, 5) + (5, 6) - 2\infty = D_r \end{aligned}$$

$|D_r| = 2 \leq 2$, so D_r is a reduced divisor.

For practical purposes, such as in Diffie-Hellmann key exchange, one needs to calculate nD where n is an integer. Calculating nD is not a problem, but finding the equivalent reduced divisor is. For example, let's assume D $= P - \infty$, and $n = 13$. One way to find the equivalent reduced divisor to $13P - 13\infty$ is to just apply algorithm 4.1 and 4.2 to it. Due to Hensel's lemma, it's possible to calculate $2P$ efficiently. This opens up the possibility to rather calculate $8P{+}4P{+}P = 13P$. This is the equivalent of three point doublings and three point additions. In a worst case scenario nD will require $\lceil \log_2(n) \rceil$ point doublings and $\lceil \log_2(n) \rceil$ point additions.

Algorithm 4.1 and 4.2 are designed to generate semi-reduced and reduced divisors from a general divisor. When adding multiple points together or doing point doubling more than once, both algorithms can be altered such that it isn't necessary to calculate the divisors at each step. It is sufficient to work with the polynomials.

Given the hyperelliptic curve $y^2 + h(x)y - f(x) = 0$, where $h(x) = x$ and $f(x) = x^5 + 5x^4 + 6x^2 + x + 3$, let's calculate $13P$ where $P = (2, 3)$.

We know that $2P$ is reduced, since $|2P| = 2 \leq 2$.

$$B(2) = 3$$

The polynomial function $y - 3$ goes through the point $(2, 3)$ with multiplicity 1. Using Hensel's lemma it is possible to double the multiplicity. Calculating $2P$:

$$\begin{aligned} F(y) &= y^2 + h(x)y - f(x) \\ F(B) &= B^2 + xB - f(x) \end{aligned}$$

let $A = x - 2 = x + 5$ as we are working over $\mathbb{F}_7$

$$\begin{aligned}
T(x)(2B + x) &\equiv -\frac{F(B)}{A} \bmod (A) \\
T(x)(2 * 3 + x) &\equiv -\frac{3^2 + 3x - f(x)}{x + 5} \bmod (x + 5) \\
T(x)(6 + x) &\equiv x^4 + 6x - 32 \bmod (x + 5) \\
T(x) &\equiv 3 \bmod (x + 5) \\
B + T(x)A &\equiv 3x + 4 \equiv 0 \bmod (x + 5)^2
\end{aligned}$$

Since $2P$ is reduced, it's not necessary to reduce it. So the unique polynomials for $2P$ are $B = 3x + 4$ and $A = x^2 + 3x + 4$. Applying Hensel's lemma to these two polynomials, we can double the multiplicity, and get a multiplicity of 4. Calculating $4P$:

$$\begin{aligned}
T(x)(2B + x) &\equiv -\frac{F(B)}{A} \bmod (A) \\
T(x)(2(3x + 4) + x) &\equiv -\frac{(3x + 4)^2 + (3x + 4)x - f(x)}{x^2 + 3x + 4} \bmod (x^2 + 3x + 4) \\
T(x)(7x + 8) &\equiv x^3 + 2x^2 + 4x + 2 \bmod (x^2 + 3x + 4) \\
T(x) &\equiv 3x + 6 \bmod (x^2 + 3x + 4)
\end{aligned}$$

$$B = B + TA = (3x + 4) + (3x + 6)(x^2 + 3x + 4) \equiv 3x^3 + x^2 + 5x$$

$4P$ is not reduced. The reduced A is given by $A = \frac{B^2 + Bh(x) - f(x)}{(\text{old}A)^2} \equiv 2(x^2 + 1)$, multiplying by 4 makes it monic, $A = x^2 + 1$. Now we can calculate the new reduced $B = -(B + h(x)) \bmod A \equiv -(3x^3 + x^2 + 5x + x) \bmod (x^2 + 1) \equiv 4x + 1$. The polynomials $4x + 1$ and $x^2 + 1$ represent the reduced form of $4P$. Now doubling $4P$, we get $8P$.

$$\begin{aligned}
T(x)(2B + x) &\equiv -\frac{F(B)}{A} \bmod (A) \\
T(x)(2(4x + 1) + x) &\equiv -\frac{(4x + 1)^2 + x(4x + 1) - f(x)}{x^2 + 1} \bmod (x^2 + 1) \\
T(x)(2x + 2) &\equiv x^3 + 5x^2 + 6x + 2 \bmod (x^2 + 1) \\
T(x)(2x + 2) &\equiv 5x + 4 \bmod (x^2 + 1) \\
T(x) &\equiv (5x + 2)(5x + 4) \bmod (x^2 + 1) \\
T(x) &\equiv 2x + 4 \bmod (x^2 + 1)
\end{aligned}$$

$$B + T(x)A = 2x^3 + 4x^2 + 6x + 5$$

It's now possible to calculate the new reduced A.

$$\begin{aligned}
A &= \frac{F(B+TA)}{A^2} \\
A &= \frac{(2x^3+4x^2+6x+5)^2 + x(2x^3+4x^2+6x+5) - f(x)}{(x^2+1)^2} \\
A &= 4x^2+x+1
\end{aligned}$$

If we multiply A by 2, we get $A = x^2+2x+2$. Using this we get $B = -(B+h(x)) \bmod A \equiv -(2x^3+4x^2+6x+5+x) \bmod (x^2+2x+2) \equiv 4x+2$. We now have the two reduced polynomials $4x+2$ and x^2+2x+2 which are equivalent with $8P$. Using the Chinese remainder theorem we can add them together to get $13P$. Starting with P and $4P$, we get:

$$\begin{aligned}
B &\equiv 3 \bmod (x+5) \\
B &\equiv 4x+1 \bmod (x^2+1)
\end{aligned}$$

the Chinese remainder theorem gives us $B \equiv 3x^2+4x+4 \bmod (x^2+1)(x+5)$. Since $(x^2+1)(x+5)$ has a degree of 3, it has to be reduced.

$$A = \frac{B^2+h(x)B-f(x)}{\text{old}A} = 6x^2+2x+4$$

multiplying by 6, results in $A = x^2+5x+3$

$$B = -(B+h(x)) \bmod A \equiv 3x+5$$

With the reduced polynomials corresponding to both $5P$ and $8P$ we can add them together using the Chinese remainder to get $13P$:

$$\begin{aligned}
B &\equiv 3x+5 \bmod (x^2+5x+3) \\
B &\equiv 4x+2 \bmod (x^2+2x+2)
\end{aligned}$$

The Chinese remainder gives us $B \equiv 4x^3+6x^2+x+5 \bmod ((x^2+2x+2)(x^2+5x+3))$. Again $A = (x^2+2x+2)(x^2+5x+3)$ has a multiplicity bigger than 2, and has to be reduced

$$A = \frac{B^2+Bh(x)-f(x)}{\text{old}A} = 2x^2+5x+6$$

multiplying by 4, results in $A = x^2+6x+3$

$$B = -(B+h(x)) \bmod (A) \equiv 4$$

With both the reduced polynomials corresponding to $13P$, it's possible to calculate the corresponding divisor.

