PMATH 940: COMPUTATIONAL ALGEBRAIC NUMBER THEORY

HEESUNG YANG

1. January 6: Multiplication and division

Many problems in algebraic number theory (especially computational ones) require good manipulation of polynomials. Addition of two polynomials is easy. Let $A(x) := a_n x^n + \cdots + a_0$ and $B(x) = b_m x^m + \cdots + b_0$. Then $C(x) = A + B$ is just

$$C(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i)x^i.$$

There is a faster method to multiply two polynomials than the naïve method we learnt in high school.

Example. Let $A(x) = a_1 x + a_0$ and $B(x) = b_1 x + b_0$. Then

$$A(x)B(x) = a_1 b_1 x^2 + (a_1 b_0 + b_1 a_0)x + a_0 b_0.$$

We need four multiplications and one addition if we are to use the naïve method.

On a computer, addition is very fast, but multiplication is not as fast. The speed of this method depends on the multiplication. The addition is irrelevant since it is "very fast".

Consider $c_0 = a_0 b_0, c_2 = a_1 b_1, d = (a_1 - a_0)(b_1 - b_0)$ and $c_1 = c_0 + c_2 - d$. We now claim that $A(x)B(x) = c_2 x^2 + c_1 x + c_0$ requires three multiplications and four additions. Thus this is faster. This can be scaled up in a number of ways. The easiest method is by using it recursively. Others include fast Fourier transforms, or higher order approximation.

Example. Let $A(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0 = A_1(x)x^2 + A_0(x)$ and $B(x) = b_3 x^3 + b_2 x^2 + b_1 x + b_0 = B_1(x)x^2 + B_0(x)$. Then $A(x)B(x) = C_2(x)x^4 + C_1(x)x^2 + C_0(x)$, where

$$\begin{aligned}
C_2(x) &= A_1(x)B_1(x) = (a_3 x + a_2)(b_3 x + b_2)\\
C_0(x) &= A_0(x)B_0(x) = (a_1 x + a_0)(b_1 x + b_0)\\
D(x) &= (A_1(x) - A_0(x))(B_1(x) - B_0(x)) = ((a_3 - a_1)x + (a_2 - a_0))((b_3 - b_1)x + (b_2 - b_0))\\
C_1(x) &= C_0(x) + C_2(x) - D(x).
\end{aligned}$$

Thus it takes nine multiplications to multiply $A(x)$ and $B(x)$. The naïve method would take 16 multiplications.

In general, to multiply two $2^k - 1$ degree polynomials would take $(2^k)^2 = 4^k$ in the naïve method, and 3^k using this recursive method. This becomes really important for large-degree polynomials.

Date: 4 April 2016.

Now we move on to division of polynomials. We saw that the high school didn't get it "right" when it comes to multiplication. It turns out that the standard method learnt in high school is exactly what we would want to use.

Let $A(x), B(x)$ be two polynomials. We wish to find $Q(x)$ and the remainder $R(x)$, with $R(x) < \deg(B)$, such that $A(x) = B(x)Q(x) + R(x)$. First, initialize wth $R(x) = A(x)$ and $Q(x) = 0$. Then loop the following computations as necessary (lcoeff(A) denotes the leading coefficient of A):

(1) If $\deg R < \deg B$, then we are done.
(2) $Q_{\text{new}} = Q(x) + \dfrac{\text{lcoeff}(R)}{\text{lcoeff}(B)} x^{\deg R - \deg B}$
(3) $R_{\text{new}} = R(x) - \dfrac{\text{lcoeff}(R)}{\text{lcoeff}(B)} x^{\deg R - \deg B} B(x)$.
(4) Rinse and repeat until the halting step is reached.

Example. $A(x) = x^3 + 3x + 1$ and $B(x) = x^2 + 2$. Start with $R(x) = x^3 + 3x + 1$ and $Q + 0$. Applying the above algorithm once gives me $Q(x) = x$ and $R(x) = x^3 + 3x + 1 - x(x^3 + 2) = x + 1$. We se that $\deg R < \deg B$, so indeed $Q(x) = x$ and $R(x) = x + 1$.

Definition 1. We say $C(x)$ is a *common divisor* of $A(x)$ and $B(x)$ if $C(x) \mid A(x)$ and $C(x) \,|\, B(x)$.

Definition 2. A common divisor $G(x)$ is the *greatest common divisor* if for all other common divisors $C(x)$ we have $C(x) \,|\, G(x)$.

There is a standard (and very old) method to find the greatest common divisor, called the *Euclidean algorithm.* Initialize $S(x) = A(x), T(x) = B(x)$ and loop the following algorithm as necessary:

(1) If $T(x) = 0$, then $S(x)$ is the gcd.
(2) Write $S(x) = Q(x)T(x) + R(x)$
(3) Set $S_{\text{new}}(x) = T(x), T_{\text{new}}(x) = R(x)$.
(4) Repeat the steps until the algorithm halts.

We do NOT want to do this over $\mathbb{R}[x]$ or $\mathbb{C}[x]$, since it's difficult to tell the difference between the case when $R(x)$ is zero and when $R(x)$ is close to zero. In fact, in some cases it is *impossible* to tell. Thus we need a "nice" field where such mess does not happen.

Example. Recall that

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Consider $A(x) = x^2 - 6 \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2}, B(x) = x - \pi$. Finding the gcd of these two guys is annoying.

Example. Find the gcd of $x^3 - 1$ and $x^5 - 1$.

$S(x)$	$T(x)$	$S(x) = Q(x)T(x) + R(x)$
$x^3 - 1$	$x^5 - 1$	$x^3 - 1 = 0 \cdot (x^5 - 1) + (x^3 - 1)$
$x^5 - 1$	$x^3 - 1$	$x^5 - 1 = x^2(x^3 - 1) + (x^2 - 1)$
$x^3 - 1$	$x^2 - 1$	$x^3 - 1 = x(x^2 - 1) + (x - 1)$
$x^2 - 1$	$x - 1$	$x^2 - 1 = (x - 1)(x + 1) + 0$
$x - 1$	0	–

Therefore, $x-1$ is the gcd.

2. January 6: Factoring polynomials, part I

Quite often in algebraic number theory, we want the minimal polynomial of some algebraic number, and what we have is some higher degree polynomial. Factoring polynomials is useful.

Fact. If $A(x)$ mod p is irreducible in $\mathbb{F}_p[x]$ then it is irreducible in $\mathbb{Z}[x]$ also. Note, however, that this requires that p does not divide the leading coefficient of $A(x)$.

However, the above fact is not as useful as we think. That is, there are polynomials that are irreducible, but always factor in $\mathbb{F}_p[x]$ for all primes p. Consider the polynomial x^4+1, for example. But sometimes, the factors mod p for multiple p's will tell us something about the factors of that polynomial.

Example. Consider $A(x) = x^4+5x^3+9x^2+10x+9$. Then $A(x) \equiv x(x^3+2x^2+1) \bmod 3$ and $A(x) \equiv (x^2+2)^2 \bmod 5$. If $A(x)$ factored, say $A(x) = B(x)C(x)$, then we see that one of $B(x), C(x)$ would be degree one, and one degree 3; and at the same time, both are degree 2. This cannot happen, so $A(x)$ is irreducible.

To factor a polynomial in $\mathbb{F}_p[x]$, there are three main steps each, each an algorithm on its own.

Step 1: Write a square-free factorization

$$A(x) = A_1(x)A_2(x)^2A_3(x)^3\cdots A_k(x)^k$$

where each A_i is co-prime to each other. These are in general not irreducible.

Step 2: Given a square-free factor A_d, write

$$A_d(x) = \prod_{i=1}^{k} \underbrace{A_{d,i}(x)}_{\text{all factors of degree } i} .$$

Step 3: Given a squarefree polynomial $A_{d,k}(x)$ with all irreducible factors of degree k, factor this polynomial completely.

3. January 8

Suppose that

$$A(x) = \prod_i A_i(x)^i.$$

Then the derivative is

$$A'(x) = \sum_{i=1}^{n} iA_i(x)^{i-1}A_i'(x)\prod_{j\neq i} A_j(x)^j.$$

But there are two potential problems: it's possible to have either $i \equiv 0 \pmod{p}$ or $A_i'(x) \equiv 0 \pmod{p}$. If $A_i''(x) = 0$, then

$$A_i(x) = a_0 + a_1x^p + \cdots + a_kx^{pk} \equiv (a_0 + a_1x + \cdots + a_kx^k)^p \pmod{p}.$$

As the $A_i(x)$ are supposed to be square-free, this can't happen. However, the other situation still *can* happen. Let

$$T(x) = \gcd(A(x), A'(x)) = \prod_{i \not\equiv 0 \pmod p} A_i(x)^{i-1} \prod_{i \equiv 0 \pmod p} A_i(x)^i.$$

Initialize $T_1 = T$ and $V_1 = A/T$. If $p \,|\, k$, define $V_{k+1} = V_k$ and $T_{k+1} = T_k/V_{k+1}$. If $p \nmid k$, then define $V_{k+1} = \gcd(V_k, T_k)$ and $T_{k+1} = T_k/V_{k+1}$. The algorithm stops when T_k is a polynomial in x^p.

Example. Let $A(x) = \prod_{i=1}^{5} A_i(x)^i \pmod 3$. Then $T_1 = \gcd(A, A') = A_1^0 A_2^1 A_3^3 A_4^3 A_5^4$ and $V_1 = A_1 A_2 A_4 A_5$. Then $V_2 = A_2 A_4 A_5$ so $T_2 = A_3^3 A_4^2 A_5^3$. Note that $A_1 = V_1/V_2$. Thus $V_3 = A_4 A_5$ and $V_3 = A_3^3 A_4 A_5^2$. We have $A_2 = V_2/V_3$ thus $V_4 = A_4 A_5$ and $T_4 = A_3^3 A_5$. Similarly, we have $V_5 = A_5$ and $T_5 = A_3^3$. The algorithm stops since T_5 is a polynomial in x^3. Thus we have $A_5 = V_5, A_4 = V_4/V_5, A_2 = V_3/V_2$ and $A_1 = V_2/V_1$. Write $\tilde{A}(x)$ such that

$$\tilde{A}(x^3) = T_5(x) = A_3(x)^3.$$

Then factor $\tilde{A}(x)$ as before. In general,

$$T_k(x) = \prod_{\substack{i \geq k+1 \\ p \nmid i}} A_i(x)^{i-k} \prod_{p|i} A_i(x)^i$$

$$V_k(x) = \prod_{\substack{i \geq k \\ p \nmid i}} A_i(x)$$

$$A_k = V_k/V_{k+1} \text{ for } p \nmid k.$$

Let $A(x) = x^9 + x^5 + x \bmod 3$. Then $T_1(x) = \gcd(x^9 + x^5 + x, 5x^4 + 1) = x^4 + 2$ and $V_1(x) = A(x)/T(x) = x^5 + 2x$. Then $T_2 = T_1/V_1 = 1$, which is a (boring) polynomial in x^3. Thus $A_2(x) = x^4 + 2$ and $A_1(x) = V_1(x)/V_2(x) = x$. So $A(x) = x(x^4 + 2)^2$.

Now we need to do more to factorize $x^4 + 2$.

3.1. Distinct degree factorization

Our goal in this section is to take a square-free polynomial and factor into parts with the same degree. As usual, we will let $A_k(x) = A_{k,1}(x) A_{k,2}(x) \times \cdots$.

Fact. If $B(x)$ is an irreducible polynomial of degree d, then $B(x) \mid x^{p^d} - x$. But actually, something stronger is true: $B(x) \,|\, x^{p^e} - x$ for all e, with $d \,|\, e$.

Example. Consider $A_2(x) = x^4 + 2$. Then $A_{2,1}(x) = \gcd(A_2(x), x^3 - x) = x^2 + 2$. In this case, we can stop, as the quotient of $A_2(x)/A_{2,1}(x) = x^2 + 1$ must be irreducible (as in having no linear factors). If we had a larger degree polynomial, we would have removed the linear part, and looked at $\gcd(A(x), x^{p^2} - x)$, and then $x^{p^3} - x$, and so forth. So far $A(x) = x(x^4 + 2)^2 = x((x^2 + 2)(x^2 + 1))^2$, and x and $x^2 + 1$ are irreducible polynomials and $x^2 + 2$ have two linear factors.

3.2. **Final factorization**

Proposition 3. *Let $p > 2$. Let $A(x)$ be a square-free polynomial such that all irreducible factors are degree d. Let $T(x) \in \mathbb{F}_p[x]$ and $T \neq 0$. Then*

$$A(x) = \gcd(A, T)\gcd(A, T^{(p^d-1)/2} - 1)\gcd(A, T^{(p^d-1)/2} + 1).$$

Remark. There is a good chance that $\gcd(A, T) = 1$, but that the other two factors are both non-trivial. We then recurse on the new factors.

Proof. Clearly $A(x) \,|\, x^{p^d} - x$, and $A(x)$ is square-free, and all factors are degree d. Further, $x^{p^d} - x$ factors completely in $\mathbb{F}_{p^d}[x]$. If $\alpha \in \mathbb{F}_{p^d}$, then $T(\alpha) \in \mathbb{F}_{p^d}$. So α is a root of $T(x)^{p^d} - T(x)$. As this is true for all α, we have $x^{p^d} - x \,|\, T(x)^{p^d} - T(x)$. Notice that

$$T(x)^{p^d} - T(x) = T(x)\left(T(x)^{(p^d-1)/2} - 1\right)\left(T(x)^{(p^d-1)/2} + 1\right).$$

Further, if $\alpha \in \mathbb{F}_{p^d}$, then only one of these factors is 0. Hence they are all co-prime, which proves the result as required. □

Let $A(x)$ and $B(x)$ be two polynomials of degree d, with roots $\alpha, \beta \in \mathbb{F}_{p^d}$. Either $\alpha^{(p^d-1)/2} + 1 = 0$, or $\alpha^{(p^d-1)/2} - 1 = 0$. The similar claim holds for β also. There is $\approx 50\%$ chance of either. The random map $T : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d}$ mixes these up. So there is a 50% chance that $T(x)$ will separate α and β and hence $A(x)$ and $B(x)$. Continue until it is completely factored.

Example. $x^2 + 2$ is a product of two linear factors.

$T(x)$	$\gcd(A, T)$	$\gcd(A, T-1)$	$\gcd(A, T+1)$
x	1	$x+2$	$x+1$
$x+1$	$x+1$	1	$x+2$
$x+2$	$x+2$	$x+1$	1

4. January 13

4.1. **Resultants and discriminants**

Definition 4. Let $A(x) = a_n x^n + \cdots + a_0$ and $B(x) = b_m x^m + \cdots + b_0$. We define the *resultant of $A(x)$ and $B(x)$* as

$$\mathrm{Res}_x(A(x), B(x)) := a_n^m B(\alpha_1)B(\alpha_2)\cdots B(\alpha_n)$$

where $A(x) = a_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$. Equivalently,

$$\begin{aligned}\mathrm{Res}_x(A(x), B(x)) &= (-1)^{mn} b_m^n A(\beta_1)A(\beta_2)\cdots A(\beta_m)\\ &= a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j),\end{aligned}$$

where $B(x) = b_m(x - \beta_1)\cdots(x - \beta_m)$.

One can write the resultant as the determinant of a matrix:

$$\det \begin{bmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 \\ & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_0 & 0 & \cdots & 0 \\ & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & \cdots & 0 & b_m & b_{m-1} & \cdots & b_0 \end{bmatrix}$$

Remark. First, it is not obvious that these are all equal (in fact they are). A proof can be easily found in most algebraic number theory texts however. Also, note that the order *does* matter, as it may change the sign. Also, we have $\operatorname{Res}_X(A, B) = 0$ if and only if A and B have a common root. Also, if $A, B \in \mathbb{Z}[x]$ then $\operatorname{Res}_X(A, B) \in \mathbb{Z}$.

Definition 5. We define the *discriminant of* $A(x)$ as

$$\operatorname{disc}(A(x)) = (-1)^{m(m-1)/2} \operatorname{Res}_X(A(x), A'(x)).$$

Note that $\operatorname{disc}(A) = 0$ if and only if $A(x)$ has a repeated root.

Example. Since $x^5 - 1$ and $x^3 - 1$ have a common root, it follows $\operatorname{Res}_x(x^5 - 1, x^3 - 1) = 0$.

Example. $\operatorname{disc}(x^3 - 1) = \operatorname{Res}_x(x^3 - 1, 3x^2) = 3 \cdot 1^2 \cdot 3\omega^2 \cdot 3\omega^4 = 27$.

4.2. **Factoring polynomials, part II**

Factoring a polynomial in $\mathbb{F}_p[x]$ can give (if we are lucky) good information about how it factors in $\mathbb{Z}[x]$. By using Hensel lifting, or the Chinese remainder theorem, this can often result in a factorization in $\mathbb{Z}[x]$. Instead we will introduce a technique called LLL (Lenstra-Lenstra-Lovasz) which requires a good approximation of a root of the polynomial. This algorithm normally recovers a polynomial of lower degree with the same root. After that, we can used gcd's to get a factor.

Definition 6. We say that L is a *lattice* if it is a discrete subset of $\mathbb{R}^d$ of the form

$$L = \left\{ \sum a_i b_i : a_i \in \mathbb{Z}, b_i \in B, |B| < \infty \right\}.$$

Example. $L = \{(a, 2b, 3c) : a, b, c \in \mathbb{Z}\}$. This is a lattice with basis $\{(1, 0, 0), (0, 2, 0), (0, 0, 3)\}$. But the following horrendous basis also works: $\{(1, 2002, 30000), (0, 2, -600000), (0, 0, 3)\}$. The first basis is much "nicer" than the second.

The goal of LLL is to find a "nice" basis, given some input basis.

Example. Let $A(x) = x^3 - x^2 - 2x + 2$ with root $\alpha \approx 1.4142828$. Consider a lattice with a basis

$$B = \{(1, 0, 0, 1000\alpha^2), (0, 1, 0, 1000\alpha), (0, 0, 1, 1000)\}.$$

This has a "nicer" basis

$$B' = \{(1, 0, -2, 1000(\alpha^2 - 2)), (0, 1, 0, 1000\alpha), (0, 0, 1, 1000)\}.$$

Note that $\alpha^2 - 2$ is quite close to 0. Note that the first basis element of B' is much smaller, as $\alpha^2 - 2 \approx 0$. We guess that α is a root of $x^2 - 2$, and note that $\gcd(A, x^2 - 2) = x^2 - 2$. So we have a factor.

Definition 7. Let V be a vector space. Consider the two-variable map $\langle \_, \_ \rangle : V \times V \to \mathbb{C}$ which satisfies

1. $\langle v_1 + v_2, w \rangle = \langle v_1, w \rangle + \langle v_2, w \rangle$
2. $\langle v, w_1 + w_2 \rangle = \langle v, w_1 \rangle + \langle v, w_2 \rangle$
3. $\langle \lambda v, w \rangle = \bar{\lambda} \langle v, w \rangle$
4. $\langle v, w \rangle = \overline{\langle w, v \rangle}$.
5. $\langle v, v \rangle = 0 \Leftrightarrow v = 0$, and $\langle v, v \rangle \geq 0$ for any $v \in V$.