If $A(\alpha) = 0$ then $B(\alpha)^2 + B(\alpha)h(\alpha) = f(\alpha)$, which makes $(\alpha, B(\alpha))$ a point on the curve. $A = x^2+6x+3 = (x-(4+i))(x-(4-i))$, which results in the roots $(4+i)$ and $(4-i)$ over $\mathbb{F}_7$. Therefor the divisor to $13P$ is $(4+i,4)+(4-i,4)-2\infty$

<table>
<tr><th colspan="4">Point doubling</th></tr>
<tr><th></th><th>A</th><th>B</th><th>Divisor</th></tr>
<tr><td>P</td><td>$x+5$</td><td>3</td><td>$(2,3)-\infty$</td></tr>
<tr><td>$2P$</td><td>$(x+5)^2$</td><td>$3x+4$</td><td></td></tr>
<tr><td>$4P$</td><td>x^2+1</td><td>$4x+1$</td><td></td></tr>
<tr><td>$8P$</td><td>x^2+2x+2</td><td>$4x+2$</td><td></td></tr>
<tr><th colspan="4">Point addition</th></tr>
<tr><td>$5P$</td><td>x^2+5x+3</td><td>$3x+5$</td><td></td></tr>
<tr><td>$13P$</td><td>x^2+6x+3</td><td>4</td><td>$(4+i,4)+(4-i,4)-2\infty$</td></tr>
</table>

Most Processors today have multiple cores, making it possible to do multiple tasks at the same time. To calculate $5P$ it's not necessary to know $8P$. This makes it possible to do the point doubling and point additions simultaneously. This procedure is described in detail by Lange[3].

5 Ideal Class Group

In this chapter we will assume that the hyper elliptic curve has a characteristic different from 2, resulting in further assumptions that $h(x) = 0$. Let $f(x)$ be a square free monic polynomial with degree $2g + 1$ in $k[x]$, and let $k[x, y]$ be the quadratic extension of $k[x]$, where $y^2 = f(x)$. This extension will be denoted by $\mathcal{O}$

Let I be an ideal under $\mathcal{O}$. Then by definition I is a subgroup of $\mathcal{O}$, such that $\alpha I \subset I$ for all $\alpha \in \mathcal{O}$.

Proposition 5.1. *An ideal $I \in \mathcal{O}$ is generated by $\langle \alpha_1, \alpha_2 \rangle$*
Where $\alpha_1, \alpha_2 \in I$

Proof: Let's denote $k[x]$ by Z. Elements in $\mathcal{O}$ are on the form $\mathcal{O} = \{A + By\}$, where $A, B \in Z$. The elements in Z^2 are on the form $Z^2 = \{A,\ B\}$. The map

$$\mathcal{O} \to Z^2$$
$$A + By \mapsto A,\ B$$

is an isomorphism. The subgroups of Z^2 are isomorphic to Z^2 and Z. Subgroups of $\mathcal{O}$ have to be isomorphic to the subgroups of Z^2. The ideal I is by definition a subgroup under $\mathcal{O}$, and therefore has to be isomorphic to Z^2 or Z. This proves that $I = \langle \alpha_1,\ \alpha_2 \rangle$.

It is possible to say even more about the generators of I. α_1 and α_2 are in $\mathcal{O}$. That implies that they are on the form $\alpha_1 = A_1 + B_1 y$ and $\alpha_2 = A_2 + B_2 y$. If the euclidean algorithm is applied to α_1 and α_2, it is possible to reduce either B_1 or B_2 to zero. This implies that $I = \langle A,\ B + Gy \rangle$, where $A, B, G \in Z$. If a polynomial A is in the ideal I, then Ay is in the ideal I as well. This results in $Ay = AX_1 + (B + Gy)X_2$, where $X_1, X_2 \in \mathcal{O}$. This implies that $A = GX_2$, which further implies that $0 \leq \deg(G) \leq \deg(A)$. It is possible to subtract multiples of A from $B + Gy$ such that $0 \leq \deg(B) < \deg(A)$. This will not change the ideal they generate.

We define the product of two ideals to be $\langle \alpha_1, \alpha_2 \rangle \cdot \langle \beta_1, \beta_2 \rangle = \langle \alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2 \rangle$. Let $I = \langle A, (B + Gy) \rangle$, then $J = \left\langle \frac{A}{v}, \frac{(B+Gy))}{v} \right\rangle$, where $v \in \mathcal{O}$, is called a fractional ideal. For all fractional ideals J there exists an other fractional ideal J', such that $J \cdot J' = \mathcal{O}$. The set of all fractional ideals form a multiplicative group, with $\mathcal{O}$ as the identity element. This group will be denoted by $\mathcal{F}$. An ideal I is called principal, if there exists an $\alpha \in I$ such that $I = \{\alpha\beta \mid \beta \in \mathcal{O}\}$. In other words, an ideal is called principal if it is generated by a single element. The set of all principal ideals form a subgroup under the group of fractional ideals $\mathcal{F}$, and will be denoted by $\mathcal{P}$. The quotient group $\mathcal{F}/\mathcal{P}$, is called the ideal class group, and will be denoted by $Cl(\mathcal{O})$.

Let $I = \langle A, B + Gy\rangle$, where $G = G'H^2$, and where $H \in Z$ and G' is square free. We already know that $G|A$. Let N be the norm, which gives us $N(B + Gy) = B^2 - G^2 f(x) = (B - Gy)(B + Gy) \in I$, and $B^2 - G^2 f(x) \in Z$. If an element is in both Z and I, then it is a multiple of A. Thus $B^2 - G^2 f(x) = AC$, for some $C \in Z$. This implies that $G|B^2$. This further implies that $G'|B$, $H|B$ and $G'H^2|A$. Thus it is possible to write $A = G'HA'$ and $B = G'HB'$, which gives us

$$\begin{aligned} I &= \left\langle G'HA', G'HB' + G'H^2 y\right\rangle \\ &= \langle G'H\rangle \cdot \langle A', B' + Hy\rangle \end{aligned}$$

Using the same arguments as above, $H|A'$ and $H|B'^2$. We can continue this process until G becomes a constant, which is equivalent to assuming that $G = 1$. Which results in $I = \langle A, B + y\rangle$.

Definition 5.1. Let $I = \langle \alpha_1, \alpha_2\rangle$, then we can define the norm of the ideal to be

$$N(I) = \frac{\det_\beta(\alpha_1, \alpha_2)}{\sigma(\det_\beta(\alpha_1, \alpha_2))}$$

where $\beta = \{1, y\}$ is the basis for $\mathcal{O}$ and $\sigma(x)$ is the leading coefficient to x.

Let $I = \langle A, B + y\rangle$, then

$$\begin{aligned} N(I) &= \frac{\det_\beta(\alpha_1, \alpha_2)}{\sigma(\det_\beta(\alpha_1, \alpha_2))} \\ &= \frac{\det_\beta(A, B + y)}{\sigma(\det_\beta(A, B + y))} \\ &= \frac{\det \begin{vmatrix} A & 0 \\ B & 1 \end{vmatrix}}{\sigma\left(\det \begin{vmatrix} A & 0 \\ B & 1 \end{vmatrix}\right)} \\ &= \frac{A}{\sigma(A)} \end{aligned}$$

If A is monic, then $N(I) = A$.

The inverse of the element $\langle A, B + y\rangle$ is $\langle A, B - y\rangle$. Multiplying them together should by definition give an element equivalent to the identity element $\mathcal{O}$.

$$\begin{aligned} &\langle A, B + y\rangle \cdot \langle A, B - y\rangle \\ =&\left\langle A^2, A(B + y), A(B - y), B^2 - y^2\right\rangle \\ =&\left\langle A^2, A(B + y), A(B - y), B^2 - f(x)\right\rangle \end{aligned}$$

Since both B^2 and $f(x)$ are elements in Z their difference has to be as well, thus $B^2 - f(x) \in Z$. All elements that are both in Z and I, are multiples of A.

$$\begin{aligned}
&\langle A, B+y\rangle \cdot \langle A, B-y\rangle \\
=&\left\langle A^2, A(B+y), A(B-y), AC\right\rangle \\
=&\langle A\rangle \cdot \langle A, (B+y), (B-y), C\rangle \\
=&\langle A\rangle \cdot \langle A, 2B, (B+y), C\rangle
\end{aligned}$$

We know that $f(x) = B^2 - AC$. If B^2 and AC have any common divisors, then $f(x)$ can't be square free as previously assumed. Thus $\gcd(A, 2B, C) = 1$. This implies that $\langle A\rangle \cdot \langle A, 2B, (B+y), C\rangle$ is a principal ideal, and equivalent to the identity element $\mathcal{O}$, in $Cl(\mathcal{O})$.

Let $\langle A, B+y\rangle$ be an element in $Cl(\mathcal{O})$, then the element $\langle C, -B+y\rangle \in Cl(\mathcal{O})$ is it's equivalent. If two elements are equivalent, if we then multiply one with the inverse of the other one, we should get the identity element.

$$\begin{aligned}
&\langle A, B+y\rangle \cdot \langle C, -B-y\rangle \\
=&\left\langle AC, A(-B-y), C(B+y), -(B+y)^2\right\rangle \\
=&\left\langle AC, A(B+y), C(B+y), B^2+2By+y^2\right\rangle
\end{aligned}$$

$B^2 - y^2 = B^2 - f = AC$, thus $B^2 \equiv y^2 \bmod AC$. This gives us

$$\begin{aligned}
=&\left\langle AC, A(B+y), C(B+y), 2B^2+2By\right\rangle \\
=&\langle AC, A(B+y), C(B+y), 2B(B+y)\rangle
\end{aligned}$$

As shown earlier, the $\gcd(A, 2B, C) = 1$. We also know that $AC = B^2 - f(x) = B^2 - y^2 = (B+y)(B-y)$ which reduces the element to

$$\langle B+y\rangle$$

This a is principal ideal, which is equivalent to $\mathcal{O}$ in $Cl(\mathcal{O})$, and therefore concludes our proof.

Proposition 5.2. *Each coset in $Cl(\mathcal{O})$ has one element such that*

$$deg(B) < deg(A) < deg(C)$$

and $deg(A) \leq g$

Proof: We have already proved that $\langle A, B+y\rangle \sim \langle C, -B+y\rangle$. Which one is called A and which one is called C does not matter, making it possible to write $\deg(A) \leq \deg(C)$. $\langle A, B+y\rangle$ is equivalent with $\langle A, B-TA+y\rangle$ where $T \in k[x]$, because the difference is a multiple of A. We have previously argued that it is possible to remove all multiples of A from B without changing the ideal, thus it has to be possible to add multiples of A without changing the ideal. This means that we can choose T, such that $\deg(B) < \deg(A)$. We know that $f(x) = B^2 - AC$ and that $\deg(f(x)) = 2g+1$. This implies that the maximum of $2\deg(B)$ and $\deg(A)+\deg(C)$ is equal to $2g+1$. However $2\deg(B)$ can't equal an odd number, forcing $\deg(A)+\deg(C) = 2g+1$. $\deg(A) \leq \deg(C)$, in addition to $\deg(A)+\deg(C) = 2g+1$, implies that $\deg(A) < \deg(C)$ and that $\deg(A) \leq g$, which concludes our proof.

Proposition 5.3. *Let $I_1 = \langle A_1, B_1+y\rangle$ and $I_2 = \langle A_2, B_2+y\rangle$ represent a coset each in $Cl(\mathcal{O})$, then the product I_1I_2 is given by $I_3 = \langle A_3, B_3+y\rangle$ if*

$$\begin{aligned} G &= gcd(A_1, A_2, B_1+B_2) = S_1A_1 + S_2A_2 + S_3(B_1+B_2) \\ A_3 &= \frac{A_1A_2}{G^2} \\ B_3 &= \frac{S_1A_1B_2 + S_2A_2B_1 + S_3(B_1B_2 + f(x))}{G} \end{aligned}$$

Proof: By definition G will divide A_1, A_2 and B_1+B_2, which are the coefficients of y. $B_i^2 \equiv f(x) \bmod G$, as $B_i^2 - f(x) = A_iC_i$ and G divides A_i. $B_1 \equiv -B_2 \bmod G$ which implies that $B_1B_2 + f(x) \equiv 0 \bmod G$. Thus all coefficients of y are divisible by G, and we can write

$$\left\langle \frac{A_1A_2}{G}, \frac{A_1(B_2+y)}{G}, \frac{A_2(B_1+y)}{G}, \frac{B_1B_2+f(x)}{G} + \frac{(B_1+B_2)y}{G} \right\rangle$$

If we now look at

$$\begin{aligned} &\left\langle \frac{S_1A_1(B_2+y)}{G} + \frac{S_2A_2(B_1+y)}{G} + \frac{S_3(B_1B_2+f(x))}{G} + \frac{S_3(B_1+B_2)y}{G} \right\rangle \\ =&\left\langle \frac{S_1A_1B_2 + S_1A_1y + S_2A_2B_1 + S_2A_2y + S_3(B_1B_2+f(x)) + S_3(B_1+B_2)y}{G} \right\rangle \\ =&\left\langle \frac{S_1A_1B_2 + S_2A_2B_1 + S_3(B_1B_2+f(x))}{G} + \frac{(S_1A_1 + S_2A_2 + S_3(B_1+B_2))y}{G} \right\rangle \\ =&\left\langle \frac{S_1A_1B_2 + S_2A_2B_1 + S_3(B_1B_2+f(x))}{G} + y \right\rangle \\ =&\langle B_3 + y\rangle \end{aligned}$$

This means that $\langle B_3+y\rangle$ is in the ideal $\left\langle \frac{A_1A_2}{G}, \frac{A_1(B_2+y)}{G}, \frac{A_2(B_1+y)}{G}, \frac{B_1B_2+f(x)}{G} + \frac{(B_1+B_2)y}{G} \right\rangle$.

The polynomial

$$\begin{aligned} &\frac{A_2}{G}\frac{A_1}{G}(B_2+y) - \frac{A_1}{G}\frac{A_2}{G}(B_1+y) \\ =&\frac{A_2A_1}{G^2}(B_2-B_1) \end{aligned}$$

is contained in the ideal above.

$$\frac{A_2A_1}{G} = \frac{A_2A_1}{G^2}G$$

is contained in the ideal as well. If we now look at the polynomial

$$\begin{aligned}&\frac{B_1+B_2}{G}\frac{A_1}{G}(B_2+y) - \frac{A_1}{G}\frac{B_1B_2+f(x)}{G} + \frac{(B_1+B_2)}{G}y\\ =&\frac{A_1}{G}\frac{B_1B_2+B_2^2-B_1B_2-f(x)}{G}\\ =&\frac{A_2A_1}{G^2}C_2\end{aligned}$$

we see that also this is contained in the ideal. Similarly we can make a polynomial

$$\frac{A_2A_1}{G^2}C_1,$$

which will be contained as well. As these four polynomials are contained in the ideal, the polynomial $\frac{A_1A_2}{G^2}(\gcd(B_2-B_1,G,C_2,C_1))$ has to be as well. By definition, the gcd will divide G, thus it will divide A_i. The gcd divides both B_1-B_2 and B_1+B_2, implying that it divides B_i as well. As $B_i^2 - A_iC_i = f(x)$, the gcd will divide $f(x)$ twice, which is a contradiction, as we have assumed $f(x)$ to be square free. Thus $\gcd(B_2-B_1,G,C_2,C_1)$ has to be one, which means that $\left\langle \frac{A_1A_2}{G^2}, B_3+y\right\rangle$ is contained in $\left\langle \frac{A_1A_2}{G}, \frac{A_1(B_2+y)}{G}, \frac{A_2(B_1+y)}{G}, \frac{B_1B_2+f(x)}{G} + \frac{(B_1+B_2)y}{G}\right\rangle$. To conclude this proof it is necessary to prove the opposite is true. $\frac{A_1A_2}{G}$ is contained in $\left\langle \frac{A_1A_2}{G^2}, B_3+y\right\rangle$. Let's take

$$\begin{aligned}&\frac{A_1}{G}(B_3+y))\\ =&\frac{A_1}{G}\left(\frac{S_1A_1B_2+S_2A_2B_1+S_3(B_1B_2+f(x))}{G}+y\right)\end{aligned}$$