Then the map $\langle \_, \_ \rangle$ is said to be an *inner product.*

Definition 8. We define a *norm* $\|b\|^2 = \langle b, b \rangle$.

Definition 9. We say $B = \{b_1, \ldots, b_n\}$ is a *reduced basis* if

1. The vector b_1 has minimal non-zero norm in the lattice. b_1 is not unique.
2. The vector b_2 has minimal norm in the lattice of those vectors linearly independent from b_1.
3. The vector b_3 has minimal norm in the lattice of those vectors linearly independent from b_1 and b_2.
4. (keep going like this...)

If we can find such reduced lattice, we are done. But the problem is that finding the reduced lattice is NP-hard. Instead, we will find a lattice that's not reduced but reduced "enough" (or "nice" enough).

Definition 10. Such sufficiently reduced lattice will be called *LLL-reduced.*

Recall the Gram-Schmidt orthogonalization process. Let $b_1, \ldots, b_n \in V$ linearly independent. Define

$$b_i^* := b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

where

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}.$$

Then $b_1^*, \ldots, b_n^*$ forms an orthogonal basis of the same subspace. That is,

$$\operatorname{span}\{b_1, \ldots, b_n\} = \operatorname{span}\{b_1^*, \ldots, b_n^*\}$$

and $\langle b_i^*, b_j^* \rangle = 0$ if and only if $i \neq j$.

Remark. We now make a few observations:

1. We can re-order the vectors in an orthogonal basis to get a reduced basis, albeit of a *different* lattice.
2. Note that

$$\begin{aligned} \frac{\langle b_i + k b_j, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} &= \frac{\langle b_i + k(b_j^* + \sum \mu_{l,j} b_l^*), b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \\ &= \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} + k \frac{\langle b_j^*, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} = \mu_{ij} + k. \end{aligned}$$

(3) If $b_1, \dots, b_n$ is a basis of L, then so are $b_1, b_2, \dots, b_j, \dots, b_i + kb_j, \dots, b_n$ and $b_1, b_2, \dots, b_{i+1}, b_i, \dots, b_n$.

Our vague goal is to use the (3) to find a new basis where $|\mu_{ij}| \leq \frac{1}{2}$ (even better if we can hit 0). If we have small vectors early then we can better adjust μ_{ij} later. So we wish to reorder when necessary. So our goal is to require

$$\|b_j^*\|^2 \geq \left(\frac{3}{4} - \mu_{j,j-1}^2\right) \|b_{j-1}^*\|^2.$$

Any time this condition is violated, swap. That is, the vectors should be, roughly speaking, in increasing order. So the summary of the algorithm goes as follows:

(1) Assume that $b_1, \dots, b_k$ is LLL-reduced.
(2) We look at b_{k+1} and add or subtract integer copies of $b_1, \dots, b_k$ to ensure that $|\mu_{k+1,j}| \leq 2^{-1}$ for $j = 1, 2, \dots, k$. That is, if $\mu_{k+1,1} = 3.14159$, then we can set $b_{k+1}^{(\text{new})} = b_{k+1}^{(\text{old})} - 3b_1$. This gives us $\mu_{k+1,1}^{(\text{new})} = 0.14159$. The basis $b_1, \dots, b_k, b_{k+1}^{(\text{new})}, \dots$ is still a basis for the lattice.
(3) Next, check if

$$\|b_{k+1}\|^2 \geq \left(\frac{3}{4} - \mu_{k+1,k}^2\right) \|b_k\|^2.$$

If true, then $b_1, \dots, b_{k+1}$ is LLL-reduced, and we repeat on $b_1, \dots, b_{k+1}$. If false, swap b_k and b_{k+1}. Then $b_1, b_2, \dots, b_{k=1}$ is LLL-reduced. Repeat. Note that reordering terms in the basis still give a basis for the same lattice.

But the algorithm is not of much use if it does not terminate. Thus, we need to show that this second case (the "false" case) cannot happen infinitely many times.

Theorem 1. *The Lenstra-Lenstra-Lovasz algorithm terminates.*

Proof. Define $D := \|b_1^*\|^n \|b_2^*\|^{n-1} \cdots \|b_n^*\|^1$. We see that $D > 0$ for all basis of a lattice. Furthermore, it is bounded below by $\|x\|^n \cdot \|x\|^{n-1} \cdots \|x\|^1 = \|x\|^{n(n+1)/2}$, where x is the smallest element (non-zero) in L. The process of adjusting b_{k+1} by

$$b_{k+1}^{(\text{new})} = b_{k+1}^{(\text{old})} + ab_j, a \in \mathbb{Z}$$

does *not* change $b_1^*, b_2^*, \dots, b_n^*$. Hence this does not change D.

The second possible action, of swapping b_k and b_{k+1} does change D. This happens if

$$\|b_{k+1}^*\|^2 < \left(\frac{3}{4} - \mu_{k+1,k}^2\right) \|b_k^*\| < \frac{3}{4}\|b_k^*\|^2.$$

If we do this, then D will increase. So

$$D^{(\text{new})} \leq \frac{3}{4} D^{(\text{old})}.$$

Thus D is bounded below, and if we swap D is decreased. So we cannot do this forever. Therefore the algorithm terminates, as desired. □

Remark. Additional remarks on the LLL algorithm:

(1) The actual running time is $O(n^3 d \log^3 B)$, where n is the number of vectors, d the dimension, and B the largest b_i in terms of norm.
(2) LLL tends to return the actual smallest element, even though it is not guaranteed.

(3) LLL can only deal with norms from inner products.
(4) LLL has a large and varied number of applications. We just have to figure out how to rewrite the problem as a lattice problem.

5. January 15: Algebraic numbers and number fields

Definition 11. Let $\alpha \in \mathbb{C}$ such that α is a root of some $A(x) \in \mathbb{Z}[x]$. Then we say that α is an *algebraic number*. If $A(x)$ is a monic polynomial, then α is an *algebraic integer*.

Example. Let $\alpha = 1+\sqrt{2}$. Since α is a solution to $(x-1-\sqrt{2})(x-1+\sqrt{2}) = x^2-2x-1$, α is an algebraic integer.

Example. All integers are algebraic integers, since $x-n$ is a polynomial with n as a root.

Example. Let $\alpha = \frac{3}{4}$. Then α is a root of $4x-3$. Here α is an algebraic number but is *not* an algebraic integer.

Example. $\pi, e, \log(2)$ are not algebraic numbers. It is unknown if $\pi + e$ is algebraic.

Proposition 12. *Let α be an algebraic number. Then there exists a* unique *polynomial $P(x)$ of minimal degree such that*

(1) $P(\alpha) = 0$
(2) $\deg P(x)$ *is minimal.*
(3) GCD of the coefficients of $P(x)$ is 1.
(4) the lead coefficient is positive.
(5) $P(x) \in \mathbb{Z}[x]$.

Proof. Assume $A(x)$ and $B(x)$ are two such polynomials of degree n; and that the lead coefficients of A and B are a and b respectively. Consider $bA(x) - aB(x)$. We see that α is a root, and this is an integer polynomial of degree less than n. We can adjust to ensure properties (3) and (4). Either $A(x) = B(x)$ or $A(x)$ and $B(x)$ were not of minimal degree. Hence such polynomial is unique. □

Definition 13. We call such polynomial a *minimal polynomial.* We say *the degree of an algebraic number* the degree of its minimal polynomial.

Example. $1+\sqrt{2}$ has minimal polynomial x^2-2x-1 and is of degree 2. Integers and rationals have degree 1.

Definition 14. Let α be an algebraic number with minimal polynomial $A(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = a_n(x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n)$. The other roots are called the *(Galois) conjugates of α.*

Example. The Galois conjugate of $1+\sqrt{2}$ is $1-\sqrt{2}$. Also, the rationals and integers have no non-trivial conjugates.

Definition 15. A *number field K* is a field such that $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ that is also a degree n vector space over $\mathbb{Q}$ for some finite number n. That is,

$$K = \{a_1 v_1 + \cdots + a_n v_n : a_i \in \mathbb{Q}\}.$$

We say this number field is degree n, i.e., $[K : \mathbb{Q}] = n$.

Example. $\mathbb{Q}(\sqrt{2})$ is of degree 2 since $\{1, \sqrt{2}\}$ forms a basis.

It is easy to check that $\mathbb{Q}(\sqrt{2})$ is closed under addition and multiplication and division. Thus $\mathbb{Q}(\sqrt{2})$ is indeed a field – a number field of degree 2.

Recall that for a number field of the form $\mathbb{Q}(\alpha)$ we see that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg P(x)$ where $P(x)$ is the minimal polynomial of α. Consider $K = \mathbb{Q}(\sqrt{2})$, and consider the embedding $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. Clearly, we have $\sigma : K \to K$. Further, $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) = (a_1 - b_1\sqrt{2})(a_2 - b_2\sqrt{2}) = a_1a_2 + 2b_1b_2 - (a_1b_2 + a_2b_1)\sqrt{2}$. So $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$. Thus σ is in fact an automorphism.

6. January 20

Let $K = \mathbb{Q}(\alpha)$, with $\deg(\alpha) = n$. Then $[K : \mathbb{Q}] = n$ and

$$K = \{a_0 + a_1\alpha + \cdots + a_{n=1}\alpha^{n-1} : a_i \in \mathbb{Q}\}.$$

Notice that we can talk about the degree of a number field over a number field. That is, if $\mathbb{Q} \subseteq L \subseteq K$, we mean by $[K : L]$ = the dimension of the vector space K over L. Recall also that

$$[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}].$$

Example. Let $L := \mathbb{Q}(\sqrt{2})$ and $K := L(\sqrt{8}) = \{a_0 + a_1\sqrt{9} + \cdots : a_i \in L\}$. We see the minimal polynomial in $\mathbb{Q}[x]$ of $\sqrt{2}$ is $x^2 - 2$. Hence $[L : \mathbb{Q}] = 2$. We see the minimal polynomial of $\sqrt{8}$ in $L[x]$ is $x - 2\sqrt{2}$, so $[K : L] = 1$, or $K = L$. Thus $[K : \mathbb{Q}] = [L : \mathbb{Q}] = 2$.

So, an interesting question in the field of computational algebraic number theory is, how do we see if $K = L$ *or* $K \cong L$? Consider the Galois map $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. This gives us an isomorphism from K to K, and hence L to L. This map takes $\sqrt{2}$ to its conjugate $-\sqrt{2}$. This map also takes $\sqrt{8}$ to its conjugate $-\sqrt{8}$. This is true in general.

Example. Let $L = \mathbb{Q}(\sqrt{2})$ and $K = L(i)$. Clearly, $\mathbb{Q} \subseteq L \subseteq K$. The minimal polynomial of $\sqrt{2}$ is $x^2 - 2$ so $[L : \mathbb{Q}] = 2$. The minimal polynomial of i over $\mathbb{Q}[x]$ is $x^2 + 1$. This is still irreducible over $L[x]$. So $[K : L] = 2$. Notation goes $K = L(i) = \mathbb{Q}(\sqrt{2})(i) = \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(i, \sqrt{2})$ (i.e., the order does *not* matter). So $[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = 2 \cdot 2 = 4$.

Claim. $K = \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$.

Proof. Clearly, $\sqrt{2} + i \in \mathbb{Q}(\sqrt{2}, i)$. Thus $\mathbb{Q}(\sqrt{2} + i) \subseteq K$. Note that

$$\frac{-(\sqrt{2} + i)^3 + 5(\sqrt{2} + i)}{6} = \sqrt{2} \in \mathbb{Q}(\sqrt{2} + i)$$
$$\frac{-(\sqrt{2} + i)^3 + (\sqrt{2} + i)}{6} = i \in \mathbb{Q}(\sqrt{2} + i)$$

So $\sqrt{2}, i \in \mathbb{Q}(\sqrt{2} + i)$ and hence $\mathbb{Q}(\sqrt{2}, i) \subseteq \mathbb{Q}(\sqrt{2} + i) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Hence they are equal. □

Definition 16. Let K be a number field. We say that $\sigma : K \hookrightarrow \mathbb{C}$ is a *field embedding* if $\sigma(K)$ is a number field, and $\sigma(K)$ is isomorphic as a field to K by σ.

Example. The map $\mathrm{id}(x) = x$ always is a field embedding.

Example. Let $K = \mathbb{Q}(\sqrt[4]{2})$. This has minimal polynomial $x^4 - 2$. So $[K : \mathbb{Q}] = 4$. Here, $\sqrt[4]{2}$ has 4 conjugates including itself: $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i$. Call these $\alpha_1, \alpha_2, \alpha_3$, and α_4 respectively. Then the map

$$\sigma_i(a + b\alpha_1 + c\alpha_1^2 + d\alpha_1^3) = a + b\alpha_i + c\alpha_i^2 + d\alpha_i^3.$$

Notice further that $\sigma_1(K) = \sigma_2(K) = K$ while $\sigma_3(K) = \sigma_4(K) \neq K$.

Theorem 2. *Let K be a number field, and $[K : \mathbb{Q}] = n$. Then the following are true:*

1. *There exists an algebraic number Θ of degree n such that $K = \mathbb{Q}(\Theta)$.*
2. *There are exactly n field embeddings of K into $\mathbb{C}$.*
3. *For any field embedding K_i and any $\Theta \in K_i$, we have $\deg(\Theta) \,|\, [K_i : \mathbb{Q}]$, so $\deg(\Theta) \,|\, n$.*

Example. $1, \sqrt{2}, \sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$. These have degree $1, 2$, and 4 respectively, all of which divide 4.

Definition 17. The *signature of a number field* is a pair (r_1, r_2) where the number field has r_1 real embeddings and $2r_2$ complex embeddings.

Example. Let $K = \mathbb{Q}(\sqrt[4]{2})$. Then K has 2 real embeddings and 2 complex embedding, so has signature $(2, 1)$.

Example. LeT $K = \mathbb{Q}(\sqrt{2})$. This has 2 real embedding, no complex, so signature $(2, 0)$. This is knows as a *totally real field.*

Example. Let $K = \mathbb{Q}(i)$. This has signature $(0, 1)$. This is a *totally complex field.*

Question 1. Given some field $K = \mathbb{Q}(\Theta)$, where Θ has minimal polynomial $A(x)$, how do we compute the signature?

We describe the first method, which is a true brute force method. That is, we brute-force compute all the roots of $A(x)$ using something like Newton's method. However,

1. This is computationally expensive.
2. It is harder than one might think to do this in a numerically stable way.
3. This gives way more info than we need.

This leads us to the second method. The method of Sturm sequences will determine how many real roots are in an interval $[a, b]$, although with no information as to what they are. We can take $a = -\infty$, and or $b = +\infty$.

Definition 18. We say a sequence of polynomials $f = f_0, f_1, f_2, \ldots, f_s$ is a *Sturm sequence* on $[a, b]$ if

1. $f(a)f(b) \neq 0$
2. $f_S(x) \neq 0$ for all $x \in [a, b]$
3. If c is a root of f_j with $c \in [a, b]$, then $f_{j-1}(c)f_{j+1}(c) < 0$ for $1 \leq j < S$.
4. If c is a root of $f_0(x)$ in $[a, b]$ then $f_0(x)f_1(x)$ has the same sign of $x - c$, locally to c.
5. f_0 is squarefree.

Definition 19. We define the *variation* of a sequence $f_0, f_1, \ldots, f_S$ at c as

$$V = \#\{(i, j) : f_i(c)f_j(c) < 0, f_k(c) = 0 \ \forall i < k < j\}.$$

This basically counts sign changes.

If $c = \pm\infty$, then we take the limit as $c \to \pm\infty$. After some point, this variation is constant.

Theorem 3. *Let f_0 be square-free, and let $f_0, f_1, \ldots, f_S$ be a sequence of Sturm on $[a, b]$. Then the number of real roots on $[a, b]$ of $f_0(x)$ is $V(b) - V(a)$.*

Theorem 4. *Let $f_0 = f$ be square-free. Define $f_1(x) = f_0'(x)$ and $f_{i+1}(x) = -f_{i-1}(x) \bmod f_i(x)$. Define $g_i(x) = f_i(x)/f_S(x)$. Then $g_i(x)$ is a sequence of Sturm.*

Example. Let $f = f_0(x) = x^5 + x^3 - 5x + 1$. Then $f_1(x) = 5x^4 + 3x^2 - 5$, $f_2(x) = \frac{1}{5}(-2x^3 + 20x + 5)$, $f_3(x) = \frac{1}{2}(-106x^2 + 25x + 10)$, $f_4(x) \approx -3.94x + 1.008$ and $f_5(x) \approx -4.75$. The sequence of signs as $c \to +\infty$ is $V(\infty) = 1$, since $-, -, +, +, +, +$. The sequence as $c \to -\infty$ is 4, since $+, -, -, +, -, +$. Thus $V(-\infty) = 4$, so there are $V(-\infty) - V(\infty) = 3$ real roots.

7. January 22

Theorem 5. *If $f_0, \ldots, f_s$ is a sequence of Sturm, then the number of real roots in $[a, b]$ is $V(b) - V(a)$.*

Proof. Consider $V(f_0, f_1, \ldots, f_s, x)$ as a function of x. This is a function from $\mathbb{R}$ to $\{0, 1, 2, \ldots, s\}$. Most of the time this function is constant. The only time this might change is if there exists a c such that $f_j(c) = 0$. Then it might change from $c - \varepsilon$ to $c + \varepsilon$.

We will show that:

(1) If $c \in [a, b]$ with $f_0(c) = 0$ then $V(c - \varepsilon) - V(c + \varepsilon) = 1$.
(2) If $c \in [a, b]$ with $f_j(c) = 0$ with $1 \leq j < s$ then $V(c - \varepsilon) - V(c + \varepsilon) = 0$.

This gives us that

$$V(b) - V(a) = \#c \in [a, b] \text{ such that } f_0(c) = 0.$$

Part 1. Assume that $c \in [a, b]$ with $f_0(c) = 0$. We know that locally to c that $f_0(x)f_1(x)$ has the same signs as $x - c$, i.e., $f_0(c - \varepsilon)f_1(c - \varepsilon) < 0 < f_0(c + \varepsilon)f_1(c + \varepsilon)$. We see that c is not a root of f_1, so if $f_1(c - \varepsilon) > 0$, then $f_0(c - \varepsilon) < 0, f_0(c + \varepsilon) > 0, f_1(c + \varepsilon) > 0$. The sign variation would start

$$\begin{array}{lcc} c - \varepsilon\text{:} & - & + \\ c + \varepsilon\text{:} & + & + \end{array}$$

If instead $f_1(c - \varepsilon) < 0$, then this gives

$$\begin{array}{lcc} c - \varepsilon\text{:} & + & - \\ c + \varepsilon\text{:} & - & - \end{array}$$

Regardless of which case we are in, we see that $V(c - \varepsilon) - V(c + \varepsilon) = 1$, as required.