Substituting S_1A_1 with $G-S_2A_2-S_3(B_1+B_2)$, results in

$$\frac{A_1}{G}(B_2+y)+\frac{A_1}{G}\left(\frac{S_2A_2(B_1-B_2)+S_3(-B_2^2+f(x))}{G}\right)$$

This proves that $\frac{A_1}{G}(B_2+y)+\frac{A_1}{G}\left(\frac{S_2A_2(B_1-B_2)+S_3(-B_2^2+f(x))}{G}\right)$ is in the ideal $\left\langle \frac{A_1A_2}{G^2}, B_3+y\right\rangle$. If we look at at

$$\begin{aligned}&\frac{A_1}{G}\left(\frac{S_2A_2(B_1-B_2)+S_3(-B_2^2+f(x))}{G}\right)\\ =&\frac{A_1A_2}{G^2}(S_2(B_1-B_2))+\frac{A_1}{G^2}S_3(f-B_2^2)\end{aligned}$$

it is now clear that $\frac{A_1A_2}{G^2}(S_2(B_1-B_2))$ is a multiple of $\frac{A_1A_2}{G^2}$ and thus is contained in the ideal. From previously we know that $B_i^2 \equiv f(x) \bmod g$, which implies that $\frac{A_1}{G^2}S_3(f-B_2^2)=0$. As both $\frac{A_1}{G^2}S_3(f-B_2^2)$ and $\frac{A_1A_2}{G^2}(S_2(B_1-B_2))$ are in the ideal, and because an ideal is a group, their sum has to be in the ideal as well. Both $\frac{A_1}{G}\left(\frac{S_2A_2(B_1-B_2)+S_3(-B_2^2+f(x))}{G}\right)$ and the sum $\frac{A_1}{G}(B_2+y)+\frac{A_1}{G}\left(\frac{S_2A_2(B_1-B_2)+S_3(-B_2^2+f(x))}{G}\right)$ are in the ideal, which implies that

$$\frac{A_1}{G}(B_2+y)\in\left\langle\frac{A_1A_2}{G^2},B_3+y\right\rangle.$$

Similarly we use

$$\begin{aligned}&\frac{A_2}{G}(B_3+y))\\=&\frac{A_2}{G}\left(\frac{S_1A_1B_2+S_2A_2B_1+S_3(B_1B_2+f(x))}{G}+y\right).\end{aligned}$$

But this time, substituting S_2A_2 with $G-S_1A_1-S_3(B_1+B_2)$ gives us

$$\begin{aligned}&\frac{A_2}{G}(B_1+y)+\frac{A_2}{G}\left(\frac{S_1A_1(B_2-B_1)+S_3(-B_1^2+f(x))}{G}\right)\\=&\frac{A_2}{G}(B_1+y)+\frac{A_1A_2}{G^2}S_1(B_2-B_1)+\frac{A_2S_3}{G^2}(f(x)-B_1^2)\end{aligned}$$

As previously, $B_i^2\equiv f(x)\bmod G$, which results in

$$=\frac{A_2}{G}(B_1+y)+\frac{A_1A_2}{G^2}S_1(B_2-B_1)+0$$

This proves that $\frac{A_2}{G}(B_1+y)+\frac{A_1A_2}{G^2}S_1(B_2-B_1)+0$ is in the ideal. The polynomial $\frac{A_1A_2}{G^2}S_1(B_2-B_1)$ is just a multiple of $\frac{A_1A_2}{G^2}$ and is therefore in the ideal, which implies that

$$\frac{A_2}{G}(B_1+y)\in\left\langle\frac{A_1A_2}{G^2},B_3+y\right\rangle$$

Looking at

$$\begin{aligned}&\frac{B_1+B_2}{G}(B_3+y)\\=&\frac{B_1+B_2}{G}\left(\frac{S_1A_1B_2+S_2A_2B_1+S_3(B_1B_2+f)}{G}+y\right)\end{aligned}$$

substituting $S_3(B_1+B_2)$ with $G-S_1A_1-S_2A_2$ results in

$$\begin{aligned}=&\frac{B_1+B_2}{G}y+\frac{B_1+B_2}{G^2}(S_1A_1B_2+S_2A_2B_1)+\frac{B_1B_2+f(x)}{G^2}(G-S_1A_1-S_2A_2)\\=&\frac{B_1+B_2}{G}y+\frac{(B_1+B_2)S_1A_1B_2}{G^2}+\frac{(B_1+B_2)S_2A_2B_1}{G^2}+\frac{B_1B_2+f(x)}{G}\\&-S_1A_1\frac{B_1B_2+f(x)}{G^2}-S_2A_2\frac{B_1B_2+f(x)}{G^2}\\=&\frac{B_1+B_2}{G}y+\frac{B_1B_2+f(x)}{G}+\frac{S_1A_1}{G^2}(B_2^2-f)+\frac{S_2A_2}{G^2}(B_1^2-f)\end{aligned}$$

From above we know that $B_i^2 - f(x) = A_iC_i$ where $C_i \in k[x]$

$$
\begin{aligned}
=&\frac{B_1+B_2}{G}y + \frac{B_1B_2+f(x)}{G} + \frac{S_1A_1}{G^2}(A_2C_2) + \frac{S_2A_2}{G^2}(A_1C_1)\\
=&\frac{B_1+B_2}{G}y + \frac{B_1B_2+f(x)}{G} + \frac{A_1A_2}{G^2}(S_1C_2) + \frac{A_1A_2}{G^2}(S_2C_1)\\
=&\frac{B_1+B_2}{G}y + \frac{B_1B_2+f(x)}{G} + \frac{A_1A_2}{G^2}(S_1C_2 + S_2C_1)
\end{aligned}
$$

It is clear that $\frac{A_1A_2}{G^2}(S_1C_2+S_2C_1)$ is a multiple of $\frac{A_1A_2}{G^2}$ and is therefore in the ideal. As both $\frac{A_1A_2}{G^2}(S_1C_2+S_2C_1)$ and $\frac{B_1+B_2}{G}y + \frac{B_1B_2+f(x)}{G} + \frac{A_1A_2}{G^2}(S_1C_2+S_2C_1)$ are in the ideal, the difference has to be as well, thus

$$\frac{B_1+B_2}{G}y + \frac{B_1B_2+f(x)}{G} \in \left\langle \frac{A_1A_2}{G^2}, B_3 + y \right\rangle$$

We have now proved that

$$\left\langle \frac{A_1A_2}{G^2}, B_3+y \right\rangle \subset \left\langle \frac{A_1A_2}{G}, \frac{A_1(B_2+y)}{G}, \frac{A_2(B_1+y)}{G}, \frac{B_1B_2+f(x)}{G} + \frac{(B_1+B_2)y}{G} \right\rangle$$

and

$$\left\langle \frac{A_1A_2}{G^2}, B_3+y \right\rangle \supset \left\langle \frac{A_1A_2}{G}, \frac{A_1(B_2+y)}{G}, \frac{A_2(B_1+y)}{G}, \frac{B_1B_2+f(x)}{G} + \frac{(B_1+B_2)y}{G} \right\rangle$$

which concludes our proof.