Part 2. Let $c \in [a, b]$ with $f_1(c) = 0$ for some $1 \leq j < s$. We know then that $f_{j-1}(c)f_{j+1}(c) < 0$. This will be true for $[c - \varepsilon, c + \varepsilon]$. Therefore,

	$j - 1$		$j + 1$
$c - \varepsilon$	$-$	$-$	$+$
$c + \varepsilon$	$-$	$+$	$+$
$c - \varepsilon$	$-$	$+$	$+$
$c + \varepsilon$	$-$	$-$	$+$
$c - \varepsilon$	$+$	$-$	$-$
$c + \varepsilon$	$+$	$+$	$-$
$c - \varepsilon$	$+$	$+$	$-$
$c + \varepsilon$	$+$	$-$	$-$

Regardless of which case we are in, we have exactly one sign change, on both sides of c. This gives $V(c-\varepsilon) - V(c+\varepsilon) = 0$. □

Example. Consider the previous example

$$\begin{aligned}
-f_0(x) &= (x^5 + x^3 - 5x + 1)\cdot(-1)\\
-f_1(x) &= (5x^4 + 3x^2 - 5)\cdot(-1)\\
-f_2(x) &= \left(\frac{1}{5}(-2x^3 + 20x + 5)\right)\cdot(-1)\\
-f_3(x) &= \left(\frac{1}{2}(-106x^2 + 25x + 10)\right)\cdot(-1)\\
-f_4(x) &\approx (-3.94x + 1.008)\cdot(-1)\\
-f_5(x) &\approx (-4.75)\cdot(-1)
\end{aligned}$$

Applying the theorem gives us

Proof of Theorem 4. We may assume $f(a)f(b) \neq 0$ – otherwise, there will be a root. Also, we assume $f_s(x) \neq 0$ for all $x \in [a,b]$, as $f_s(x)$ is essentially the gcd of f with $f'(x)$. Let $c \in [a,b]$ be a root of $f_j(x)$. We know that $f_{j+1}(x) = -f_{j-1}(x) \bmod f_j(x)$. Then $f_{j+1}(x) = -f_{j-1}(x) + f_j(x)\cdot g(x)$, so $f_{j+1}(c) = -f_{j-1}(c) + 0$. This gives us that $f_{j+1}(c)f_{j-1}(c) < 0$. Let $c \in [a,b]$ be a root of $f_0(x)$. Two cases are possibilities. If $f_0(x)$ is increasing at c, then $f_1(x) = f_0'(x) > 0$. This gives $f_0(x)f_1(x)$ has the desired property. The case where $f_0(x)$ is decreasing is similar. □

7.1. **Representing algebraic numbers**

To do algebraic number theory on a computer, we need to figure out how to represent them. We also need to be able to do standard manipulations (addition and multiplication) of these objects. For instance, $\sqrt{5+2\sqrt{6}} = \sqrt{2}+\sqrt{3}$ is not the best representation as the representation is not unique, and we can't pull this trick off for general degree polynomials (of degree at least 5). Also, addition and multiplication are messy if we want some "simple" representation. It also ignores "branch" cuts. So, some alternate methods:
First method. The minimal polynomial is unique. All of its roots are distinct. With enough numerical accuracy, we can uniquely identify which algebraic numbers we are talking about. But the problem is that addition and multiplication are not obvious. Let α_1 have minimal polynomial $A(x) = \prod(x-\alpha_i)$. Let β_1 have minimal polynomial $B(x) = \prod(x-\beta_j)$. We want a polynomial with $\alpha_1\beta_1$, or $\alpha_1+\beta_1$, or α_1/β_1 as a root. For addition, consider the resultant:

$$\begin{aligned}
\mathrm{Res}_y(A(x-y), B(y)) &= \mathrm{Res}_y\Big(\prod(x-y-\alpha_i), \prod(y-\beta_j)\Big)\\
&= \mathrm{Res}_y\Big(\pm\prod(y-x-+\alpha_i), \prod(y-\beta_j)\Big)\\
&= \prod_{i,j}(x-\alpha_i-\beta_j).
\end{aligned}$$

This has $\alpha_1+\beta_1$ as a root. Nonetheless, this has an issue: the problem is that this polynomial may not be *minimal.* We also have to compare $\alpha_1+\beta_1$ to $\alpha_i+\beta_j$ to ensure that we have enough accuracy.

As for multiplication, consider $\mathrm{Res}_y(A(x/y)y^{\deg(A)}, B(y))$; for division, $\mathrm{Res}_y(A(xy), B(y))$.

Second method. Quite often, we know something more about the algebraic numbers. For example, all $\alpha_i \in K = \mathbb{Q}(\theta)$, where θ has a minimal polynomial $A(x)$. In this case, we can represent all algebraic numbers as

$$\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$$

with $\deg(\theta) = n$ and $a_i \in \mathbb{Q}$. In fact, any basis for K over $\mathbb{Q}$ works. Addition is easy. For multiplication, we look at $(a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1})(b_0+b_1\theta+\cdots+b_{n-1}\theta^{n-1}) \bmod A(\theta)$. Now let's consider division. Let $\beta(\theta) = b_0+b_1\theta+\cdots+b_{n-1}\theta^{n-1}$. We see that $\gcd(\beta(\theta), -A(\theta)) = 1$. So there exists $a(\theta)$ and $b(\theta)$ such that $a(\theta)b(\theta) + b(\theta)A(\theta) = 1$.

8. January 27

We now have a way to represent algebraic numbers and number fields. There are some computational questions we might like to answer.

(1) Given $\alpha, \beta, K = \mathbb{Q}(\alpha), L = \mathbb{Q}(\beta)$, can we determine if:
   (a) $K = L$
   (b) $K \cong L$
   (c) is K an extension of L, or the other way around?
   (d) is K isomorphic to a subfield of L (i.e., $K \cong K' \subseteq L$)
   (e) Is $\alpha \in \mathbb{Q}(\beta)$?
   (f) If $\alpha \in L' \cong \mathbb{Q}(\beta)$.

(2) Let $K = \mathbb{Q}(\theta_1, \theta_2, \ldots, \theta_n)$. We know there exists an α such that $K = \mathbb{Q}(\alpha)$. How do we find such α?

Many of these questions are related. Before exploring how to answer them, we need a bit of more terminology.

8.1. Trace, norm, and characteristic polynomial

Definition 20. Let $\alpha \in K$, and let $\sigma_1, \ldots, \sigma_n$ be the n field embeddings of K. (Here, $\deg(K) = n$.) Then the *characteristic polynomial of α over K* as

$$C_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)).$$

Remark. $C_\alpha(x) \in \mathbb{Q}[x]$, and this can be strengthened to $C_\alpha(x) \in \mathbb{Z}[x]$ whenever α is an algebraic integer. Also, note that if the field is not specified, then we shall often assume that $K = \mathbb{Q}(\alpha)$.

Example. Let $K = \mathbb{Q}(\sqrt[10]{2})$. Then $C_1(x) = \prod(x - \sigma_i(1)) = \prod(x-1) = (x-1)^{10}$.

Proposition 21. *If* $\deg(\alpha) = \deg(K)$ *then the characteristic polynomial of α over K is* irreducible *in* $\mathbb{Q}[x]$.

Definition 22. We define the *trace* of α over K as

$$\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

As before, if α is an algebraic number then $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$. If α is an algebraic integer then $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. However, note that this statement is *not an "if and only if" statement.*

Example. Let α be the root of $x^{10}+3x^9-\frac{1}{2}$, assuming that this polynomial is irreducible. Let

$$C_\alpha(x) := \prod(x-\sigma_i(\alpha)) = x^{10}-(\sigma_1(\alpha)+\cdots+\sigma_{10}(\alpha))x^9+\cdots-\frac{1}{2}.$$

So here, we have

$$\mathrm{tr}_{K/\mathbb{Q}}(\alpha)=\sigma_1(\alpha)+\cdots+\sigma_{10}(\alpha)=-3.$$

So in general, $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)=a_{n-1}$ coefficient of characteristic polynomial.

Definition 23. Let $\alpha\in K$ and $\sigma_1,\dots,\sigma_n$ the n field embeddings of K. We define the norm of α over K as

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha)=\prod_{i=1}^{n}\sigma_i(\alpha).$$

As before, if $\mathrm{N}(\alpha)\in\mathbb{Q}$ and if α is an algebraic integer then $\mathrm{N}_{K/\mathbb{Q}}(\alpha)\in\mathbb{Z}$. And given $C_\alpha(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$, then we see that $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)=-a_{n-1}$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha)=(-1)^na_0$.

Given these quantities, we now wish to figure out how to compute them. This will depend on how we represented the algebraic number.

(1) Representation I

We represented α by a floating point approximation, and its minimal polynomial

$$A(x)=a_nx^n+\cdots+a_0.$$

If $K=\mathbb{Q}(\alpha)$, then the characteristic polynomial is $a_n^{-1}A(x)$. Similarly, trace is $-a_{n-1}/a_n$ and $\pm a_0/a_n$. What if $\alpha\in K,\deg(\alpha)=n$ and $\deg(K)=mn$? Then the characteristic polynomial is $(a_n^{-1}A(x))^m$. Trace is $-ma_{n-1}/a_n$, norm $((-1)^na_0/a_n)^m$.

(2) Representation II

Let $K=\mathbb{Q}(\theta)$, where θ has minimal polynomial $T(x)$, of degree n. We can assume without loss of generality that θ is an algebraic integer. For $\alpha\in K$, we have $\alpha=a_0+a_1\theta+a_2\theta^2+\cdots+a_{n-1}\theta^{n-1}$. We wish to compute its trace, norm, and characteristic polynomial. Suppose that θ has minimal polynomial

$$T(x)=x^n+t_{n-1}x^{n-1}+\cdots+t_0.$$

Then notice that

$$\begin{aligned}\mathrm{tr}_K(\alpha)&=\mathrm{tr}(a_0)+\mathrm{tr}(a_1\theta)+\cdots+\mathrm{tr}(a_{n-1}\theta^{n-1})\\&=a_0\,\mathrm{tr}(1)+a_1\,\mathrm{tr}(\theta)+\cdots+a_{n-1}\,\mathrm{tr}(\theta^{n-1}),\end{aligned}$$

where $\mathrm{tr}(\theta)=-t_{n-1}$.

Proposition 24. $\mathrm{tr}(\theta^k)=-k\cdot t_{n-k}-\sum_{i=1}^{k-1}t_{n-i}\,\mathrm{tr}(\theta^{k-i})$.

Proof. This will be one of the problems in Assignment #2. □

Proposition 25. *Let $K=\mathbb{Q}(\theta)$, where $T(x)$ is a monic minimal polynomial. Let*

$$\alpha := \frac{1}{d}\sum_{i=0}^{n-1}a_i\theta^i.$$

Then

$$C_\alpha(x)=d^{-n}\,\mathrm{Res}_y(T(y),dx-A(y))$$

and

$$\mathrm{N}_K(\alpha) = (-1)^n d^{-n} \operatorname{Res}_y(T(y), -A(y)).$$

Proof. Note that

$$\begin{aligned}\operatorname{Res}_y(\prod(y-\sigma_i(\theta)), dx - A(y)) &= \prod(dx - A(\sigma_i(\theta)))\\ &= \prod(dx-\sigma_i(\alpha))\\ &= d^n \prod(x-\sigma_i(\alpha)).\end{aligned}$$ □

8.2. **Discriminants and integral basis**

Definition 26. Let K be a number field, and $\sigma_1,\dots,\sigma_n$ its n field embeddings. Let $\alpha_1,\dots,\alpha_n \in K$. We define the *discriminant* of $\alpha_1,\dots,\alpha_n$ as

$$\operatorname{disc}(\alpha_1,\dots,\alpha_n) := \det\begin{pmatrix}\sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1)\\ \vdots & & \vdots\\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n)\end{pmatrix}^2.$$

Proposition 27. $\operatorname{disc}(\alpha_1,\dots,\alpha_n) = \det\begin{pmatrix}\operatorname{tr}(\alpha_1\alpha_1) & \cdots & \operatorname{tr}(\alpha_1\alpha_n)\\ \vdots & & \vdots\\ \operatorname{tr}(\alpha_n\alpha_1) & \cdots & \operatorname{tr}(\alpha_n\alpha_n)\end{pmatrix}.$

Corollary 1. $\operatorname{disc}(\alpha_1,\dots,\alpha_n) \in \mathbb{Q}$. *If $\alpha_1,\dots,\alpha_n$ are algebraic integers, then so are $\alpha_i\alpha_j$. Therefore* $\operatorname{disc}(\alpha_1,\dots,\alpha_n) \in \mathbb{Z}$.

Let $M := (\sigma_i(\alpha_j))_{i,j}$. We note that $\det(M) = \det(M^t)$. Hence $\det(M)^2 = \det(M^2) = \det(M)\det(M) = \det(M)\det(M^T) = \det(MM^T)$. The i,j-th entry of MM^T is

$$\sigma_1(\alpha_i)\sigma_1(\alpha_j) + \cdots + \sigma_n(\alpha_i)\sigma_n(\alpha_j) = \operatorname{tr}(\alpha_i\alpha_j)$$

as required.

Theorem 6. *Let $\alpha_1,\dots,\alpha_n \in K$. Then* $\operatorname{disc}(\alpha_1,\dots,\alpha_n) = 0$ *if and only if there exists $\lambda_i \in \mathbb{Q}$ not all 0 such that $\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n = 0$. That is, the discriminant is not zero if and only if $\alpha_1,\dots,\alpha_n$ are $\mathbb{Q}$-linearly independent.*

Proof. Assume there exist $\lambda_1,\dots,\lambda_n$ such that $\lambda_1\alpha_1+\cdots+\lambda_n\alpha_n = 0$. Then $\sigma_1(\lambda_1\alpha_1)+\cdots+\lambda_n\alpha_n) = \sigma_1(0) = 0$. This is true for all σ_i, so

$$\lambda_1\sigma_i(\alpha_1) + \cdots + \lambda_n\sigma_i(\alpha_n) = 0.$$

This gives that $\lambda_1\cdot\mathrm{row}_1 + \cdots + \lambda_n\cdot\mathrm{row}_n = (0,0,\dots,0)$. So the matrix is not full rank, and $\det(M) = 0$. Thus $\operatorname{disc}(\alpha_1,\dots,\alpha_n) = 0$.

As $\operatorname{disc}(\alpha_1,\dots,\alpha_n) = 0$ and the second form is over $\mathbb{Q}^{n\times n}$, there exist $\lambda_1,\dots,\lambda_n$ in $\mathbb{Q}$ such that

$$\lambda_i \operatorname{tr}(\alpha_j\alpha_i) = 0$$

for all j. Therefore $\operatorname{tr}\left(\sum\lambda_i\alpha_j\alpha_i\right) = 0 \Rightarrow \operatorname{tr}\left(\alpha_j\sum\lambda_i\alpha_i\right) = 0$. Let $x = \lambda_i\alpha_i \in K$. Let $u = x^{-1} = \sum\mu_j\alpha_j$ with $\mu_j \in \mathbb{Q}$. This is possible as we are assuming $\alpha_1,\dots,\alpha_n$ are a basis for K. Now consider $\sum\mu_j\operatorname{tr}(\alpha_j x) = 0$ as $\operatorname{tr}(\alpha_j x) = 0$ for all j.

$$\sum\mu_j\operatorname{tr}(\alpha_j x) = \operatorname{tr}\left(\left(\sum\mu_j\alpha_j\right)x\right) = \operatorname{tr}(\mu\cdot x) = \operatorname{tr}(1) = n \neq 0.$$

This contradicts the fact that $\alpha_1, \dots, \alpha_n$ are being linearly independent. So there exist $\lambda_1, \dots, \lambda_n \in \mathbb{Q}$ with the desired property. □

9. January 29

Definition 28. A *vector space* V over a field F satisfies:

1. $u + (v + w) = (u + v) + w$
2. $u + v = v + u$
3. there exists 0 such that $0 + v = v$
4. there exists $1 \in F$ such that $1 \cdot v = v$.
5. for any u there exists $-u$ such that $u + (-u) = 0$.
6. $a(bu) = (ab)u$ where $a, b \in F$
7. $a(u + v) = au + av$
8. $(a + b)u = au + bu$

Definition 29. A module is a "vector space" over a ring (i.e., replace the word "field" with a "ring").

Remark. Every module we consider in this course will be a module over a *commutative ring.*

Example. Let $R = \mathbb{Z}$. Then $M = \{(a, b) : a, b, \in \mathbb{Z}\}$ is a $\mathbb{Z}$-module of dimension 2.

Example. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b, \in \mathbb{Z}\}$ is a $\mathbb{Z}$-module of dimension 2.

Example. The set of algebraic integers or algebraic integers in a number field are $\mathbb{Z}$-modules.

In each of these examples, the eight axioms are obvious. We need to show that $\alpha + \beta$ and $n \cdot \alpha$ are algebraic integers, where $n \in \mathbb{Z}$.

Let $A(x)$ and $B(x)$ be minimal polynomials for α and β. Recall that $\mathrm{Res}_x(A(x-y), B(y))$ has $\alpha + \beta$ as a root and is monic in $\mathbb{Z}[x]$. So $\alpha + \beta$ is an algebraic integer. Similarly, $n^{\deg(A)}A(x/n)$ is a monic polynomial in $\mathbb{Z}[x]$ with $n \cdot \alpha$ as a root.

Definition 30. We define $\mathbb{Z}_K$ as the set of algebraic integers in K.

Proposition 31. *$\mathbb{Z}_K$ is a* finite-dimensional *$\mathbb{Z}$-module of dimension $n = \deg(K)$.*

Corollary 2. *There exist $\alpha_1, \dots, \alpha_n \in \mathbb{Z}_K$ such that*

$$\mathbb{Z}_K = \{a_1\alpha_1 + \cdots + a_n\alpha_n : a_i \in \mathbb{Z}\}.$$

Note, however, that this basis is not *unique.*

Definition 32. Let $\alpha_1, \dots, \alpha_n$ be a basis for $\mathbb{Z}_K$. Then the *discriminant of* K is

$$\mathrm{disc}(K) = \mathrm{disc}(\alpha_1, \dots, \alpha_n).$$

Note that the definition is independent of the choice of basis.

Example. Let $K = \mathbb{Q}(i)$. Let $a + bi \in \mathbb{Q}(i)$ with $a, b \in \mathbb{Q}$. This has minimal polynomials $x - 1$ if $b = 0$, or $x^2 - 2ax + a^2 + b^2$ if $b \neq 0$. From the second, we have $2a \in \mathbb{Z}$, so $a \in \frac{1}{2}\mathbb{Z}$. From $a^2 + b^2 \in \mathbb{Z}$, and playing with congruences we have $a, b \in \mathbb{Z}$. So $\mathbb{Z}_K = \mathbb{Z}[i]$. This clearly has a basis $\{1, i\}$. So

$$\mathrm{disc}(\mathbb{Q}(i)) = \mathrm{disc}(1, i) = \left(\det\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}\right)^2 = (-i - i)^2 = -4.$$

Example. Note that we can write $K = \mathbb{Q}(\alpha)$ where α is a root of x^2+1, x^2+4, or x^2+9. These have discriminant

$$\begin{aligned}\operatorname{disc}(x^2+1) &= \operatorname{Res}(x^2+1, 2x) = -4\\ \operatorname{disc}(x^2+4) &= \operatorname{Res}(x^2+4, 2x) = -16 = -4\cdot 2^2\\ \operatorname{disc}(x^2+9) &= -36 = -4\cdot 3^2.\end{aligned}$$

Proposition 33. *Let $A(x)$ be an irreducible polynomial of degree n in $\mathbb{Z}[x]$ with root θ, which is an algebraic integer. Let $K = \mathbb{Q}(\theta)$. Then*

(1) $\operatorname{disc}(A(x)) = \operatorname{disc}(1, \theta, \theta^2, \dots, \theta^{n-1})$
(2) $\operatorname{disc}(A(x)) = \operatorname{disc}(K) f^2$ *where* $f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$.

Proof. You will prove this in Assignment #2. □

Proposition 34 (Stickelburger's theorem)**.** *Let $\alpha_1, \dots, \alpha_n$ be algebraic integers. Then*

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) \equiv 0 \textit{ or } 1 \pmod 4.$$

Proposition 35. *If K and L are number field with $K \subseteq L$ then* $\operatorname{disc}(K)^{[L:K]} \mid \operatorname{disc}(L)$.

9.1. **The subfield problem**

Given K and L number fields, we wish to know if $K \subseteq L$ or $K \cong K' \subseteq L$. Some simpler methods first:

(1) Degree divisibility check: the easiest way to check is whether $\deg(K) \nmid \deg(L)$. If this is the case, then K cannot be a subfield of L.
(2) With discriminant of two fields: If $\operatorname{disc}(K)^{[L:K]} \nmid \operatorname{disc}(L)$, then K cannot be a subfield of L. But the problem with this approach is that this requires finding an integral basis, which is easier said than done.
(3) However, we don't need to find an integral basis. In fact, we can just use $\operatorname{disc}(A(x))$ and $\operatorname{disc}(B(x))$ where $A(x)$ is the minimal polynomial of α, $K = \mathbb{Q}(\alpha)$ and $B(x)$ similarly defined.

Example. Let $K_1 = \mathbb{Q}(\theta_1)$ where θ_1 is a root of $x^3 - 4x - 8$. Similarly, let $K_2 = \mathbb{Q}(\theta_2)$ where θ_2 is a root of $x^3 - x - 2$ and $K_3 = \mathbb{Q}(\theta_3)$ where θ_3 is a root of $x^6 - x^2 - 1$. Since

$$\begin{aligned}\operatorname{disc}(x^3-4x-8) &= -2^6\cdot 23\\ \operatorname{disc}(x^3-x-2) &= 2^2\cdot 2\cdot 13\\ \operatorname{disc}(x^6-x^2-1) &= 2^6\cdot 23^2.\end{aligned}$$

We see that $K_2 \subsetneq K_3$ as $13^2 \nmid \operatorname{disc}(x^6 - x^2 - 1)$. Similarly, $K_1 \ncong K_2$ as $23 \nmid \operatorname{disc}(x^3 - x - 2)$. It is possible that $K_1 \subseteq K_3$.

There are three methods we will introduce to solve this problem.

(1) LLL method
Let $K = \mathbb{Q}(\alpha)$ where α has minimal polynomial $A(x)$. Let $L = \mathbb{Q}(\beta)$ where β has minimal polynomial $B(x)$. We see that $K \subseteq L$ if and only if $\alpha \in L$. This is equivalent to finding rationals a_i such that

$$\alpha = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{n-1}\beta^{n-1}.$$

This is equivalent to finding integers $k_0, k_1, \ldots, k_{n-1}, K$ such that $K \cdot \alpha = k_0 + k_1\beta + \cdots + k_{n-1}\beta^{n-1}$, and equivalently $0 = -K\cdot\alpha + k_0 + k_1\beta + \cdots + k_{n-1}\beta^{n-1}$. Now consider the basis

$$\begin{aligned}
&[1, 0, 0, \ldots, 0, M \cdot \alpha] \\
&[0, 1, 0, \ldots, 0, M \cdot \beta^0] \\
&[0, 0, 1, \ldots, 0, M \cdot \beta^1] \\
&[0, 0, 0, \ldots, 1, M \cdot \beta^{n-1}].
\end{aligned}$$

Example. Let $\theta_1 \approx 2.6494\ldots$, which is a root of $x^3 - 4x - 8$ and $\theta_3 \approx 1.15096\ldots$ a root of $x^6 - x^2 - 1$. Construct this basis using $M = 1000$. The LLL-reduced basis gives us

$$\begin{aligned}
&[-1, 0, 0, 2, 0, 0, 0, 0] \\
&[-2, 0, 0, 0, 1, 1, 1, 0.38446\ldots] \\
&\qquad\qquad\vdots
\end{aligned}$$

This gives us a guess that $\alpha = 2\beta^2$. But of course we still need to verify this. If true, then $x^3 - 4x - 8$ evaluated at $2\beta^2$ should be 0. Indeed, $(2\beta^2)^2 - 4(2\beta^2) - 8 = 8(\beta^6 - \beta^2 - 1) = 0$ as required. Therefore $a \in \mathbb{Q}(\beta)$ so $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta)$. If we wish to know if $K \cong K' \subseteq L$, we need to check if $\alpha' \in Q(\beta)$ for all conjugates of α. For LLL, we LLL-reduce all rows containing the β's first, and use this as a starting point for adding the last row dependent on the conjugates of α.

10. February 3: the subfield problem, continued – the linear algebra method

Consider the subfield problem; let $K = \mathbb{Q}(\alpha)$, with minimal polynomial $A(x)$, and $L = \mathbb{Q}(\beta)$ with minimal polynomial $B(x)$. We want to know whether $K \subseteq L$ or $K \cong K_i \subseteq L$. The next proposition covers the linear algebra method.

Proposition 36. *Let $A(x) = \prod(x-\alpha_i) \in \mathbb{Z}[x]$ and $B(x) = \prod(x-\beta_i) \in \mathbb{Z}[x]$ with $K_i = \mathbb{Q}(\alpha_i)$ and $L = \mathbb{Q}(\beta)$. Assume $\deg(A)\,|\deg(B)$. Then $K_i \subseteq L$ for some i if and only if there exists a map φ from $[1, 2, \ldots, \deg(B)]$ to $[1, 2, \ldots, \deg(A)]$ that is $\deg(B)/\deg(A)$ to 1 such that*

$$s_h := \sum_{i=1}^{\deg(B)} \alpha_{\varphi(i)}\beta_i^h \in \mathbb{Z}$$

for all $h, 1 \le h < \deg(B)$.

Proof. ($\Rightarrow$) Let $n = \deg(B), m = \deg(A)$. Assume that $K_i \subseteq L$ for some i. This implies that $\alpha_i \in L = \mathbb{Q}(\beta)$. So there exists some $P(x) \in \mathbb{Q}[x]$ such that $\alpha_i = P(\beta)$. This implies that $P(\beta_j) = \alpha_k$ for some k depending on j. This is a map from $[\beta_1, \ldots, \beta_n]$ to $[\alpha_1, \ldots, \alpha_m]$

that is n/m to 1. Take φ such that $\varphi(j) = i$ when $\alpha_i = P(\beta_j)$. Notice

$$\begin{aligned} s_h &:= \sum_{i=1}^{\deg(B)} \alpha_{\varphi(i)} \beta_i^h \\ &= \sum_{i=1}^{\deg(B)} P(\beta_i)\beta_i^h = \operatorname{tr}(P(\beta_i)\beta_i^h). \end{aligned}$$

Note that $\alpha_j \beta_i^h = P(\beta_i)\beta_i^h$ is an algebraic integer, since β_i and $P(\beta_i) = \alpha_{\varphi(i)}$ are algebraic integers, which implies that $P(\beta_i)\beta_i^h$ is an algebraic integer. Therefore $\operatorname{tr}(P(\beta_i)\beta_i^h) \in \mathbb{Z}$ as required.

($\Leftarrow$) Assume the other direction, that there exists $\varphi : [1, 2, \ldots, n] \to [1, 2, \ldots, m]$ such that

$$s_h = \sum \alpha_{\varphi(i)} \beta_i^h \in \mathbb{Z}$$

for $1 \le h < n$. Consider the equation

$$\underbrace{\begin{pmatrix} \operatorname{tr}(\beta^0\beta^0) & \cdots & \operatorname{tr}(\beta^{n-1}\beta^0) \\ \vdots & & \vdots \\ \operatorname{tr}(\beta^0\beta^{n-1}) & \cdots & \operatorname{tr}(\beta^{n-1}\beta^{n-1}) \end{pmatrix}}_{=:M} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}.$$

We see that $\det(M) = \operatorname{disc}(1, \beta, \cdots, \beta^{n-1}) \neq 0$. Hence there exists a unique solution $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. Write $P(x) = a_{n-1}x^{n-1} + \cdots + a_0$. We have

$$\begin{aligned} \operatorname{tr}(P(\beta)\beta^h) &= \operatorname{tr}\left(\left(\sum a_i \beta^i\right) \beta^h\right) \\ &= \sum a_i \operatorname{tr}(\beta^i \beta_h) \\ &= s_h \in \mathbb{Z}. \end{aligned}$$

We claim that $P(\beta_i) = \alpha_{\varphi(i)}$. To see this, consider

$$\begin{pmatrix} \beta_1^0 \\ \vdots \\ \beta_1^{n-1} \\ 0 \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}.$$

By construction of P, we see that $P(\beta_i) = \gamma_i$ is a solution. By assumption of the existence of φ, we have $\gamma_i = a_{\varphi(i)}$ is a solution. As the determinant of the matrix is non-zero, this has a unique solution. Hence $\alpha_{\varphi(i)} = P(\beta_i) \in \mathbb{Q}(\beta_i)$. This proves the result. □

Example. Let $K = \mathbb{Q}(\alpha)$ with a root of $A(x) = x^3 - 4x - 8$, and $L = \mathbb{Q}(\beta)$ with β the root of $B(x) = x^6 - x^2 - 1$.

Step I. Check discriminants (already done in a previous example).

Step II. We want a two-to-one map from $[1, 2, \ldots, 6]$ to $[1, 2, 3]$. There are $6!/(2!2!2!) = 90$ possible maps. Only six of those maps have $s_1 \in \mathbb{Z}$. Out of those six maps, only three satisfy $s_2 \in \mathbb{Z}$ and $s_3 \in \mathbb{Z}$. However, only one of the surviving three maps has $s_4 \in \mathbb{Z}$. This one also has $s_5 \in \mathbb{Z}$.

Note that if there were no maps in the last step, then $K_i \subsetneq L$ for all i. The one map that survives is $\varphi : 3,4 \mapsto 1; 2,5 \mapsto 2; 1,6 \mapsto 3$. This map has $s_0 = s_1 = 0, s_2 = 8, s_3 = 0, s_4 = 12, s_5 = 0$. By solving

$$M \begin{pmatrix} a_0 \\ s_1 \\ \vdots \\ a_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 8 \\ 0 \\ 12 \\ 0 \end{pmatrix}$$

we find such that $\alpha_i = P(\beta_j)$,

Remark. Some remarks on the subfield problem methods we covered:

(1) LLL will prove (eventually) that $K_i \subseteq L$ for some i, assuming it is true.
(2) LLL will *never* be able to show that $K_i \subseteq L$ for all i.
(3) The linear algebra method will answer both directions, but the number of maps can be *very* high for large degree polynomials.

11. February 3: the subfield problem, continued – the factoring method

11.1. Factoring polynomials re-visited (Part 3)

The last method for looking at the subfield problem requires us to factor $P(x)$ in $K[x]$, where $K = \mathbb{Q}(\theta)$. Let $K = \mathbb{Q}(\theta)$, where θ is an algebraic integer with minimal polynomial $T(x)$. We wish to factor $A(x) \in K[x]$. Our gcd and division algorithms from before still work. As before, we can assume without loss of generality that $A(x)$ is square-free by looking at $P(x)/\gcd(P, P')$. Recall that we defined the norm of $\alpha \in K$ as $\mathrm{N}(\alpha) = \prod \sigma_i(\alpha)$ where σ_i are all the field embeddings.

We can extend this to the norm of a polynomial

$$\mathrm{N}(\alpha_n x^n + \cdots + \alpha_0) = \prod (\sigma_i(\alpha_n)x^n + \cdots + \sigma_i(\alpha_0)).$$

Note that $\deg(\mathrm{N}(P)) = \deg(K) \cdot \deg(P)$. Recall that $\mathrm{N}(\alpha) \in \mathbb{Q}$. Similarly, we have $\mathrm{N}(P(x)) \in \mathbb{Q}[x]$. There are three main results that allow us to factor in $K[x]$.

Lemma 1. *Let $P(x)$ be an irreducible polynomial in $K[x]$. Then $\mathrm{N}(P(x))$ is a power of an irreducible polynomial in $\mathbb{Q}[x]$.*

Example. Let $P(x) = x - 1$. Then $\mathrm{N}(P) = (x-1)^{\deg(K)}$ is not irreducible but is a power of an irreducible polynomial.

Example. Consider $A(x) = x^3 - \sqrt{2}x + 2 \in \mathbb{Q}(\sqrt{2})[x]$. Then

$$\mathrm{N}(A) = (x^3 - \sqrt{2}x + 2)(x^3 + \sqrt{2}x + 2) = x^6 - 2x^4 - 2x^2 + 4 = (x^2 - 2)(x^4 - 2).$$

Hence $A(x)$ is not irreducible.

Remark. The converse of Lemma 1 above is *not* true. Consider $A(x) = (x - \sqrt{2})^2(x + \sqrt{2}) \in \mathbb{Q}(\sqrt{2})[x]$. Then $\mathrm{N}(A) = (x^2 - 2)^3$.

Lemma 2. *Let $P(x)$ be square-free in $K = \mathbb{Q}(\theta)$. Then there are finitely many $k \in \mathbb{Q}$ such that $\mathrm{N}(P(x - k\theta))$ is not square-free.*

Example. Let $A(x) = x^2 - 2 \in \mathbb{Q}(\sqrt{2})[x]$. Then $\mathrm{N}(A(x)) = (x^2-2)^2$ is not square-free, and $\mathrm{N}(A(x-\sqrt{2})) = \mathrm{N}(x^2 - 2\sqrt{2}x + 2 - 2) = x^2(x^2-8)$ not square-free. But $\mathrm{N}(A(x-2\sqrt{2})) = (x^2-2)(x^2-18)$ is square-free.

Theorem 7. *Let $P \in K[x]$ be square-free and $\mathrm{N}(P(x)) in \mathbb{Q}[x]$ square-free. Write $\mathrm{N}(P(x)) = \prod N_i(x)$. Then $P(x) = \prod \gcd(P, N_i)$ is a factorization of $P(x)$.*

12. February 3 lecture corrigendum

Last class, it was said that if there are more than one maps "surviving" then one needs to increase the digits of accuracy, but it was wrong.

We get a map $\varphi(i) = j$ if there exists a polynomial $P(x)$ such that $\alpha_j = P(\beta_i)$. Let $L = \mathbb{Q}(\sqrt[4]{2})$ and $K = \mathbb{Q}(\sqrt{2})$. Here $\beta_1 = \sqrt[4]{2}, \beta_2 = -\sqrt[4]{2}, \beta_3 = \sqrt[4]{2}i, \beta_4 = -\sqrt[4]{2}i$. Here, $\alpha_1 = \beta_1^2 = \beta_2^2$ and $\alpha_1 = -\beta_3^2 = -\beta_4^2$. All of these give us legitimate maps $P_1(x) = x^2, P_2(x) = -x^2$. That is, both maps φ_1 and φ_2 give us valid maps, where

$$\varphi_1(x) = \begin{cases} 1 & (x = 1, 2) \\ 2 & (x = 3, 4) \end{cases}$$

and

$$\varphi_1(x) = \begin{cases} 2 & (x = 1, 2) \\ 1 & (x = 3, 4) \end{cases}$$

13. February 5

Example. Let $A(x) = x^5 - \sqrt{2}x^4 + (-\sqrt{2} - 2)x^3 + (2\sqrt{2} + 2)x^2 + 2\sqrt{2}x - 4 \in \mathbb{Q}(\sqrt{2})[x]$.

Step 1: Make sure that we are looking at a squarefree polynomial.

Since $\gcd(A, A') = x - \sqrt{2}$, write $A_0 := A/G$ be the squarefree part. Note $A_0(x) = x^4 + (-\sqrt{2} - 2)x + 2\sqrt{2}$. There are only finitely many k where $\mathrm{N}(A_0(x - k\sqrt{2}))$ is not squarefree. Find a k where this is squarefree.

$$\begin{aligned} \mathrm{N}(A_0(x)) &= (x^4 - 2)(x^2 - 2)^2 \\ \mathrm{N}(A_0(x - \sqrt{2})) &= x^2(x^2 - 8)(x^4 - 4x^2 - 8x - +2) \\ \mathrm{N}(A_0(x - 2\sqrt{2})) &= (x^2 - 18)(x^2 - 2)(x^4 - 16x - 16x + 62). \end{aligned}$$

We see that $\mathrm{N}(A_0(x - 2\sqrt{2}))$ is squarefree. We have

$$\begin{aligned} A(x - 2\sqrt{2}) =& \gcd(A_0(x - 2\sqrt{2}), x^2 - 18) \cdot \gcd(A_0(x - 2\sqrt{2}), x^2 - 2) \cdot \\ & \gcd(A_0(x - 2\sqrt{2}), x^4 - 16x^2 - 16x + 62) \\ =& (x - 3\sqrt{2})(x - \sqrt{2})(x^2 - 4\sqrt{2}x + 8 - \sqrt{2}). \end{aligned}$$

Hence $A_0(x) = (x - \sqrt{2})(x + \sqrt{2})(x^2 - \sqrt{2})$, and $A_(x) = (x - \sqrt{2})^2(x + \sqrt{2})(x^2 - \sqrt{2})$ is the full factorization.