6 Form Class Group

As in the previous chapter we will continue to assume that the characteristic of the curve has to be different from 2, thus assuming that $h(x) = 0$. Let $f(x)$ be a square free polynomial in $k[x]$, with degree $2g+1$. A binary quadratic form is as the name suggests: a quadratic homogeneous polynomial in two variables

$$Q(x, y) = Ax^2 + 2Bxy + Cy^2,$$

where $A, B, C \in k[x]$ and where $B^2 - AC = f(x)$ is the determinant. For simplicity, binary quadratic forms will be referred to by short form (A, B, C). The polynomial greatest common divisor will denoted by pgcd. If $\text{pgcd}(A, B, C) = 1$, the binary quadratic form is called primitive.

We will assume that all binary quadratic forms are primitive. Two binary quadratic forms Q_1 and Q_2 are said to be equivalent if there exists a matrix $\begin{pmatrix} U & R \\ V & S \end{pmatrix}$ such that

1. $U, R, V, S \in k[x]$
2. $Q_2(x, y) = Q_1(Ux + Ry, Vx + Sy)$
3. $\begin{vmatrix} U & R \\ V & S \end{vmatrix} = 1$

Also, we define $(mA, B, \frac{C}{m})$, where $m \in k^*$, to be equivalent to (A, B, C), thus we can assume A to be monic. A binary quadratic form $Q(x, y) = Ax^2 + 2Bxy + Cy^2$ is called reduced if A is monic, $\deg(A) \leq g$, and

$$\deg(B) < \deg(A) < \deg(C)$$

Proposition 6.1. *A binary quadratic form $Q(x, y) = Ax^2 + 2Bxy + Cy^2$ is equivalent to a reduced binary quadratic form, which is unique.*

Proof: We have defined all binary quadratic forms to be equivalent to a binary quadratic form where A is monic. By using the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, we get $Cx^2 - 2Bxy + Ay^2$. Thus the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ changes places on A and C, and also changes the sign on B, which means that it is possible to get $\deg(A) \leq \deg(C)$.

We know that $B^2 - AC = f(x)$, and that $\deg(f(x)) = 2g+1$. This implies that maximum $(2\deg(B), \deg(A) + \deg(C)) = 2g+1$. Because $2\deg(B)$ can't equal

$2g+1$, we know that $\deg(A)+\deg(C)=2g+1$. This, in addition to the fact that $\deg(A)\leq\deg(C)$, implies that

$$\deg(A)<\deg(C)$$

Furthermore, this implies that $\deg(A)\leq g$. This proves that there exists a reduced binary quadratic form which is equivalent to any given binary quadratic form. To conclude the proof, we still need to prove that two reduced binary quadratic forms can't be equivalent.

Assuming there exist two reduced binary quadratic forms $Q_1(x,y)$ and $Q_2(x,y)$ which are equivalent, there must exist a matrix $\begin{pmatrix} U & R \\ V & S \end{pmatrix}$ with determinant 1, such that $Q_2(x,y)=Q_1(Ux+Ry,Vx+Sy)$.

$$A_1(Ux+Ry)^2+2B_1(Ux+Ry)(Vx+Sy)+C_1(Vx+Sy)^2$$

$$\begin{aligned}
=&A_1(U^2x^2+2URxy+R^2y^2)\\
+&2B_1(UVx^2+USxy+RVxy+RSy^2)\\
+&C_1(V^2x^2+2VSxy+S^2y^2)\\
\\
=&x^2(A_1U^2+2B_1UV+C_1V^2)\\
+&xy(2A_1UR+2B_1(US+RV)+2C_1VS)\\
+&y^2(A_1R^2+2B_1RS+C_1S^2)
\end{aligned}$$

This results in

$$\begin{aligned}
A_2 &= (A_1U^2+2B_1UV+C_1V^2)\\
A_2 &= (A_1U^2+2B_1UV+\left(\frac{B_1^2-f(x)}{A}\right)V^2)\\
A_2A_1 &= A_1^2U^2+2A_1B_1UV+B_1^2V^2-f(x)V^2\\
A_2A_1 &= (A_1U+B_1V)^2-f(x)V^2
\end{aligned}$$

As both $Q_1(x,y)$ and $Q_2(x,y)$ are reduced, we know that $\deg(A_1)\leq g$ and $\deg(A_2)\leq g$. This implies that $\deg(A_2A_1)<\deg(f(x))=2g+1$. As A_2A_1 is given by $A_2A_1=(A_1U+B_1V)^2-f(x)V^2$, which implies that $V=0$. This results in $A_2A_1=(A_1U)^2$. Which further implies that A_2 is given by $A_2=A_1U^2$. With $V=0$, we get the matrix $\begin{pmatrix} U & R \\ 0 & S \end{pmatrix}$. By definition, this matrix has a determinant of one. This implies that $US=1$ and further that $S=U^{-1}$. As $S=U^{-1}$, we know that $U,S\in k^*$, which further implies that $\deg(A_1)=\deg(A_2)$. As both A_1 and A_2 are monic by definition and $A_2=A_1U^2$, we know that $U=\pm1$. As previously stated, B_2 is given by $2B_2=(2A_1UR+2B_1(US+RV)+2C_1VS)$. However we know that $V=0$, thus $2B_2=2A_1UR+2B_1US$. By definition $\deg(B_2)<\deg(A_2)=\deg(A_1)$. This implies that $R=0$, such that $2B_2=2B_1$.

To get a determinant of one, $U = S = \pm 1$. From previous calculations we know that $Q_2(x, y)$ is given by

$$\begin{aligned}
&=x^2(A_1U^2 + 2B_1UV + C_1V^2)\\
&+xy(2A_1UR + 2B_1(US + RV) + 2C_1VS)\\
&+y^2(A_1R^2 + 2B_1RS + C_1S^2)
\end{aligned}$$

$V = R = 0$, which results in $x^2(A_1U^2) + xy(2B_1US) + y^2(C_1S^2)$, which implies that

$$\begin{aligned}
A_2 &= A_1U^2\\
2B_2 &= 2B_1US\\
C_2 &= C_1S^2
\end{aligned}$$

This proves that both $U = S = -1$ and $U = S = 1$ result in $Q_1(x, y) = Q_2(x, y)$, which contradicts our assumption, and concludes our proof.

Definition 6.1 (Form Class Group)**.** The set of equivalence classes on binary quadratic forms with determinant f form an Abelian group under the group law: $(A_1, B_1, C_1) \cdot (A_2, B_2, C_2) = (A_3, B_3, C_3)$

$$\begin{aligned}
G &= \text{pgcd}(A_1, A_2, (B_1 + B_2)) = \alpha_1 A_1 + \alpha_2 A_2 + \alpha_3(B_1 + B_2)\\
A_3 &= \frac{A_1A_2}{G^2}\\
B_3 &= \frac{\alpha_1 A_1 B_2 + \alpha_2 A_2 B_1 + \alpha_3(B_1B_2 + f)}{G}\\
C_3 &= \frac{B_3^2 + f}{A_3}
\end{aligned}$$

This group is called the form class group, and will be denoted by $Cl(F)$.