Lemma 3. *If $A(x) \in K[x]$ is an irreducible polynomial, then $\mathrm{N}(A(x))$ is a power of an irreducible polynomial in $\mathbb{Q}[x]$.*

Proof. Write $\mathrm{N}(A(x)) = N_1(x)^{e_1} \cdots N_k(x)^{e_k}$. We know that $A(x) \,|\, \mathrm{N}(A(x))$, hence there is some i such that $A(x) \mid \mathrm{N}_i(x)$. Consider σ a field embedding from K to $\mathbb{C}$. We see that $\sigma(A(x)) \,|\, \sigma(\mathrm{N}_i(x))$ as σ leaves $\mathbb{Q}$ fixed, we have $\sigma(\mathrm{N}_i(x)) = \mathrm{N}_1(x)$. So $\sigma(A(x)) \,|\, \mathrm{N}_i(x)$ for all σ. Therefore

$$\prod_\sigma \sigma(A(x)) \,|\, \prod_\sigma \mathrm{N}_i(x),$$

so indeed $\mathrm{N}(x) \mid \mathrm{N}_i(x)^{\deg(K)}$. This proves that $\mathrm{N}(A(x))$ is a power of an irreducible as required. □

Lemma 4. *Let $A(x)$ be squarefree. Then there are only finitely many k such that $\mathrm{N}(A(x - k\theta))$ is not squarefree. (Here, $K = \mathbb{Q}(\theta)$.)*

Proof. Let $A(x) = \prod(x - \alpha_i)$, so $A(x - k\theta) = \prod(x - \alpha_i - k\theta)$. Let $\sigma_1, \dots, \sigma_n$ be the $n = \deg(K)$ field embeddings. So

$$\mathrm{N}(A(x - k\theta)) = \prod_{j=1}^{n} \prod_i (x - \sigma_j(\alpha_i) k \sigma_j(\theta)).$$

If this is *not* squarefree, then there exist i_1, i_2, j_1, j_2 such that

$$\alpha_{i_1,j_1} + k\sigma_{j_1}(\theta) = \alpha_{i_2,j_2} + k\sigma_{j_2}(\theta).$$

Thus

$$k = \frac{\alpha_{i_2,j_2} - \alpha_{i_1,j_1}}{\sigma_{j_1}(\theta) - \sigma_{j_2}(\theta)}.$$

There are only finitely many choices for i_1, i_2, j_1, j_2. □

Lemma 5. *Let $A(x)$ be squarefree and $\mathrm{N}(A(x)) = \mathrm{N}_1(x)\,\mathrm{N}_2(x) \cdots \mathrm{N}_k(x)$ also be squarefree. Then*

$$A(x) = \prod \gcd(\mathrm{N}_i(x), A(x)).$$

Proof. Let $A_i(x)$ be an irreducible factor of $A(x)$. We know that $\mathrm{N}(A_i(x))$ divides $\prod \mathrm{N}_j(x)$, and is a power of an irreducible. As $\prod \mathrm{N}_j(x)$ is squarefree, we have that $\mathrm{N}(A_i(x))$ is irreducible. So $\mathrm{N}(A_i(x)) = \mathrm{N}_j(x)$ for some j. By reordering if necessary, we can assume that $\mathrm{N}(A_i(x)) = \mathrm{N}_i(x)$. We see that $A_i(x) \mid \mathrm{N}_i(x)$. Furthermore, for all $j \neq i$, we have $\gcd(A_j(x), \mathrm{N}_i(x)) = 1$. Therefore, $A_i(x) = \gcd(A(x), \mathrm{N}_i(x))$. □

13.1. The subfield problem: the third method

Theorem 8. *Let $K = \mathbb{Q}(\alpha)$ with $A(x)$ the minimal polynomial of α. Let $L = \mathbb{Q}(\beta)$ with $B(x)$ the minimal polynomial of β. Then $\alpha \in L$ if and only if $A(x)$ factored in $L[x]$ has a factor $x - \alpha$. Equivalently, there is a one-to-one correspondence between the linear factors of $A(x)$ in $L[x]$ and subfields conjugate to K, subfields of L.*

Example. Let $\alpha \approx 2.2599$ with minimal polynomial $x^3 - 3x^2 + 3x - 3$ and $\beta \approx -0.6299 - 2.0911i$ with minimal polynomial $x^6 - 3x^4 - 4x^3 + 3x^2 + 12x + 5$. First, discriminants of these two polynomials are $2^2 \cdot 3^3$ and $2^{10} \cdot 3^6 \cdot 7 \cdot 89$ respectively. Factoring $x^3 - 3x^2 + 3x - 3$ over $L[x]$ gives $(x^2 + C_1(\beta)x + C_0(\beta))(x - \frac{6}{11}\beta^5 + \frac{9}{22}\beta^4 - \frac{20}{11}\beta^3 + \frac{39}{11}\beta^2 - \frac{50}{11}\beta - \frac{113}{11}) \approx (x^2 - 0.72x + 1.327)(x - 2.2599)$. This tells us that

$$\alpha = \frac{6}{11}\beta^5 + \cdots + \frac{113}{11} \in \mathbb{Q}(\beta),$$

so $K \subseteq L$.

13.2. Applications

Given α, β, we have shown how to check if $\alpha \in \mathbb{Q}(\beta)$, thereby proving that $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta)$. If $\deg(\alpha) = \deg(\beta)$ then this is equivalent to $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$.

We know that if $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ then there exists a single element θ such that $K = \mathbb{Q}(\theta)$. How do we find this θ? We see that if we can do this for $k = 2$ then we can do the general case by induction.

Let $K = \mathbb{Q}(\alpha, \beta)$. Let $A(x) = x - \alpha$. This is clearly irreducible. So there are only finitely many β such that $\mathrm{N}(A(x - k\beta))$ is not squarefree. Pick a k such that $\mathrm{N}(A(x - k\beta))$ is squarefree. So $\mathrm{N}(A(x - k\beta))$ is squarefree and irreducible of degree $\deg(K)$. Let $L = \mathbb{Q}(\alpha + k\beta)$. Clearly $\deg(K) = \deg(L)$ and $\alpha + k\beta \in K$ so $L \subseteq K$. Hence $K = L = \mathbb{Q}(\alpha + k\beta)$, and we can keep going by induction. In practice, we check if $\beta \in \mathbb{Q}(\alpha + k\beta)$ which gives $\alpha \in \mathbb{Q}(\alpha + k\beta)$ for various k until it works.

14. February 10: Orders and ideals

Many of these concepts have meaning outside of number fields, but we will assume we are in a number field to make life easier.

Definition 37. we say that M is an *order* of $K = \mathbb{Q}(\alpha)$ if M is a subring of K, and a finitely generated sub-module of rank $n := \deg(K)$.

Example. Let $K = \mathbb{Q}(\sqrt{2})$. $\mathbb{Z} \subseteq K$ is a subring of K and a finitely-generated $\mathbb{Z}$-module, but its rank is 1, which is not equal to $\deg(K) = 2$. Therefore $\mathbb{Z}$ is *not* an order.

Consider instead $\mathbb{Z}[2^{-1}] := \{a_0 + a_1 2^{-1} + a_2 2^{-2} + \cdots + a_n 2^{-n} : a_i \in \mathbb{Z}, n \in \mathbb{Z}\} = \{a \cdot 2^{-k} : a \in \mathbb{Z}, k \in \mathbb{N}\}$. This is a subring of K, and a $\mathbb{Z}$-submodule of K. However, there is no finite basis that works. Therefore this is not an order.

However, the subring $M := 2\mathbb{Z}_K = \{2a + 2\sqrt{2}b : a, b, \in \mathbb{Z}\}$ is a subring of K, and a $\mathbb{Z}$-submodule of K of rank $2 = \deg(K)$. Therefore this is an order.

Theorem 9. *The following are equivalent:*

(1) α is an algebraic integer.
(2) $\mathbb{Z}[\alpha]$ is a finitely generated abelian group
(3) α belongs to a subring of $\mathbb{C}$ that is a finitely generated abelian group
(4) There exists a non-zero finitely-generated abelian group L of $\mathbb{C}$ such that $\alpha L \subseteq L$.

Corollary 3. *Let R be an order of K and $\alpha \in R$. Then $\alpha \in \mathbb{Z}_K$.*

Corollary 4. *If R is an order, then $R \subseteq \mathbb{Z}_K$.*

Definition 38. An *ideal of* $\mathbb{Z}_K$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}_K$ such that whenever $i \in I$ and $r \in \mathbb{Z}_K$, it follows $ir \in I$.

Example. Let $K = \mathbb{Q}$ and $\mathbb{Z}_K = \mathbb{Z}$. The subrings of $\mathbb{Z}$ look like $a\mathbb{Z} = \{an : n \in \mathbb{Z}\}$. It is easy to see that all $a\mathbb{Z}$ are ideals. The two trivial ideals of $\mathbb{Z}_K$ are the $\mathbb{Z}_K$ itself and the zero ideal $\{0\}$.

Example. Let $K = \mathbb{Q}(\sqrt{2})$. Then $\mathbb{Z}_K = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Let $I = 2\mathbb{Z}_K = \{2a + 2b\sqrt{2} : a, b, \in \mathbb{Z}\}$. To see that I is an ideal we note that

$$(2a + 2b\sqrt{2})(c + d\sqrt{2}) = 2(ac + 2bd) + 2(ad + bc)\sqrt{2} \in I.$$

Thus I is an ideal.

Example. $\mathbb{Z}$ is not an ideal in $\mathbb{Z}_K$ where $K = \mathbb{Q}(\sqrt{2})$: clearly $\sqrt{2} \in \mathbb{Z}_K$ and $1 \in \mathbb{Z}$ but $\sqrt{2} \cdot 1 \notin \mathbb{Z}$.

Lemma 6. *Let I be a non-zero ideal. Then* $\operatorname{rank}(I) = \deg(K)$.

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis for $\mathbb{Z}_K$. Let $i \in I$ be non-zero. Then $\{i\alpha_1, \ldots, i\alpha_n\} \subseteq I$, and $\operatorname{span}\{i\alpha_1, \ldots, i\alpha_n\}$ has rank n. Thus I has rank n. □

Proposition 39. *Let I and J be ideals. Then the following are also ideals:*

(1) $IJ := \{\sum a_n b_n : a_n \in I, b_n \in J, n \in \mathbb{N}\}$
(2) $I \cap J = \{a : a \in I, a \in J\}$
(3) $I + J = \{a + b : a \in I, b \in J\}$

Example. Let $K = \mathbb{Q}(\sqrt{2})$. Then $I = 3\mathbb{Z}_K = \{3a + 3b\sqrt{2} : a, b \in \mathbb{Z}\}$ and $J = \{2a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. One can verify that I and J are ideals. Then

$$\begin{aligned} IJ &= \{(3a + 3b\sqrt{2})(2c + d\sqrt{2}) : a, b, c, d \in \mathbb{Z}\} \\ &= \{6ac + 6bd + 3a \cdot \sqrt{2}d + 6bc\sqrt{2} : a, b, c, d \in \mathbb{Z}\} \\ &= \{6e + 3f\sqrt{2} : e, f \in \mathbb{Z}\} \\ I \cap J &= \{6a + 3b\sqrt{2} : a, b \in \mathbb{Z}\} = IJ \\ I + J &= \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} = \mathbb{Z}_K. \end{aligned}$$

Example. Let $K = \mathbb{Q}$ and $\mathbb{Z}_K = \mathbb{Z}$. If $I = 4\mathbb{Z}$ and $J = 6\mathbb{Z}$, then $IJ = 24\mathbb{Z}, I \cap J = 12\mathbb{Z}, I + J = 2\mathbb{Z}$.

In both cases we have $IJ \subseteq I \cap J \subseteq I \subseteq I + J$.

Theorem 10. *Let I and J be ideals of $\mathbb{Z}_K$. If $I + J = \mathbb{Z}_K$ then $IJ = I \cap J$.*

Proof. We have $IJ \subseteq I \cap J$. Assume $I + J = \mathbb{Z}_K$. Then there exist $i \in I$ and $j \in J$ such that $i + j = 1$. Let $x \in I \cap J$. As $i \in I, x \in I \cap J \subseteq J$ we have $ix \in IJ$. Similarly, $xj \in IJ$. So $ix + xj = x(i + j) = x \cdot 1 = x \in IJ$. Therefore $I \cap J \subseteq IJ$ as required. □

So if we consider the case $K = \mathbb{Q}$, we see that ideals are of the form $a\mathbb{Z}$, for $a \in \mathbb{Z}$. We have $(a\mathbb{Z})(b\mathbb{Z}) = (ab)\mathbb{Z}$, and $a\mathbb{Z} \cap b\mathbb{Z} = \operatorname{lcm}(a, b)\mathbb{Z}$ and $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$. Many of the concepts over the integers (e.g. factorization) extend to ideals of $\mathbb{Z}_K$. That is, we can factor an ideal in $\mathbb{Z}_K$ uniquely into prime ideals.

In general, this does not work in $\mathbb{Z}_K$. That is, there are K's such that $\mathbb{Z}_K$ is *not* a unique factorization domain (UFD). The extent to which $\mathbb{Z}_K$ is not a UFD is measured by something called the *class group*.

We are going to build the tools to factor ideals into prime ideals, and to do computations on this class group. Before doing any of these, we wish to find a good representation for ideals. In particular, we need a representation that allows us to compute $IJ, I \cap J, I + J, I \subseteq J$.

14.1. Representations and calculations on $\mathbb{Z}$-modules and Hermite normal forms

Let $\alpha_1, \ldots, \alpha_n$ be a basis of $\mathbb{Z}_K$. Any $\mathbb{Z}$-submodule of $\mathbb{Z}_K$ will have a basis $\theta_1, \ldots, \theta_n$. Then we can write

$$\theta_i = \sum w_{ij}\alpha_j \text{ for some } w_{ij} \in \mathbb{Z}.$$

Definition 40. The representation

$$W = \begin{pmatrix} w_{11} & w_{12} & \cdots & w_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ w_{n1} & w_{n2} & \cdots & w_{nn} \end{pmatrix}$$

is the *Hermite normal form* if:

(1) $w_{ij} = 0$ if $i > j$
(2) $w_{ii} > 0$
(3) $0 \leq w_{ij} < w_{jj}$ for all $i < j$.

Example. Consider the module with basis $\alpha_1, \alpha_2, \alpha_3$, where

$$\alpha_1 = 2\sqrt[3]{2}^2 + 9\sqrt[3]{2} - 17$$
$$\alpha_2 = 6\sqrt[3]{2}^2 + 6\sqrt[3]{2} + 3$$
$$\alpha_3 = 4\sqrt[3]{2}^2 + 3\sqrt[3]{2} + 6.$$

If $\alpha_1, \alpha_2, \alpha_3$ is a basis for M, then the following are also basis for M:

(1) any permutation of $\alpha_1, \alpha_2, \alpha_3$
(2) any scalar multiple of a basis element
(3) $\alpha_1 + k\alpha_2, \alpha_2, \alpha_3$ for some scalar k also forms a basis.

So start with, in our example,

$$\begin{pmatrix} 2 & 9 & -17 \\ 6 & 6 & 3 \\ 4 & 3 & 6 \end{pmatrix} \to \begin{pmatrix} 2 & 9 & -17 \\ 0 & -21 & 54 \\ 0 & -15 & 40 \end{pmatrix} \to \begin{pmatrix} 2 & 9 & -17 \\ 0 & 15 & -40 \\ 0 & 21 & -54 \end{pmatrix} \to$$
$$\begin{pmatrix} 2 & 9 & -17 \\ 0 & 15 & -40 \\ 0 & 6 & -14 \end{pmatrix} \to \begin{pmatrix} 2 & 9 & -17 \\ 0 & 3 & -12 \\ 0 & 6 & -14 \end{pmatrix} \to \begin{pmatrix} 2 & 9 & -17 \\ 0 & 3 & -12 \\ 0 & 0 & 10 \end{pmatrix} \to$$
$$\begin{pmatrix} 2 & 9 & -17 \\ 0 & 3 & 8 \\ 0 & 0 & 10 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & -41 \\ 0 & 3 & 8 \\ 0 & 0 & 10 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 9 \\ 0 & 3 & 8 \\ 0 & 0 & 10 \end{pmatrix}.$$

So we can read $[\mathbb{Z}_K : M]$ from this matrix. This is just the product of the diagonal entries. Thus $[\mathbb{Z}_K : M] = 60$.

15. February 12

Given a module (or an order, or an ideal), it is easy to see that its Hermite normal form (HNF) is unique up to order and choice of basis for $\mathbb{Z}_K$. That is, for two $\mathbb{Z}$-modules in $\mathbb{Z}_K$, we can check equality by checking if they have the same HNF. We now wish to show how we can compute $M_1 + M_2, M_1 \cdot M_2, M_1 \cap M_2$ or check if $M_1 \subseteq M_2$.

(1) Addition. $M_1 + M_2 := \{m_1 + m_2 : m_1 \in M_1, m_2 \in M_2\}$. To find a basis for $M_1 + M_2$, it suffices to combine the basis elements of M_1 with those of M_2, i.e., the basis with $2n$ elements $\{a_1, \ldots, b_n\}$ where $\{a_1, \ldots, a_n\}$ is a basis for M_1 and similarly for the b_i. But there are too many elements; however this is okay since we will figure out

which ones to toss out by using the Hermite normal form. That is, we write this as a matrix with “too many” rows, and convert it toi HTF, and remove the zero vectors.

Example. Let $M_1 = \{(2\theta^2+\theta)a+(3\theta+b)+8c\}$ and $M_2 = \{(4\theta^2+\theta+1)a+(2\theta+5)b+6c\}$, where $\theta^3 = 2$.

$$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 3 & 6 \\ 0 & 0 & 8 \\ 4 & 1 & 1 \\ 0 & 2 & 5 \\ 0 & 0 & 6 \end{pmatrix} \to \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \\ 0 & -1 & 1 \\ 0 & 2 & 5 \\ 0 & 0 & 6 \end{pmatrix} \to \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Thus $M_1 + M_2 = \{2\theta^2 a + \theta b + c : a, b, c \in \mathbb{Z}\}$.

(2) Multiplication. Recall that $I \cdot J = \{\sum a_i b_i : a_i \in I, b_i \in J\}$. We can multiply basis elements of I by those of J and this gives a basis for $I \cdot J$. But this method has some issues. First, there are too many (n^2 of them) multiplications. There is a faster/better way if I and J are both ideals. For instance, let $I = (1+i)\mathbb{Z}_K$ and $J = (2+i)\mathbb{Z}_K$ where $K = \mathbb{Q}(i)$ and $\mathbb{Z}_K = \mathbb{Z}[i]$. I has a basis $\{(1+i), i(1+i)\}$ and J has a basis $\{(2+i), (2+i)i\}$. So a basis for IJ is $\{\pm(1+i)(2+i), \pm(1+i)(2+i)\}$. Two of these are redundant, and we can use the Hermite normal form to see that a basis is $\{(1+i)(2+i), (1+i)(2+i)i\} = \{1+3i, (1+3i)i\}$.

(3) Intersection. $I \cap J = \{a : a \in I \text{ and } a \in J\}$. We will do this via the dual basis.

Definition 41. Let L be a lattice of full rank in $\mathbb{Z}^n$. Then the dual lattice, $\hat{L}$ is $\{v : \langle v.y \rangle \in \mathbb{Z} \text{ for } y \in L\}$.

Example. Let $I = \{a + 2b\sqrt{2} : a, b \in \mathbb{Z}\}$ as a $\mathbb{Z}$-submodule of $\mathbb{Z}_{\mathbb{Q}(\sqrt{2})}$. This has HNF $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. We can think of this as the lattice in $\mathbb{Z}^2$ of $L = \{(1,0)a+(0,2)b : a, b \in \mathbb{Z}\}$. Thus $\hat{L} = \{v : \langle v, x \rangle \in \mathbb{Z}, x \in L\}$. As inner products are linear with respect to addition, it suffices to look at basis elements

$$\begin{aligned} \hat{L} &= \{v : \langle v, x \rangle \in \mathbb{Z}, x \in \{(1,0), (0,2\}\} \\ &= \{(v_1, v_2) : \langle (v_1, v_2), (1,0) \rangle \in \mathbb{Z}, \langle (v_1, v_2), (0,2) \rangle \in \mathbb{Z}\} \\ &= \{(v_1, v_2) : v_1 \in \mathbb{Z}, 2v_2 \in \mathbb{Z}\} = \{(a, b/2) : a, b \in \mathbb{Z}\}. \end{aligned}$$

This is basis $(1,0), (0, 2^{-1})$.

But this is a rather ad-hoc way of finding a dual basis. But the following theorem provides a more systematic way of finding a dual basis:

Theorem 11. *Let L be a lattice with full rank and let B be a basis. Then $\hat{L}$ has basis $D = (B^T)^{-1}$.*

Example. In the previous example, L had basis $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ and $\hat{L}$ had basis $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1/2 \end{smallmatrix}\right)$.

Proof. We will show that $\hat{L} \subseteq D[\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and vice versa. Let $v_1 \in \mathbb{Z}^n$ and $Dv_1 \in D\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Then

$$\langle Dv_1, Bv_2 \rangle = v_1^T D^T B v_2 = v_1^T ((B^T)^{-1})^T B v_2 = v_1 B^{-1} B v_2 = v_1^T v_2 \in \mathbb{Z}.$$

Therefore $D\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \subseteq \hat{L}$. Let $v \in \hat{L}$.Then $\langle v_1, Bv_2 \rangle \in \mathbb{Z}$. This is true for all choices of v_2, including the basis elements. SO $\langle Bv_2, v \in \mathbb{Z}$, so $v_2^T B_5 t \in \mathbb{Z}$, hence $B^T v \in \mathbb{Z}^n$. This implies that $v \in (B^T)^{-1}\mathbb{Z}^n$ or $v \in D\mathbb{Z}^n$. Thus $\hat{L} \in D\mathbb{Z}^n$ as required. □

Theorem 12. *Let I and J be $\mathbb{Z}$-modules with bases B_I and B_J respectively. Let D be the basis of the lattice coming from $\hat{B}_I + \hat{B}_J$. Then $\hat{D}$ is the basis for $I \cap J$.*

Proof. Let N be the $\mathbb{Z}$-submodule with basis $\hat{D}$. Let $v \in N$. Then $\langle v, x \rangle \in \mathbb{Z}$ for all $x \in \hat{B}_I + \hat{B}_J$. So $\langle v, x_I \rangle \in \mathbb{Z}$ for $x_I \in \hat{B}_I \subseteq \hat{B}_I + \hat{B}_J$ and $\langle v, x_J \rangle \in \mathbb{Z}$ for $x_J \in \hat{B}_J$. So $v \in \widehat{(\hat{B}_I)}$ and $v \in \widehat{(\hat{B}_J)}$. But $\widehat{(\hat{B})} = B$, so this says $v \in I$ and $v \in J$, so $v \in I \cap J$.

Let $v \in I \cap J$. Then $\langle v, x_I \rangle \in \mathbb{Z}$ for $x_I \in \hat{B}_I$ and $\langle v, x_J \rangle \in \mathbb{Z}$ for $x_J \in \hat{B}_J$. So $\langle v, x_I + x_J \rangle \in \mathbb{Z}$ for $x_I + x_J \in \hat{B}_I + \hat{B}_J$. Thus $v \in \hat{D}\mathbb{Z}^n$ as required. □

Example. Let I have basis $\{2, 2\sqrt{2}\}$ and J have basis $\{4+\sqrt{2}, 1+2\sqrt{2}\}$ (in $\mathbb{Z}[\sqrt{2}]$). So in this case,

$$B_I = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, B_J = \begin{pmatrix} 4 & 1 \\ 1 & 2 \end{pmatrix}, B_J' = \begin{pmatrix} 1 & 2 \\ 0 & 7 \end{pmatrix}.$$

So

$$\hat{B}_I = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}, \hat{B}_J = \begin{pmatrix} 1 & 0 \\ -2/7 & 1/7 \end{pmatrix}$$

$$\hat{B}_I + \hat{B}_J = \frac{1}{14}\begin{pmatrix} 7 & 0 \\ 0 & 7 \\ 14 & 0 \\ 4 & -2 \end{pmatrix} \to \frac{1}{14}\begin{pmatrix} 7 & 0 \\ 0 & 7 \\ 4 & -2 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 3 \\ 0 & 7 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus

$$\widehat{\hat{B}_I + \hat{B}_J} = \begin{pmatrix} 14 & 0 \\ -6 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 4 \\ 0 & 14 \end{pmatrix}.$$

Thus $I \cap J$ has basis $\{2+4\sqrt{2}, 14\sqrt{2}\}$.

15.1. **Norms**

Proposition 42. *If I is an ideal, then it is a submodule of a maximal rank.*

Corollary 5. *This implies that $\mathbb{Z}_K/I$ is a finite ring (abelian). The size of this ring is called the norm of I, denoted $\mathrm{N}(I)$.*

Example. $2\mathbb{Z}[\sqrt{2}]$ is an ideal of $\mathbb{Z}[\sqrt{2}]$. Thus if $a+b\sqrt{2} \sim c+d\sqrt{2}$ then $(a-c)+(b-d)\sqrt{2} \in I$. Thus $a \equiv c, b \equiv d \pmod 2$. So this is a ring with four elements. Multiplication is given by

	0	1	$\sqrt{2}$	$1+\sqrt{2}$
0	0	0	0	0
1	0	$1\ \sqrt{2}$	$1+\sqrt{2}$	
$\sqrt{2}$	0	$\sqrt{2}$	0	$\sqrt{2}$
$1+\sqrt{2}$	0	$1+\sqrt{2}$	$\sqrt{2}$	1

Note that this ring is *not* a field, nor is it an integral domain. Here, $\mathrm{N}(I) = 4$. Also, if I is written in the Hermite normal form, then $\mathrm{N}(I) = \prod a_{ii}$. ALso, if I and J are ideals over $\mathbb{Z}_K$ then $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$.

16. February 24

Proposition 43. *Let I be a non-zero ideal of $\mathbb{Z}_K$. Then I is a $\mathbb{Z}$-submodule of $\mathbb{Z}_K$ of full rank.*

Definition 44. As I is of full rank this means that $\mathbb{Z}_K/I$ is a finite ring. This size of this ring is called the *norm of* I, denoted $\mathrm{N}(I)$.

Example. Let $I = \{2a + 2b\sqrt{2} : a, b \in \mathbb{Z}\}$ as an ideal of $\mathbb{Z}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$. We say that $a + b\sqrt{2} \sim_I c + d\sqrt{2}$ if and only if $a \equiv c, b \equiv d \pmod 2$. So our ring can be thought of as $\mathbb{F}_2 + \sqrt{2}\mathbb{F}_2 = \{a + b\sqrt{2} : a, b \in \mathbb{F}_2\}$. Thus $\mathbb{Z}[\sqrt{2}]/I$ has size 4, so $\mathrm{N}(I) = 4$. Note that this ring is a finite abelian ring but is not an integral domain, as $\sqrt{2}\sqrt{2} = 2 = 0$. Also, the norm can be read off of the Hermite normal form, which is $2I_2 = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$. Thus $\mathrm{N}(I)$ is the determinant of the Hermite normal form, or the product of the diagonal entries.

Proposition 45. *If I and J are ideals of $\mathbb{Z}_K$ then* $\mathrm{N}(I \cdot J) = \mathrm{N}(I)\,\mathrm{N}(J)$.

16.1. **Prime ideals**

Definition 46. We say I is a *prime ideal* if $\mathbb{Z}_K/I$ is an integral domain.

Proposition 47. *Any finite abelian ring that is also an integral domain is a finite field. Therefore if I is a prime ideal, then $\mathbb{Z}_K/I$ is a finite field.*

Example. $2\mathbb{Z}[\sqrt{2}] = \{2a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is *not* a prime ideal. Let $I = \sqrt{2}\mathbb{Z}[\sqrt{2}] = \{2a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. This has norm $\mathrm{N}(I) = \det\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right) = 2$. Thus $\mathbb{Z}[\sqrt{2}]/\sqrt{2}\mathbb{Z}[\sqrt{2}] \cong \mathbb{F}_2$. Therefore I is a prime ideal.

Theorem 13. *Let $\mathfrak{p}$ be a prime ideal such that $\mathfrak{p} \supseteq I_1 \cdot I_2 \cdot \cdots \cdot I_k$. Then there exists a j such that $\mathfrak{p} \supseteq I_j$.*

Remark. In the special case where $K = \mathbb{Q}$, this says $p\mathbb{Z} \supseteq a_1 I \cdot a_2 I \cdot \cdots \cdot a_k I$ implies $p \,|\, a_1 a_2 \cdots a_k$. Thus there exists j such that $p \,|\, a_j$, i.e., $p\mathbb{Z} \supseteq a_j I$.

Proof. The theorem is trivially true if $k = 1$. Assume $k = 2$. Let $\mathfrak{p} \supseteq I_1 \cdot I_2$. Assume that $I_i \not\subseteq \mathfrak{p}$ for all $i = 1, 2$. Then pick $x \in I_1, x \notin \mathfrak{p}$. Pick $y \in I_2, y \notin \mathfrak{p}$. Notice that the map $\mathbb{Z}_K \to \mathbb{Z}_k/\mathfrak{p}$ takes both x and y to non-zero elements. As $\mathbb{Z}_K/\mathfrak{p}$ is an integral domain, it follows that the image of $x \cdot y$ is non-zero. Hence $x \cdot y \notin \mathfrak{p}$. Clearly, $x \cdot y \in I_1 \cdot I_2 \subseteq \mathfrak{p}$, so we have a contradiction. Thus $\mathfrak{p} \supseteq I_1$ or $\mathfrak{p} \supseteq I_2$. This argument can be extended to the general case by induction. □

Remark. It should be noted that testing if $\mathfrak{p} \supseteq I_1$ is easy. We have $\mathfrak{p} \supseteq I$ if and only if $\mathfrak{p} + I = \mathfrak{p}$, which we can check by using the Hermite normal form.

Example. Let $I = 2\mathbb{Z}[\sqrt{2}]$ and $\mathfrak{p} = \sqrt{2}\mathbb{Z}[\sqrt{2}]$. We see that the Hermite normal form of $\mathfrak{p} + I$ is $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ so $\mathfrak{p} \supseteq I$. In fact, $I = \mathfrak{p} \cdot \mathfrak{p}$.

Theorem 14. *Every ideal I of $\mathbb{Z}_K$ can be written* uniquely *as*

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)} \text{ with } v_{\mathfrak{p}}(I) \geq 1$$

as a product over finitely many prime ideals.

Remark. We make some following remarks regarding $v_{\mathfrak{p}}(I)$, which is called the *valuation of I with respect to $\mathfrak{p}$*:

(1) $I \supseteq J \Rightarrow v_{\mathfrak{p}}(I) \leq v_{\mathfrak{p}}(J)$
(2) $v_{\mathfrak{p}}(I + J) = \min(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))$ (i.e., gcd)
(3) $v_{\mathfrak{p}}(I \cap J) = \max(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))$ (i.e., lcm)
(4) $v_{\mathfrak{p}}(IJ) = v_{\mathfrak{p}}(I) + v_{\mathfrak{p}}(J)$

Proposition 48. *Let $\mathfrak{p}$ be a prime ideal. Then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p.*

Proof. We see that $\mathfrak{p} \cap \mathbb{Z}$ is a subset of the integers closed under addition, i.e., $a\mathbb{Z}$ for some a. Consider the case when $a = 1$. Then $1 \in \mathfrak{p}$, but since $\mathfrak{p}$ is an ideal so we exclude this case. Now suppose that $a = m \cdot n$ be composite. So $m \cdot n \notin \mathfrak{p}$ hence have a non-zero image under $\mathbb{Z}_K \to \mathbb{Z}_K/\mathfrak{p}$. But their product is 0 under this image. Hence $\mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}$ for some prime p. □

Proposition 49. *The following are equivalent:*

(1) $\mathfrak{p} \supseteq p\mathbb{Z}$
(2) $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$
(3) $\mathfrak{p} \cap \mathbb{Q} = p\mathbb{Z}$.

Theorem 15. $p\mathbb{Z}_K \cap \mathbb{Z} = p\mathbb{Z}$.

Proof. Exercise! □

Definition 50. If $\mathfrak{p}$ is a prime ideal and $p \cap \mathbb{Z} = p\mathbb{Z}$, then we say that $\mathfrak{p}$ is *above p*, or p is *below* $\mathfrak{p}$.

Theorem 16. *Let $\mathfrak{p}$ be a prime ideal above $\mathfrak{p}$. Then $\mathfrak{p} \supseteq p\mathbb{Z}_K$.*

Proof. We know that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, hence $p \in \mathfrak{p}$. This implies that (as $\mathfrak{p}$ is an ideal) that $p \cdot x \in \mathfrak{p}$ for all $x \in \mathbb{Z}_K$. Hence $p\mathbb{Z}_K \subseteq \mathfrak{p}$. □

Theorem 17. *Let p be prime. Then there exists a unique factorization*

$$p\mathbb{Z}_K = \prod \mathfrak{p}_i^{e_i}$$

with $\mathfrak{p}_i$ above p.

Proof. Note that $\mathrm{N}(p\mathbb{Z}_K) = p^{\deg(K)}$, since the Hermite normal form of $p\mathbb{Z}_K$ is

$$\begin{pmatrix} p & & & & 0 \\ & p & & & \\ & & p & & \\ & & & \ddots & \\ 0 & & & & p \end{pmatrix}.$$

Note that $\mathrm{N}(\mathfrak{p}_i) = p^{f_i}$ for some f_i. Further, norms are multiplicative. Therefore $p^{\deg(K)} = \mathrm{N}(p\mathbb{Z}_K) = \mathrm{N}(\prod \mathfrak{p}_i^{e_i}) = \prod p^{e_i f_i}$. Therefore, it follows that $\deg(K) = e_1 f_1 + \cdots + e_j f_j$. □

Let I be an ideal. We know it has a unique factorization $I = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$ into prime ideals. We want to find this factorization, First we look at $\mathrm{N}(I) = p_1^{a_1} \cdots p_s^{a_s}$ for primes p_i. If we can factor $p\mathbb{Z}_K = \prod \mathfrak{p}_i^{e_i}$ for some $p \mid \mathrm{N}(I)$, then we can quickly check if $\mathfrak{p}_i \supseteq I$ or $\mathfrak{p}_i^t \supseteq I$ for some t. So the big question is how we factor $p\mathbb{Z}_K$.

Definition 51. Recall

$$p\mathbb{Z}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i} \text{ and } \mathrm{N}(\mathfrak{p}_i) = p^{f_i}.$$

Then

(1) If $e_i = f_i$ and $g = \deg(K)$ then we say $p\mathbb{Z}_K$ *splits completely.*
(2) If $e_1 = 1, g = 1$ then $p\mathbb{Z}_K$ is *inert.*
(3) If $e_i \geq 2$ for any e_i then we say that $p\mathbb{Z}_K$ is *ramified.*
(4) If $e_i = 1$ for all i, then $p\mathbb{Z}_K$ is *unramified.*

Theorem 18. *A prime p is ramified if and only if $p \,|\, \mathrm{disc}(K)$.*

Corollary 6. *For any fixed K there are only finitely many ramified primes.*

17. February 26

Example. Let $K = \mathbb{Q}(i)$. Then $\mathbb{Z}_K = \mathbb{Z}[i]$. We see that $2\mathbb{Z}_K$ is not prime by observing that $(1+i) \in \mathbb{Z}_K/2\mathbb{Z}_K$ but $(1+i)^2 = 0$. We can verify that $2\mathbb{Z}_K = (\underbrace{(1+i)\mathbb{Z}_K}_{=:\mathfrak{p}})^2 = \mathfrak{p}^2$.

Consider $3\mathbb{Z}_K$. Let $a + bi \in \mathbb{Z}_K/3\mathbb{Z}_K$ and $a, b \in \mathbb{F}_3$. Assume that $(a+bi)(c+di) = 0$ in $\mathbb{Z}_K/3\mathbb{Z}_K$. Thus we have $ac - bd = 0$ and $ad + bc = 0$. Thus $ac = bd$ and $ad = -bc$, so $a^2cd = -b^2cd$. If both c and d are non-zero then $a = b = 0$. Or $-abc^2 = abd^2$, so $c = d = 0$. Thus $\mathbb{Z}_K/3\mathbb{Z}_K$ is an integral domain so $3\mathbb{Z}_K$ is a prime ideal and is inert. Lastly, $5\mathbb{Z}_K$ splits, namely $5\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1 = (1+2i)\mathbb{Z}_K$ and $\mathfrak{p}_2 = (1+3i)\mathbb{Z}_K$. We observe that these are not the same, since $1 + 2i \in \mathfrak{p}_1 \cap \mathfrak{p}_2$ then there would exist $a + bi \in \mathbb{Z}_K$ such that $(1+3i)(a+bi) = 1+2i$. But since $a, b \notin \mathbb{Z}$, this "gives" a contradiction.

Thus $5\mathbb{Z}_K$ is not inert and is unramified. Further, it splits completely.

Theorem 19. *Let $K = \mathbb{Q}(\theta)$ be a number field, and θ an algebraic integer. Let $T(x)$ be the minimal polynomial of θ. Let $f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Assume that $p \nmid f$, and write*

$$T(x) = \prod T_i(x)^{e_i} \pmod{p}.$$

Let $\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta)\mathbb{Z}_K$. Then $p\mathbb{Z}_K = \prod \mathfrak{p}_i^{e_i}$ is the unique prime factorization of $p\mathbb{Z}_K$.

Example. Let $K = \mathbb{Q}(\sqrt{3})$ and $\mathbb{Z}_K = \mathbb{Z}[\sqrt{3}]$. Thus $f = [\mathbb{Z}_K : \mathbb{Z}[\sqrt{3}]] = 1$. Note that

$$\begin{aligned} x^2 - 3 &\equiv (x+1)^2 \pmod 2 \\ &\equiv x^2 \pmod 3 \\ &\equiv x^2 - 3 \pmod 7 \\ &\equiv (x-5)(x-6) \pmod{11}. \end{aligned}$$

So $2\mathbb{Z}_K, 3\mathbb{Z}_K$ are ramified; $7\mathbb{Z}_K$ is inert; and $11\mathbb{Z}_K$ splits completely.

For the mod 2 case, note $2\mathbb{Z}_K = \mathfrak{p}^2$ where $\mathfrak{p} := 2\mathbb{Z}_K + (1+\sqrt{3})\mathbb{Z}_K$. This has a basis

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 1 & 1 \\ 3 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix},$$

so $\mathfrak{p} = \{(1+\sqrt{3})a + 2\sqrt{3}b\}$.

For the mod 7 case, since $7\mathbb{Z}_K$ is inert, $7\mathbb{Z}_K = \mathfrak{p} = 7\mathbb{Z}_K + (\sqrt{3}^2 - 3)\mathbb{Z}_K = \{7a + 7b\sqrt{3} : a, b \in \mathbb{Z}\}$.