The unity element in $Cl(F)$ is $(1, 0, -f)$. To prove this, let's take

$$(A, B, C) \cdot (1, 0, -f)$$

which should be equivalent to (A, B, C).

$$G = \text{pgcd}(A, 1, (B + 0)) = \alpha_1 A + \alpha_2 + \alpha_3(B + 0) = 1$$

which implies that $\alpha_1 = \alpha_3 = 0$ and $\alpha_2 = 1$

$$\begin{aligned}
A_3 &= \frac{A}{G} = A\\
B_3 &= \frac{0 + B + 0}{1} = B\\
C_3 &= \frac{B^2 - f}{A} = C
\end{aligned}$$

7 The isomorphism between $Cl(\mathcal{O})$ and $Cl(F)$

Theorem 7.1. *The ideal class group $Cl(\mathcal{O})$, is isomorphic to the form class group $Cl(F)$.*

This theorem will be proved through a series of lemmas. We will start with proving that there exists a well defined map ϕ from $Cl(F)$ to $Cl(\mathcal{O})$.

For a map to be well defined, it can't map one element to several elements, or classes in this case. So we need to prove that one equivalence class maps to no more than one coset in the ideal class group.
The form class group consists of equivalence classes, where equivalences are based on matrices with determinants equal to one. The group of all such matrices, is called $SL_2(Z)$. Thus it suffices to look at how the generators of this group behave when mapped.

Lemma 7.2. $SL_2(Z) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \;|A, B, C, D \in k[x],\; AD - BC = 1 \right\}$ *and is generated by*

$$T_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$T_2(M) = \begin{pmatrix} 1 & M \\ 0 & 1 \end{pmatrix}$$

where $M \in k[x]$

Proof: Let $W = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be any matrix in $SL_2(Z)$. If $\deg(C) < \deg(A)$ we can write the matrix as

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -C & -D \\ A & B \end{pmatrix}$$
$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = T_1 \begin{pmatrix} -C & -D \\ A & B \end{pmatrix}$$

Thus we can safely assume that $\deg(A) \leq \deg(C)$. Because $\deg(A) \leq \deg(C)$ there exists a Q and an R, such that

$$C = QA + R$$

where $Q, R \in k[x]$, and $\deg(R) < \deg(A)$, which implies that it is possible to write

$$\begin{aligned}&\begin{pmatrix} A & B \\ C & D \end{pmatrix}\\ &= \begin{pmatrix} A & B \\ QA + R & D \end{pmatrix}\\ &= \begin{pmatrix} 1 & 0 \\ Q & 1 \end{pmatrix}\begin{pmatrix} A & B \\ R & D - QB \end{pmatrix}\end{aligned}$$

By definition of the reminder, $\deg(R) < \deg(A)$ and we know that $\deg(A) \leq \deg(C)$, which implies that $\deg(R) < \deg(C)$. It is possible to repeat this process, and because $\deg(R) < \deg(C)$, we get a descending chain that is bound to terminate in finitely many steps. Thus after finitely many steps, C becomes 0. So we can write $W = E_1 E_2 ... E_s W'$, where $E_i = \begin{pmatrix} 1 & 0 \\ Q_i & 1 \end{pmatrix}$ and $W' = \begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix}$ The matrix E_i

$$\begin{aligned}&= \begin{pmatrix} 1 & 0 \\ Q_i & 1 \end{pmatrix}\\ &= T_3(-1)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -Q_i \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\\ &= T_3(-1)T_1T_2(-Q_i)T_1\end{aligned}$$

where

$$\begin{aligned}T_3(\alpha) &= \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}\\ &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & \alpha^{-1} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & \alpha^{-1} \\ 0 & 1 \end{pmatrix}\\ &= T_1T_2(\alpha^{-1})T_1T_2(\alpha)T_1T_2(\alpha^{-1})\end{aligned}$$

This proves that the matrices E_i are just multiples of T_1 and $T_2(M)$. The determinant of E_i is one for all i. By definition of the matrix W, its determinant is equal to one as well. We know that $\det(AB) = \det(A) * \det(B)$. This implies that the determinant of the matrix $W' = \begin{pmatrix} A' & B' \\ 0 & D' \end{pmatrix}$ has to be one. Which further implies that $D' = A'^{-1}$, resulting in the matrix

$$\begin{aligned}W' &= \begin{pmatrix} A' & B' \\ 0 & A'^{-1} \end{pmatrix}\\ &= \begin{pmatrix} 1 & A'B' \\ 0 & 1 \end{pmatrix}\begin{pmatrix} A' & 0 \\ 0 & A'^{-1} \end{pmatrix}\\ &= T_2(A'B')T_3(A')\end{aligned}$$

This implies that W' is just a multiple of T_1 and $T_2(M)$. We know that $W = E_1E_2...E_sW'$, and we just proved that the matrices E_i and W' are multiples of T_1 and $T_2(M)$, which in turn proves that W is a multiple of T_1 and $T_2(M)$. This proves that $SL_2(Z)$ is generated by T_1 and $T_2(M)$.

Lemma 7.3. *Let ϕ : be a map from $Cl(F)$ to $Cl(\mathcal{O})$, such that*

$$\phi : Ax^2 + 2Bxy + Cy^2 \mapsto \langle A, B + y\rangle$$

By this, ϕ is a well defined surjective map.

Proof: As a result of lemma 7.2, it is sufficient to look at how the generators T_1 and $T_2(M)$, map. The matrix T_1 maps (A, B, C) to $(C, -B, A)$.

$$(A, B, C) \mapsto \langle A, B + y\rangle$$
$$(C, -B, A) \mapsto \langle C, -B + y\rangle$$

$\langle A, B + y\rangle$ and $\langle C, -B + y\rangle$ have already been proved to be equivalent to each other. The matrix $T_2(M)$ maps $(A, B, C) \in Cl(F)$, to $(A, (B + AM), C)$, where $M \in k[x]$.

$$(A, B, C) \mapsto \langle A, B + y\rangle$$
$$(A, (B + AM), C) \mapsto \langle A, (B + AM) + y\rangle$$

$\langle A, B + y\rangle$ and $\langle A, (B + AM) + y\rangle$ are equivalent to each other, because it is only a multiple of A that differentiates them.

We also defined $(mA, B, \frac{C}{m})$ to be equivalent to (A, B, C) therefore we have to prove this as well.

$$(A, B, C) \mapsto \langle A, B + y\rangle$$
$$\left(mA, B, \frac{C}{m}\right) \mapsto \langle mA, B + y\rangle$$

$\langle mA, B + y\rangle$ and $\langle A, B + y\rangle$ are equivalent to each other, because m is an element in k^*, thus it does not change the ideal it generates. This proves that the map ϕ is well defined, as it maps one class to one coset. Proposition 6.1 guarantees that all binary quadratic forms are equivalent to a reduced binary quadratic form, where $\deg(B) < \deg(A) < \deg(C)$ and $\deg(A) \leq g$. Proposition 5.2 guarantees that each coset in the ideal class group $Cl(\mathcal{O})$ has one element such that $\deg(B) < \deg(A) < \deg(C)$ and $\deg(A) \leq g$. As all elements in the form class group $Cl(F)$ are equivalent to an element on the form $\deg(B) < \deg(A) < \deg(C)$ and $\deg(A) \leq g$, and all cosets in the ideal class group $Cl(\mathcal{O})$ have one element on the same form, the map ϕ has to be surjective. This concludes our proof.