For the mod 11 case, we can write $11\mathbb{Z}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$. Then $\mathfrak{p}_1 = 11\mathbb{Z}_K + (\sqrt{3} - 5)\mathbb{Z}_K = \{(1+2\sqrt{3})a + 11\sqrt{3}b : a, b \in \mathbb{Z}\}$ and $\mathfrak{p}_2 = \{(1+9\sqrt{3})a + 11\sqrt{3}b : a, b \in \mathbb{Z}\}$.

Lemma 7. *Let $f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$, and $p \nmid f$. Construct the T_i and $\mathfrak{p}_i$ as before. Then either $\mathfrak{p}_i = \mathbb{Z}_K$ or $\mathbb{Z}_k/\mathfrak{p}_i$ is a field of size $p^{\deg(T_i)}$.*

Proof. Set $K_i \cong \mathbb{F}_p[x]/\langle T_i(x)\rangle \cong \mathbb{Z}[x]/\langle p, T_i(x)\rangle$. We see that $T_i(x)$ is irreducible in $\mathbb{F}_p[x]$. Thus K_i is a field of size $p^{\deg(T_i)}$. We wish to show that either $\mathfrak{p}_i = \mathbb{Z}_K$ or $\mathbb{Z}_K/\mathfrak{p}_i \cong K_i$. Consider a homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_k/\mathfrak{p}$ by $\varphi(A(x)) = A(\theta) \bmod \mathfrak{p}$.

We see that $\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta)\mathbb{Z}_K$. This gives us that $p \in \ker\varphi$. Similarly, $T_i(x) \in \ker\varphi$. As $\langle p, T_i(x)\rangle$ is a maximal ideal of $\mathbb{Z}[x]$ (since $\mathbb{Z}[x]/\langle p, T_i(x)\rangle$ is a field), this tells us that $\ker\varphi = \mathbb{Z}[x]$ or $\ker\varphi = \langle p, T_i(x)\rangle$.

If $\mathbb{Z}[\theta] = \mathbb{Z}_K$ we would be done since $\varphi(\mathbb{Z}[x]) = \mathbb{Z}[x]/\ker\varphi$. The problem is that we might have $\mathbb{Z}[\theta] \neq \mathbb{Z}_K$. This doesn't matter that much though; as long as we can show that the map is surjective we would be done. Thus we need to show that this map is onto. That is, for all $b \in \mathbb{Z}_k/\mathfrak{p}$, there exists an $A(x) \in \mathbb{Z}[x]$ such that $\varphi(A(x)) = b$. Therefore there exist $c, d \in \mathbb{Z}_K$ such that $A(\theta) = b + pc + T_i(\theta)d$. Hence, $b = A(\theta) - pc - T_i(\theta)d$ so $Z_K = Z[\theta] + \mathfrak{p}_i$. Note that $p\mathbb{Z}_K \subseteq p\mathbb{Z}_K + T_i(\theta)\mathbb{Z}_K = \mathfrak{p}_i$. Hence $\mathbb{Z}[\theta] + p\mathbb{Z}_K \subseteq \mathbb{Z}[\theta] + \mathfrak{p}_i$, so

$$[\mathbb{Z}_K : \mathbb{Z}[\theta] + \mathfrak{p}_i] \,|\, [\mathbb{Z}_K : \mathbb{Z}[\theta] + p\mathbb{Z}_K].$$

Look at the Hermite normal form of $\mathbb{Z}[\theta]$. Then $f = a_{11} \cdots a_{nn}$ and $p \nmid a_{ii}$ for all i.

$$\begin{pmatrix} a_{11} & & & (*) \\ & a_{22} & & \\ & & \ddots & \\ 0 & & & a_{nn} \end{pmatrix}$$

The Hermite normal form of $p\mathbb{Z}_K$ is pI_n. So the Hermite normal form of $\mathbb{Z}[\theta] + p\mathbb{Z}_K$ is

$$\begin{pmatrix} a_{11} & & & (*) \\ & a_{22} & & \\ & & \ddots & \\ 0 & & & a_{nn} \\ p & & & \\ & p & & \\ & & \ddots & \\ & & & p \end{pmatrix} \to \begin{pmatrix} b_{11} & & & (*) \\ & b_{22} & & \\ & & \ddots & \\ 0 & & & b_{nn} \end{pmatrix} = I_n$$

since $b_{11} = \gcd(a_{11}, p) = 1$ and $b_{ii} \mid \gcd(a_{ii}, p) = 1$. Therefore $\mathbb{Z}[\theta] + p\mathbb{Z}_K = \mathbb{Z}_K$. Hence $\mathfrak{p} + \mathbb{Z}[\theta] \supseteq p\mathbb{Z}_K + \mathbb{Z}[\theta] = \mathbb{Z}_K$. Thus φ is a surjective map as desired. This gives us the desired conclusion. □

Theorem 20. *Let $\mathfrak{p}_i$ and $\mathfrak{p}_j$ be as before and $i \neq j$. Then $\mathfrak{p}_i + \mathfrak{p}_j = \mathbb{Z}_K$.*

Proof. We have $\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta)\mathbb{Z}_K$. We know that $T_i(x)$ and $T_j(x)$ are irreducible, distinct, (coprime) factors in $\mathbb{F}_p[x]$. Since $\gcd(T_i(x), T_j(x)) = 1$ in $\mathbb{F}_p[x]$, there exist $U(x)$ and $V(x)$ so that $T_i(x)U(x) + T_j(x)V(x) \equiv 1 \pmod{p}$, or $T_iU + T_jV = 1 + p \cdot W(x)$. Therefore $\underbrace{T_i(\theta)U(\theta)}_{\in T_i(\theta)\mathbb{Z}_K} - \underbrace{pW(\theta)}_{\in p\mathbb{Z}_K} + \underbrace{T_j(\theta)V(\theta)}_{\in T_j(\theta)\mathbb{Z}_K} = 1$. So $T_i(\theta)U(\theta) - pW(\theta) \in \mathfrak{p}_i$ and $T_j(\theta)V(\theta) \in \mathfrak{p}_j$. Thus $1 \in \mathfrak{p}_i + \mathfrak{p}_j$, as required. □

18. March 2

Example. Let $K = \mathbb{Q}(\sqrt{3})$. We know that $11\mathbb{Z}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$, where

$$\mathfrak{p}_1 = \{(1 + 2\sqrt{3})a + 11\sqrt{3}b : a, b \in \mathbb{Z}\}$$
$$\mathfrak{p}_2 = \{(1 + 9\sqrt{3})a + 11\sqrt{3}b : a, b \in \mathbb{Z}\}.$$

$\mathfrak{p}_1 + \mathfrak{p}_2$ has the following Hermite normal form:

$$\begin{pmatrix} 1 & 2 \\ 0 & 11 \\ 1 & 9 \\ 0 & 11 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 0 & 11 \\ 0 & 7 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Thus, $\mathfrak{p}_1 + \mathfrak{p}_2 = \mathbb{Z}_K$.

Lemma 8. $p\mathbb{Z}_K \supseteq \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g}$.

Proof. Note $\mathfrak{p}_1^{e_1} = (p\mathbb{Z}_K + T_1(\theta)\mathbb{Z}_K)^{e_1} = p^{e_1}\mathbb{Z}_K^{e_1}\binom{e_1}{1}p^{e_1-1}T_1(\theta)\mathbb{Z}_K^{e_1} + \cdots + T_1(\theta)^{e_1}\mathbb{Z}_K^{e_1}$. Note that $\mathbb{Z}_K^{e_1} \subseteq \mathbb{Z}_K$ and $1 \in \mathbb{Z}_K$, so $\mathbb{Z}_K^{e_1} = \mathbb{Z}_K$. This simplifies to

$$\underbrace{p\left(p^{e_1-1}\mathbb{Z}_K\binom{e_1}{1}p^{e_1-1}T_1(\theta)\mathbb{Z}_K + \cdots + \binom{e_1}{1}T_1(\theta)^{e_1-1}\mathbb{Z}_K\right)}_{\subseteq \mathbb{Z}_K} + T_1(\theta)^{e_1}\mathbb{Z}_K \subseteq p\mathbb{Z}_K + T_1(\theta)^{e_1}\mathbb{Z}_K.$$

Thus

$$\begin{aligned}\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} &\subseteq (p\mathbb{Z}_K + T_1(\theta)^{e_1}\mathbb{Z}_K)(p\mathbb{Z}_K + T_2(\theta)^{e_2}\mathbb{Z}_K)\\ &\subseteq p^2\mathbb{Z}_K + p(T_1(\theta)^{e_1}\mathbb{Z}_K + T_2(\theta)^{e_2}\mathbb{Z}_K) + T_1(\theta)^{e_1}T_2(\theta)^{e_2}\mathbb{Z}_K.\end{aligned}$$

As before, the middle term simplifies to $\mathbb{Z}_K$ so this is $\subseteq p^2\mathbb{Z}_K + p\mathbb{Z}_K + T_1(\theta)^{e_1}T_2(\theta)^{e_2}\mathbb{Z}_K$. Therefore,

$$\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \subseteq p\mathbb{Z}_K + T_1(\theta)^{e_1}T_2(\theta)^{e_2}\mathbb{Z}_K.$$

The full product works the same way. That is,

$$\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g} \subseteq p\mathbb{Z}_K + T_1(\theta)^{e_1}\cdots T_g(\theta)^{e_g}\mathbb{Z}_K.$$

Notice $T(x) = T_1(x)^{e-1}\cdots T_g(x)^{e_g} \pmod{p}$, so $T(\theta) = T_1(\theta)^{e_1}\cdots T_g(\theta)^{e_g} \pmod{p}$. Yet $T(\theta) = 0$, so $T_1^{e_1}(\theta)\cdots T_g(x)^{e_g} = pk$ for some k. Therefore $\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g} \subseteq p\mathbb{Z}_K + pk\mathbb{Z}_K = p\mathbb{Z}_K$. □

Theorem 21. $p\mathbb{Z}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$.

Proof. Now that we proved $p\mathbb{Z}_K \supseteq \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$, we show this time that it has a prime factorization $p\mathbb{Z}_K = \mathfrak{p}_1^{d_1}\cdots\mathfrak{p}_g^{d_g}$. Reorder these so that $\mathfrak{p}_1,\ldots,\mathfrak{p}_s$ are prime ideals, and $\mathfrak{p}_{s+1},\ldots,\mathfrak{p}_g$ are $\mathbb{Z}_K$. Note as $p\mathbb{Z}_K \supseteq \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$ we see that $\mathfrak{p}_1^{d_1}\cdots\mathfrak{p}_g^{d_g} \supseteq \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$, Hence there are no extra prime factors on the LHS. Morevore $d_1 \le e_1, d_2 \le e_2$; in fact, we have $d_i \le e_i$ for $i = 1, 2, \ldots, s$.

Note that $\mathrm{N}(p\mathbb{Z}_K) = \mathrm{N}(\mathfrak{p}_1^{d_1}\cdots\mathfrak{p}_s^{d_s}) = p^{\deg(K)} = \prod \mathrm{N}(\mathfrak{p}_i^{d_i}) = \prod p^{d_i f_i} = p^{\sum d_i f_i}$, where $\mathrm{N}(\mathfrak{p}_i) = p^{f_i}$. This gives $\deg K = \sum d_i f_i$.

Notices that $\mathrm{N}(\mathfrak{p}_i) = p^{\deg(T_i)}$. Therefore $\mathrm{N}(\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}) = p^{\deg(T_1(x)^{e_1}\cdots T_s(x)^{e_s})} = p^A$, where $A \le \deg(T(x)) = \deg(K)$. As $e_i \ge d_i$, this only works if $s = g$ and $d_i = d_i$. Hence $p\mathbb{Z}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$, and $T(x) = T_1(x)^{e_1}\cdots T_g(x)^{e_g} \pmod{p}$ as desired. □

Remark. A key assumption in the first lemma (and hence the main theorem) was that $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$. In some cases we can work around this problem by finding a different θ_2 such that $\mathbb{Q}(\theta) = \mathbb{Q}(\theta_2)$.

Definition 52. Suppose that K is a number field where, regardless of the choices of θ, we always have $p \mid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Such primes are called *inessential discriminant divisors.* It is knows that such p have $p \le \deg(K) - 1$.

Remark. If p is an inessential discriminant divisor, then new/harder methods are necessary.

Example. Let $K = \mathbb{Q}(i)$ so that $\mathbb{Z}_K = \mathbb{Z}[i]$. Let $I = \{(32+6i)a + (13+19i)b : a, b \in \mathbb{Z}\}$. Here I has Hermite normal form

$$\begin{pmatrix} 32 & 6 \\ 13 & 19 \end{pmatrix} \to \begin{pmatrix} 6 & -32 \\ 13 & 19 \end{pmatrix} \to \begin{pmatrix} 6 & -32 \\ 1 & 83 \end{pmatrix} \to \begin{pmatrix} 1 & 83 \\ 0 & 530 \end{pmatrix}.$$

This is an ideal if any $(a+bi) \in \mathbb{Z}[i]$ has $(a+bi)(c+di) \in I$ with $c + di \in I$. Equivalently if $\mathbb{Z}_K \cdot I + I = I$ then $\mathbb{Z}_K \cdot I + I$ has the same Hermite normal form as I. So I is an ideal. Note that $\mathrm{N}(I) = 2 \cdot 5 \cdots 53$, and that $x^2 + 1 = (x+1)^2 \bmod 2$, $x^2 + 1 = (x+2)(x+3) \bmod 5$, and that $x^2 + 1 = (x+23)(x+30) \bmod 53$. Thus $2\mathbb{Z}_K = \mathfrak{p}_2^2$ where $\mathfrak{p}_2 = 2\mathbb{Z}_K + (1+i)\mathbb{Z}_K$. So we know that $\mathfrak{p}_2$ is a factor of I. On the other hand, $5\mathbb{Z}_K = \mathfrak{p}_{5,a} \cdot \mathfrak{p}_{5,b}$, where $\mathfrak{p}_{5,a} = 5\mathbb{Z}_K + (i+2)\mathbb{Z}_K$ and $\mathfrak{p}_{5,b} = 5\mathbb{Z}_K + (i+3)\mathbb{Z}_K$. Note that $\mathfrak{p}_{5,b}$ has the Hermite normal form

$$\begin{pmatrix} 5 & 0 \\ 0 & 5 \\ 3 & 1 \\ -1 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & -3 \\ 0 & 5 \\ 5 & 0 \\ 3 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 0 & 5 \\ 0 & 15 \\ 0 & 10 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 0 & 5 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

We see $\mathfrak{p}_{5,b}$ is a factor of I if $\mathfrak{p}_{5,b} + I = \mathfrak{p}_{5,b}$. Indeed,

$$\begin{pmatrix} 1 & 83 \\ 0 & 530 \\ 1 & 2 \\ 0 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 0 & 81 \\ 0 & 5 \\ 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

This tells us that $\mathfrak{p}_{5,b}$ is not a factor of I, so $\mathfrak{p}_{5,a}$ is a factor of I. We can do $\mathfrak{p}_{53}$ in the same way to get

$$I = \mathfrak{p}_2 \cdot \mathfrak{p}_{5,a} \cdot \mathfrak{p}_{53,a}$$

where $\mathfrak{p}_2 = 2\mathbb{Z}_K + (1+i)\mathbb{Z}_K, \mathfrak{p}_{5,a} = 5\mathbb{Z}_K + (2+i)\mathbb{Z}_K, \mathfrak{p}_{53,a} = 53\mathbb{Z}_K + (23+i)\mathbb{Z}_K$.

18.1. **Fractional ideals, ideal inversion, and the class group**

Definition 53. We say that I is a *fractional ideal* if there exists a d such that $d \cdot I$ is an ideal over $\mathbb{Z}_K$.

Remark. Note all the elements of I are algebraic integers. All will be algebraic numbers.

Example. Let $I = \frac{1}{2}\mathbb{Z}_K$. Note that $4 \cdot \frac{1}{2}\mathbb{Z}_K = 2\mathbb{Z}_K$ is an ideal of $\mathbb{Z}_K$. Note that $\frac{1}{2} \in I$, and $\frac{1}{2}$ is not an algebraic integer but is an algebraic number.

19. March 4

Definition 54. Let I be a fractional ideal. We say I is *invertible* if there exists a fractional ideal J such that $IJ = \mathbb{Z}_K$. In this case we say $I^{-1} = J$.

Example. Let $K = \mathbb{Q}(i)$. We know from before that $2\mathbb{Z}_K = \mathfrak{p}_2^2$, so $\mathfrak{p}_2^{-1} = \frac{1}{2}\mathfrak{p}_2$.

In general, if $p\mathbb{Z}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g}$, we have

$$\mathfrak{p}_i \left(\frac{1}{p} \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_{i-1}^{e_{i-1}} \mathfrak{p}_{i+1}^{e_{i+1}} \cdots \mathfrak{p}_g^{e_g} \right) = \mathbb{Z}_K,$$

so

$$\mathfrak{p}_i^{-1} = \frac{1}{p} \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_{i-1}^{e_{i-1}} \mathfrak{p}_{i+1}^{e_{i+1}} \cdots \mathfrak{p}_g^{e_g}.$$

Using this idea, we can show that

Corollary 7. *All fractional ideals in $\mathbb{Z}_K$ are invertible.*

Theorem 22. *Let I be any fractional ideal. Then there exists a* unique *factorization*

$$I = \prod \mathfrak{p}_i^{v_i}, v_i \in \mathbb{Z} \setminus \{0\} \, \forall i.$$

Definition 55. We say two fractional ideals I, J are *equivalent* if there exists $\alpha \in K$ such that $\alpha I = J$; or equivalently, if I and J are ideals then there exist $\alpha, \beta \in \mathbb{Z}_K$ such that $\alpha I = \beta J$. In this case we write $I \sim J$.

Remark. The relation $\sim$ has the following properties:

(1) $I \sim I$
(2) $I \sim J$ by $\alpha I = J$ implies $J \sim I$ by $\alpha^{-1} J = I$
(3) $I \sim J, J \sim K$ implies $I \sim K$ (transitivity)

Therefore, $\sim$ is a proper equivalence relation.

Observe that the product of any two fractional ideals is a fractional ideal. Moreover, $(IJ)K = I(JK)$ and $IJ = JI$. We see that $I \cdot \mathbb{Z}_K = I$; that is, $\mathbb{Z}_K =$ "1". This gives us that the set of fractional ideals is an *abelian group* under multiplication.

Definition 56. The class group of K is $\mathrm{Cl}(K)$. The *class number* is $h(K) = |\mathrm{Cl}(K)|$.

Example (a stupid one). Let $K = \mathbb{Q}$. Then $\mathbb{Z}_K = \mathbb{Z}$. All ideals are of the form $m\mathbb{Z}$ where $m \neq 0$. All the fractional ideals look like $\frac{m}{n}\mathbb{Z}$ with $m, n \neq 0$. All the fractional ideals satisfy $\frac{m}{n}\mathbb{Z} \sim \mathbb{Z}$. Therefore $\mathrm{Cl}(\mathbb{Q}) = \{1\}$.