Lemma 7.4. *Let $I = \langle \alpha_1, \alpha_2 \rangle$, where $\alpha_1, \alpha_2 \in \mathcal{O}$, and ψ be a map form $Cl(\mathcal{O})$ to $Cl(F)$, such that*

$$\psi : \langle \alpha_1, \alpha_2 \rangle \mapsto \frac{N(\alpha_1 x + \alpha_2 y)}{N(I)} = q_{\alpha_1,\alpha_2}$$

where $N(\alpha_1 x + \alpha_2 y) = (\alpha_1 x + \alpha_2 y)(\tilde{\alpha_1} x + \tilde{\alpha_2} y)$, and $\tilde{\alpha_1}$ and $\tilde{\alpha_2}$ are equal to α_1 and α_2 conjugated. $N(I) = \frac{det_\beta(\alpha_1,\alpha_2)}{\sigma(det_\beta(\alpha_1,\alpha_2))}$ as defined in definition 5.1
By this ψ is a well defined and surjective map.

Proof:

$$\begin{aligned}
&N(\alpha_1 x, \alpha_2 y)\\
=&(\alpha_1 x + \alpha_2 y)(\tilde{\alpha_1} x + \tilde{\alpha_2} y)\\
=&\alpha_1\tilde{\alpha_1}x^2 + (\alpha_1\tilde{\alpha_2} + \alpha_2\tilde{\alpha_1})xy + \alpha_2\tilde{\alpha_2}y^2
\end{aligned}$$

We know that $\alpha_1\tilde{\alpha_1}$, $(\alpha_1\tilde{\alpha_2}+\alpha_2\tilde{\alpha_1})$ and $\alpha_2\tilde{\alpha_2}$ are in the ideal I. We also know that $y^2 = f(x)$, which is in $k[x]$. This implies that $(\alpha_1\tilde{\alpha_1}), (\alpha_1\tilde{\alpha_2} + \alpha_2\tilde{\alpha_1})$, and $(\alpha_2\tilde{\alpha_2})$ are in $k[x]$ and thus multiples of $N(I)$. This implies that $(\alpha_1\tilde{\alpha_1}), (\alpha_1\tilde{\alpha_2} + \alpha_2\tilde{\alpha_1})$, and $(\alpha_2\tilde{\alpha_2})$ are divisible by $N(I)$.

This further implies that it is possible to write

$$\begin{aligned}
\frac{\alpha_1\tilde{\alpha_1}}{N(I)} &= A\\
\frac{(\alpha_1\tilde{\alpha_2} + \alpha_2\tilde{\alpha_1})}{N(I)} &= 2B\\
\frac{\alpha_2\tilde{\alpha_2}}{N(I)} &= C
\end{aligned}$$

thus proving that $\frac{N(\alpha_1 x+\alpha_2 y)}{N(I)}$ is a binary quadratic form.

The discriminant to $Ax^2 + 2Bxy + Cy^2$ is

$$\begin{aligned}
&(2B)^2 - 4AC\\
=&\left(\frac{\alpha_1\tilde{\alpha_2} + \alpha_2\tilde{\alpha_1}}{N(I)}\right)^2 - 4\left(\frac{\alpha_1\tilde{\alpha_1}\alpha_2\tilde{\alpha_2}}{N(I)^2}\right)\\
=&\frac{(\alpha_1\tilde{\alpha_2} + \alpha_2\tilde{\alpha_1})^2 - 4\alpha_1\tilde{\alpha_1}\alpha_2\tilde{\alpha_2}}{N(I)^2}\\
=&\frac{(\alpha_1\tilde{\alpha_2} - \alpha_2\tilde{\alpha_1})^2}{N(I)^2}
\end{aligned}$$

Let $\alpha_1 = A$ and $\alpha_2 = B + y$, resulting in

$$\begin{aligned}
&\frac{(\alpha_1\tilde{\alpha_2} - \alpha_2\tilde{\alpha_1})^2}{N(I)^2} \\
=&\frac{(A(B-y) - (B+y)A)^2}{N(I)^2} \\
=&\frac{4A^2y^2}{N(I)^2} \\
=&4f(x)
\end{aligned}$$

as $y^2 = f(x)$. The discriminant to a basis $\langle A, B + y\rangle$ is $4f(x)$, thus it is the same as for $\psi(Ax^2 + 2Bxy + Cy^2)$.

Proposition 5.1 states that an ideal I in $\mathcal{O}$ is on the form $\langle\alpha_1, \alpha_2\rangle$. In the proof we went even further, by proving that an ideal in $\mathcal{O}$ is actually on the form $\langle A, B + y\rangle$. None of the operations used in the proof will change the discriminant.

It is clear that $\langle\alpha_1, \alpha_2\rangle$ is equivalent to $\langle U\alpha_1 + R\alpha_2, V\alpha_1 + S\alpha_2\rangle$. Thus we need to prove that q_{α_1,α_2} is equivalent to $q_{U\alpha_1+R\alpha_2,V\alpha_1+S\alpha_2}$. Let $\begin{pmatrix} U & R \\ V & S \end{pmatrix} \in SL_2(Z)$.

If we look at

$$\begin{aligned}
q_{\alpha_1,\alpha_2} &= \frac{N(\alpha_1 x + \alpha_2 y)}{N(I)} \\
&= \frac{\alpha_1\tilde{\alpha_1}x^2 + (\alpha_1\tilde{\alpha_2} + \alpha_2\tilde{\alpha_1})xy + \alpha_2\tilde{\alpha_2}y^2}{N(I)}
\end{aligned}$$

which again gives us

$$\begin{aligned}
N(I)A &= \alpha_1\tilde{\alpha_1} \\
N(I)2B &= (\alpha_1\tilde{\alpha_2} + \alpha_2\tilde{\alpha_1}) \\
N(I)C &= \alpha_2\tilde{\alpha_2}
\end{aligned}$$

Looking at $q_{U\alpha_1+R\alpha_2,V\alpha_1+S\alpha_2}$ gives us

$$\begin{aligned}
&\left(\frac{(U\alpha_1+R\alpha_2)(U\tilde{\alpha}_1+R\tilde{\alpha}_2)}{N(I)}\right)x^2\\
&+\left(\frac{(U\alpha_1+R\alpha_2)(V\tilde{\alpha}_1+S\tilde{\alpha}_2)+(V\alpha_1+S\alpha_2)(U\tilde{\alpha}_1+R\tilde{\alpha}_2)}{N(I)}\right)xy\\
&+\left(\frac{(V\alpha_1+S\alpha_2)(V\tilde{\alpha}_1+S\tilde{\alpha}_2)}{N(I)}\right)y^2
\end{aligned}$$

$$\begin{aligned}
=&\left(\frac{U^2(\alpha_1\tilde{\alpha}_1)+RU(\alpha_1\tilde{\alpha}_2+\tilde{\alpha}_1\alpha_2)+R^2(\alpha_2\tilde{\alpha}_2)}{N(I)}\right)x^2\\
&+\left(\frac{2VU(\alpha_1\tilde{\alpha}_1)+(US+RV)(\alpha_1\tilde{\alpha}_2+\alpha_2\tilde{\alpha}_1)+2SR(\alpha_2\tilde{\alpha}_2)}{N(I)}\right)xy\\
&+\left(\frac{V^2(\alpha_1\tilde{\alpha}_1)+VS(\alpha_1\tilde{\alpha}_2+\alpha_2\tilde{\alpha}_1)+S^2(\alpha_2\tilde{\alpha}_2)}{N(I)}\right)y^2
\end{aligned}$$

which gives us

$$\begin{aligned}
&\left(\frac{N(I)(U^2A+RU2B+R^2C)}{N(I)}\right)x^2\\
&+\left(\frac{N(I)(2VUA+(US+RV)2B+2SRC)}{N(I)}\right)xy\\
&+\left(\frac{N(I)(V^2A+VS2B+S^2C)}{N(I)}\right)y^2\\
=&\left(AU^2+2BRU+CR^2\right)x^2\\
&+(2AUV+2B(US+RV)+2CRS)\,xy\\
&+\left(AV^2+2BVS+CS^2\right)x^2
\end{aligned}$$

We see that

$$Ax^2+2Bxy+Cy^2$$

and

$$\begin{aligned}
&\left(AU^2+2BRU+CR^2\right)x^2\\
&+(2AUV+2B(US+RV)+2CRS)\,xy\\
&+\left(AV^2+2BVS+CS^2\right)x^2
\end{aligned}$$

are equivalent under $\begin{pmatrix}U & V\\ R & S\end{pmatrix}$. As $\begin{pmatrix}U & R\\ V & S\end{pmatrix}$ has a determinant of one, then so does $\begin{pmatrix}U & V\\ R & S\end{pmatrix}$, thus it is in $SL_2(Z)$.

$$q_{\alpha_1,\alpha_2}=Ax^2+2Bxy+Cy^2$$

and

$$\begin{aligned}&q_{U\alpha_1+R\alpha_2,V\alpha_1+S\alpha_2}\\ =&\left(AU^2+2BRU+CR^2\right)x^2\\ &+(2AUV+2B(US+RV)+2CRS)\,xy\\ &+\left(AV^2+2BVS+CS^2\right)y^2\end{aligned}$$

implying that q_{α_1,α_2} and $q_{U\alpha_1+R\alpha_2,V\alpha_1+S\alpha_2}$ are equivalent. This proves that the map ψ is well defined.

Again, we use proposition 6.1 and 5.2 which guarantees that all binary quadratic forms in $Cl(F)$ and cosets in $Cl(\mathcal{O})$ are equivalent to an element, where $\deg(B)<\deg(A)<\deg(C)$ and $\deg(A)\leq g$. As all elements in the form class group $Cl(F)$ are equivalent to an element on the form $\deg(B)<\deg(A)<\deg(C)$ and $\deg(A)\leq g$, and all cosets in the ideal class group $Cl(\mathcal{O})$ have one element on the same form, and the fact that ψ is well defined, this implies that ψ has to be surjective. This concludes our proof.

Lemma 7.5. *Let ϕ be as defined in lemma 7.3, and ψ be as defined in lemma 7.4, then*

$$\begin{aligned}&\phi\circ\psi\\ &\textit{and}\\ &\psi\circ\phi\end{aligned}$$

are identity maps.

Proof: For $\phi\circ\psi$ to be an identity map, then

$$\phi(\psi(\langle A,B+y\rangle))=\langle A,B+y\rangle$$

$$\begin{aligned}&\psi(\langle A,-B+y\rangle)\\ =&q_{\alpha_1,\alpha_2}\\ =&\frac{\alpha_1\tilde{\alpha_1}x^2+(\alpha_1\tilde{\alpha_2}+\alpha_2\tilde{\alpha_1})xy+\alpha_2\tilde{\alpha_2}y^2}{N(I)}\end{aligned}$$

We know that $\alpha_1=A$ og $\alpha_2=B+y$, which results in

$$\begin{aligned}&\psi(\langle A,B+y\rangle)\\ =&\frac{A^2x^2+2ABxy+(B^2-f)y^2}{N(I)}\end{aligned}$$

In the form class group, we know that A is monic, thus $N(I) = A$

$$\begin{aligned}&= \frac{A^2x^2 + 2ABxy + (B^2 - f)y^2}{N(I)} \\ &= Ax^2 + 2Bxy + (\frac{B^2 - f}{A})y^2 \\ \psi(\langle A, B + y\rangle) &= Ax^2 + 2Bxy + Cy^2\end{aligned}$$

$$\begin{aligned}&\phi(\psi(\langle A, B + y\rangle)) \\ &= \phi(Ax^2 + 2Bxy + Cy^2) \\ \phi(\psi(\langle A, B + y\rangle)) &= \langle A, B + y\rangle\end{aligned}$$

This proves that $\phi \circ \psi$ is an identity mapping. We know that ψ is surjective. By definition, it is then possible to write all binary quadratic forms as $q = \psi(I)$ for some ideal I. This further implies that $\psi(\phi(q)) = \psi(\phi(\psi(I)))$. We just proved that $\phi \circ \psi$ is an identity mapping, thus $\psi(\phi(q)) = \psi(\phi(\psi(I))) = \psi(I) = q$, which proves that $\psi \circ \phi$ is an identity mapping as well, and concludes our proof.

Definition 7.1. Let q_1 and q_2 be in $Cl(F)$, and $\cdot$ be the group operation in $Cl(\mathcal{O})$. We then define the group operation in $Cl(F)$ to be

$$\psi(\phi(q_1) \cdot \phi(q_2))$$

To prove that ϕ is an homomorphism, let q_1 and q_2 be binary quadratic forms. Then, by definition,

$$\phi(q_1q_2) = \phi(\psi(\phi(q_1) \cdot \phi(q_2)))$$

As $\phi \circ \psi$ is an identity mapping, this implies that

$$\phi(q_1q_2) = \phi(\psi(\phi(q_1) \cdot \phi(q_2))) = \phi(q_1)\phi(q_2)$$

which proves that ϕ is an homomorphism.

To prove that ψ is an homomorphism, let I_1 and I_2 be ideals in $Cl(\mathcal{O})$. Lemma 7.3 guarantees that ϕ is surjective, and all ideals in $Cl(\mathcal{O})$ can therefore be written as $I = \phi(q)$. This gives us

$$\psi(I_1 \cdot I_2) = \psi(\phi(q_1) \cdot \phi(q_2))$$

This is the definition of the group operation in $Cl(F)$, thus

$$\begin{aligned}\psi(I_1 \cdot I_2) &= \psi(\phi(q_1) \cdot \phi(q_2)) \\ &= q_1q_2\end{aligned}$$

As $\phi(q_i) = I_i$, for $i = 1, 2$, then $\psi(I_i) = q_i$. This gives us

$$q_1q_2 = \psi(I_1)\psi(I_2)$$

This proves that ψ is an homomorphism and concludes the proof of theorem 7.1.

8 Conclusion

We have described the four faces of hyperelliptic curves and proved that the form class group and ideal class group are isomorphic. We have also described an algorithm that does group operations strictly in the jacobian of hyperelliptic curves. Further work would have included comparison of the group operations in the jacobian and the ideal class group, to see which one is theoretically faster. Ease of visualization would have been emphasized as well, as it seems that some computer security researchers are reluctant to use hyperelliptic curve cryptography because of its complexity. A special case of hyperelliptic curves have recently been given attention as a candidate as the post quantum cryptographic algorithm. Supersingular isogeny Diffie–Hellman key exchange (SIDH), as it is called is based on supersingular elliptic curves and the isogenies between them.

References

[1] Robert J. Zuccherato Alfred J. Menezes Yi-Hong Wu. “An elementary introduction to hyperelliptic curves”. In: (1996). URL: https://www.math.uwaterloo.ca/~ajmeneze/publications/hyperelliptic.pdf.

[2] William Fulton. *Algebraic curves.* http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf. 2008.

[3] Tanja Lange. “Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae”. In: (2003). URL: https://eprint.iacr.org/2002/121.pdf.

[4] Krysta M. Svore Kristin Lauter Martin Roetteler Michael Naehrig. “Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms”. In: (2017). URL: https://arxiv.org/abs/1706.06752v3.

[5] Joseph H. Silvermann. *The Arithmetic of Elliptic Curves.* Springer Sience+Business Media, LLC, 2016. ISBN: 978-0-387-09493-9.