Example. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $h(K) \geq 2$. It suffices to find an ideal I such that $I \not\sim \mathbb{Z}_K$. First, we start by factoring $3\mathbb{Z}_K$. Note that $x^2 + 5 \equiv (x+2)(x+1) \bmod 3$. Let $\mathfrak{p}_1 = 3\mathbb{Z}_K + (2 + \sqrt{-5})\mathbb{Z}_K$ and $\mathfrak{p}_2 = 3\mathbb{Z}_K + (1 + \sqrt{-5})\mathbb{Z}_K$. Then $3\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$. We claim now that $\mathfrak{p}_1 \not\sim \mathbb{Z}_K$. For this, we will compute the Hermite normal form of $\mathfrak{p}_1$:

$$\begin{pmatrix} 3 & 0 \\ 0 & 3 \\ 2 & -5 \\ 1 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 0 & 6 \\ 0 & 3 \\ 0 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}.$$

Hence $\mathfrak{p}_1 = \{(2 + \sqrt{-5})a + 3b : a, b \in \mathbb{Z}\}$. Assume that there exists α such that $\mathfrak{p}_1 = \alpha\mathbb{Z}_K$. Choose d such that $d\alpha \in \mathbb{Z}_K$ so $d\alpha = a + b\sqrt{-5} \in \mathbb{Z}_K$. We can assume that $\gcd(a, b, d) = 1$. We already know that $\mathrm{N}(\mathfrak{p}_1) = 3$. Therefore $\mathrm{N}(d\alpha\mathbb{Z}_K) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$. Thus

$$\mathrm{N}(\alpha\mathbb{Z}_K) = \frac{1}{d^2}\mathrm{N}(d\alpha\mathbb{Z}_K) = \frac{a^2 + 5b^2}{d^2} = 3 = \mathrm{N}(\mathfrak{p}_1)$$
$$\Rightarrow a^2 + 5b^2 = 3d^2 \ (a, b, d \in \mathbb{Z})$$

Upon reducing $a^2 + 5b^2 = 3d^2$ mod 5, we see that $a \equiv d \equiv 0 \pmod 5$. Upon reducing the same equation mod 25, we see that $b \equiv 0 \pmod 5$ since we know $a \equiv d \equiv 0 \pmod 5$. This contradicts the assumption that $\gcd(a, b, d) = 1$. Hence $\mathfrak{p}_1 \not\sim \mathbb{Z}_K$ so $h(k) \geq 2$. The fact that $h(\mathbb{Q}(\sqrt{-5})) \geq 2$ has implications for factorization over $\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}$.

Consider the factorization $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. If we could write $3 = \alpha\beta$ over $\mathbb{Z}_K$, then $3\mathbb{Z}_K = (\alpha\mathbb{Z}_K)(\beta\mathbb{Z}_K)$. But $3\mathbb{Z}_K$ factors into $\mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1, \mathfrak{p}_2 \not\sim \mathbb{Z}_K$. Therefore 3 does not factor further.

Proposition 57. *$\mathbb{Z}_K$ is a unique factorization domain (UFD) if and only if $h(K) = 1$.*

We now wish to prove that $h(K)$ is finite; that is, $\mathrm{Cl}(K)$ is a *finite* abelian group.

Lemma 9. *Let K be a number field. Then there exists $\lambda > 0$ (dependent on K) such that for any ideal I there exists $\alpha \in I$ satisfying $|\mathrm{N}_K(\alpha)| \leq \lambda\,\mathrm{N}(I)$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be a basis for $\mathbb{Z}_K$ and $\sigma_1, \dots, \sigma_n$ the n field embeddings. Let

$$\lambda = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|.$$

Pick the unique m such that

$$m^n \le \mathrm{N}(I) < (m+1)^n.$$

Consider the $(m+1)^n$ elements

$$\left\{ \sum_{i=1}^{n} a_i \alpha_i : 0 \le a_i < m \right\}.$$

Looking at the images of these in $\mathbb{Z}_K/I$ gives a_i, a_i' such taht $\sum a_i\alpha_i - \sum a_i'\alpha_i \in I$. This can be written as $\sum b_i\alpha_i$ with $|b_i| \le m$. Let $\alpha = \sum b_i \alpha_i$. We claim that $|\mathrm{N}(\alpha)| \le \lambda \mathrm{N}(I)$. Indeed, we have

$$\begin{aligned} \mathrm{N}(\alpha) &= \left| \mathrm{N}\left(\sum_i b_i \alpha_i \right) \right| \\ &= \left| \prod_{j=1}^{n} \sigma_i \left(\sum_i b_i \alpha_i \right) \right| \\ &= \left| \prod_{j=1}^{n} \sum_{i=1}^{n} b_i \sigma_j(\alpha_i) \right| \le \prod_{j=1}^{n} \sum_{i=1}^{n} |b_i \sigma_j(\alpha_i)| \\ &\le \prod_{j=1}^{n} \sum_{i=1}^{n} m \cdot |\sigma_j(\alpha_i)| = m^n \prod_{j=1}^{n} \sum_{i=1}^{n} |\sigma_j(\alpha_i)| \le \lambda \cdot \mathrm{N}(I), \end{aligned}$$

as required. □

Lemma 10. *With $\lambda > 0$ as above, every equivalence class has an ideal J such that* $\mathrm{N}(J) \le \lambda$.

Proof. Let $\mathcal{C}$ be an equivalence class of ideals. Note that $\mathcal{C}^{-1} = \{I^{-1} : I \in \mathcal{C}\}$ is an equivalence class of ideals. Pick $I \in \mathcal{C}^{-1}$ an ideal, and find $\alpha \in I$ such that $\mathrm{N}(\alpha) \le \lambda \mathrm{N}(I)$. Notice $\alpha\mathbb{Z}_K \subseteq I$. So there exists J such that $\alpha\mathbb{Z}_K = IJ$. Note that $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$ and $\mathrm{N}(\alpha\mathbb{Z}_K) = \mathrm{N}(\alpha) \le \lambda \mathrm{N}(I)$. From these two inequalities, it follows that $\mathrm{N}(J) \le \lambda$ as required. □

There are only finitely many ideals J with $\mathrm{N}(J) \le \lambda$, which we can deduce upon looking at the Hermite normal form. As each equivalence class has one of these ideals, there are only finitely many equivalence class; therefore $h(K)$ is finite.

Corollary 8. $\mathrm{Cl}(K)$ *is finite.*

20. March 9 & 11

20.1. Quadratic number fields

Let θ be a root of $ax^2 + bx + c$, i.e., $\theta = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$. Notice that

$$\mathbb{Q}\left(\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \right) = \mathbb{Q}(\sqrt{b^2 - 4ac}).$$

We may assume without loss of generality that $K = \mathbb{Q}(\sqrt{d})$ where d is squarefree and $d \neq 0, 1$.

Proposition 58. *Let $K = \mathbb{Q}(\sqrt{d})$ with d squarefree and $d \neq 0, 1$. Then*

(1) If $d \equiv 1 \pmod 4$, then $\mathbb{Z}_K = \left\{a + b\left(\frac{1+\sqrt{d}}{2}\right) : a, b \in \mathbb{Z}\right\}$.

(2) If $d \equiv 2, 3 \pmod 4$, then $\mathbb{Z}_K = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$.

Proof. Assume $d \equiv 1 \pmod 4$ and $a + b\sqrt{d} \in \mathbb{Z}_K$ with $a, b \in \mathbb{Q}$. The minimal polynomial of $a + b\sqrt{d}$ is $x^2 - 2ax + (a^2 - db^2)$. We see that $2a, a^2 - db^2 \in \mathbb{Z}$. This gives us that $a = m \in \mathbb{Z}$ or $a = \frac{2m+1}{2}, m \in \mathbb{Z}$. If $a = m$, then $m^2 - db^2 \in \mathbb{Z}$. Since d is squarefree, it follows that $b \in \mathbb{Z}$. If $a = \frac{2m+1}{2}$, then

$$\left(\frac{2m+1}{2}\right)^2 - db^2 \in \mathbb{Z}.$$

Hence $4m^2 + 4m + 1 - 4db^2 \in 4\mathbb{Z}$. Hence $1 - 4db^2 \in 4\mathbb{Z}$. Thus $b = \frac{2n+1}{2}$ for some $n \in \mathbb{Z}$. Thus either $a, b \in \mathbb{Z}$ or $a = \frac{2m+1}{2}, b = \frac{2n+1}{2}, n, m \in \mathbb{Z}$. Therefore

$$\mathbb{Z}_K = \mathbb{Z} + \left(\frac{1+\sqrt{d}}{2}\right)\mathbb{Z}.$$

The other case is similar but easier. □

20.2. **Discriminants**

Let d be squarefree and $d \neq 0, 1$. If $d \equiv 1 \pmod 4$, then

$$\operatorname{disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} \det \begin{bmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{bmatrix}^2 = d & (d \equiv 1 \pmod 4) \\ \det \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix}^2 = 4d & (d \not\equiv 1 \pmod 4) \end{cases}$$

Corollary 9 (Stickelberger's theorem)**.** *If K is a quadratic number field, then* $\operatorname{disc}(K) \equiv 0$ *or* 1 *mod* 4.

Definition 59. We say that

$$D = \operatorname{disc}(K) = \begin{cases} 4d & d \equiv 1 \pmod 4 \\ d & d \not\equiv 1 \pmod 4. \end{cases}$$

is the *fundamental discriminant* of K.

Let

$$\tau_D = \begin{cases} \frac{1+\sqrt{D}}{2} = \frac{1+\sqrt{d}}{2} & (d \equiv 1 \pmod 4) \\ \frac{\sqrt{D}}{2} = \sqrt{d} & (d \not\equiv 1 \pmod 4). \end{cases}$$

That is $\mathbb{Z}_K = \{a + b\tau_D : a, b \in \mathbb{Z}\}$.

Lemma 11. *Let I be an ideal in $\mathbb{Z}_K$. Then there exist $a, g, b \in \mathbb{Z}$ such that*

$$I = \{g(ax + (b + \tau_D)y) : x, y \in \mathbb{Z}\}.$$

Proof. Let I be an ideal. Write this in the Hermite normal form with respect to the basis $\{\tau_D, 1\}$: We know that I is an ideal and $C \in I$, where the Hermite normal form looks like

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}.$$

As I is an ideal, $C \cdot \tau_D \in I$. This gives us that $A \,|\, C$, as $C\tau_D = (a\tau_D + B)x + y$ for some $x, y \in \mathbb{Z}$ and we isolate the τ_D term. Further $A\tau_D + B \in I$ so $(A\tau_D + B)\tau_D \in I$. Note that

$$\tau_D^2 = \begin{cases} \left(\frac{1+\sqrt{D}}{2}\right)^2 = \frac{1+d}{4} + \frac{\sqrt{d}}{2} = \frac{d-1}{4} + \tau_D & (d \equiv 1 \pmod 4) \\ \sqrt{d}^2 = d & (d \not\equiv 1 \pmod 4). \end{cases}$$

Hence

$$(A\tau_D + B)\tau_D = \begin{cases} B\tau_D + A\tau_D + \frac{d-1}{4}A & (d \equiv 1 \pmod 4) \\ B\tau_D + Ad & (d \not\equiv 1 \pmod 4). \end{cases}$$

In both cases, this implies that $A \,|\, B$. So let $g = A, ga = C, gb = B$. So

$$\begin{aligned} I &= \{(A\tau_D + B)x + Cy : x, y \in \mathbb{Z}\} \\ &= \{g((\tau_D + B)x + Ay) : x, y \in \mathbb{Z}\} \\ &= \{g(Ax + (b + \tau_D)y) : x, y \in \mathbb{Z}\}. \end{aligned}$$ □

Ideals have a nicer form than one might originally expect. Recall that the fractional ideals I and J satisfy $I \sim J$ if there exists an $\alpha \in K$ such that $I = \alpha J$. Equivalently, two ideals are $I \sim J$ if there exist $\alpha, \beta \in \mathbb{Z}_K$ such that $\alpha I = \beta J$. There is a relationship between ideals, and equivalent classes of ideals, and something called a binary quadratic form, and equivalent classes of binary quadratic forms. Hence, to compute a class number it suffices to count the number of equivalent classes of binary quadratic forms.

20.3. **Binary quadratic forms (with a negative discriminant)**

Definition 60. We say $(a, b, c) = ax^2 + bxy + cy^2$ is a binary quadratic form with disc $b^2 - 4ac$.

Example. Consider $\{x^2 + y^2 : x, y \in \mathbb{Z}\} = \{0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, \dots\}$, the numbers representable by $(1, 0, 1)$. It is not hard to see that $\{(x + y)^2 + y^2 : x, y \in \mathbb{Z}\}$ represents the same list of numbers. Note that $(x + y)^2 + y^2 = x^2 + 2xy + 2y^2 = (1, 2, 2)$.

In general, we have

$$a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2$$

with $\alpha\delta - \gamma\beta = 1$ represents the same list of numbers. We will say that two binary quadratic forms related in this way are equivalent.

Definition 61. We will say that a binary quadratic form is *reduced* if $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

Proposition 62. *Every binary quadratic form with negative discriminant is equivalent to a* unique *reduced binary quadratic form.*

Proof (Part 1: Existence). A binary quadratic form is equivalent to a reduced binary quadratic form. If $a > c$ then $(a, b, c) \sim (c, -b, a)$ by $x_{\text{new}} = y$ and $y_{\text{new}} = -x$. Then $ay^2 + b(y)(-x) + c(-x)^2 = cx^2 - bxy + ay^2$. If $b \notin (-a, a]$ pick a k such that $b + 2ak \in (-a, a]$. We have $(a, b, c) \sim (a, b + 2ak, c + bk + ak^2)$. Use $x_{\text{new}} = x + ky, y_{\text{new}} = y$ and note that $a(x + ky)^2 + b(x + ky)y + cy^2$ is of desired form. We apply these two steps until neither conditions hold (that is, when $a \leq c, b \in (-a, a]$). If $a < c$ we are done. If $a = c$ use $(a, b, a) \sim (a, -b, a)$ if necessary so that $0 \leq b \leq a$. Note that this algorithm will terminate only if we are in the reduced form. We see that the first term must decrease every two steps, and must remain a positive integer. Therefore this algorithm will terminate. □

Proof (Part 2: Uniqueness). We now wish to show that (a, b, c) is equivalent to a *unique* binary quadratic form. Assume that (a, b, c) and (d, e, f) are two reduced, equivalent binary quadratic form. Assume also without loss of generality that $d \leq a$. Note that two equivalent binary quadratic forms represent the same set of integers, i.e., $\{ax^2 + bxy + cy^2 : x, y \in \mathbb{Z}\} = \{dx^2 + exy + fy^2 : x, y \in \mathbb{Z}\}$. Clearly $d \in \{dx^2 + exy + fy^2 : x, y \in \mathbb{Z}\}$. So there exist $x_0, y_0 \in \mathbb{Z}$ such that $d = ax_0^2 + bx_0y_0 + cy_0^2 \geq a(x_0^2 + y_0^2) + bx_0y_0 \geq a(x_0^2 + y_0^2) - a|x_0y_0| \geq a_0|x_0y_0|$. Therefore $a \geq d \geq a|x_0y_0|$. This implies that $x_0 = 0$ or $y_0 = 0$ or $|x_0y_0| = 1$ (the last condition implies that $a = d$). If $y_0 = 0$ then $d = ax_0^2 \geq dx_0^2$ so $a = d$. If $x_0 = 0$ then $d \geq cy_0^2 \geq ay_0^2 \geq dy_0^2$ so $a = d$. Therefore $a = d$.

Recall that there exist $\alpha, \beta, \gamma, \delta$ with $\alpha\delta - \beta\gamma = 1$ such that

$$a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2 = dx^2 + exy + fy^2 = ax^2 + exy + fy^2.$$

By looking at the x^2 term we have $ax^2 + a\alpha^2x^2 + b\alpha\gamma x^2 + c\gamma^2x^2$ or $a = a\alpha^2 + b\alpha\gamma + c\gamma^2 \geq a|\alpha\gamma|$. As before, we get restriction $\gamma = 0, \alpha = 0$, or $|\alpha\gamma| = 1$.

First, suppose $\gamma = 0$. As $a = a\alpha^2$, it follows that $\alpha^2 = 1$. As $\alpha\delta - \beta\gamma = 1$ we have $\alpha = \delta$ and $\delta^2 = 1$. Matching the xy term gives $e = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = 2a\alpha\beta + b$. Note that $-a < b \leq a$ and $-a < e \leq a$. This implies $\alpha\beta = 0$. We know $\alpha \neq 0$ so $\beta = 0$. Hence $\beta = \gamma = 0$ and $\alpha = \delta = \pm 1$. Using this transformation gives us $(a, b, c) = (d, e, f)$.

Second, assume $\alpha = 0$. As $a = c\gamma^2 \geq a\gamma^2$, this gives that $a = c$ and $\gamma^2 = 1$. We also have $\gamma\beta = -1$, since $\alpha\delta - \beta\gamma = 1$. As before, match up the xy term. Then we would have $e = 2\alpha\beta a + b\alpha\delta + b\gamma\beta + 2c\gamma\delta = -b + 2c\gamma\delta = -b + 2a\gamma\delta$. Notice that $-b \in [-a, 0]$, so $-b + 2a\gamma\delta \in [2a\gamma\delta - a, 2a\gamma\delta]$. So either $\gamma\delta = 1$ or $\gamma\delta = 0$. This is only in the correct range if $a = b = c$ and $\gamma\delta = 1$, or if $\gamma\delta = 0$. If $\gamma\delta = 0$ and $\gamma \neq 0$ then $\delta = 0$ and $\beta \neq 0, \alpha = 0$. Hence $\alpha = \delta = 0$ and $\beta = -\gamma = \pm 1$ so $(d, e, f) = (c, -b, a)$. But $a = c$ so $b \geq 0$; therefore $(a, b, c) = (d, e, f) = (a, 0, a)$, so the uniqueness is proven in this case.

Thus let $\gamma\delta \neq 0$, i.e., $\gamma\delta = 1, a = b = c, \gamma\beta = -1, \alpha = 0$. Then $a(\alpha x + \beta y)^2 + a(\alpha x + \beta y)(\gamma x + \delta y) + a(\gamma x + \delta y)^2$. If $\beta = 1$ then $ay^2 + a(y)(-x - y) + a(-x - y)^2 = ax^2 + axy + ay^2$.

Finally, suppose $|\alpha\delta| = 1$ and $a = c$. So $a = a\alpha^2 + b\alpha\gamma + c\gamma^2 = a + c \pm b = 2a \pm b$. This gives us $\alpha\gamma = -1$ and $b = a$. Note that $\alpha\delta - \beta\gamma = 1$, so $\alpha\gamma\delta - \beta\gamma^2 = \gamma$ hence $-\delta - \beta = \gamma$. Using these in $a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2$ give us

$$a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2 = ay^2 + axy + ay^2,$$

which concludes the proof. □

Corollary 10. *$(a, b, c) \sim (d, e, f)$ if and only if they are equivalent to the same reduced binary quadratic form.*

Recall that two binary quadratic forms are *equivalent* if there exist $\alpha, \beta, \gamma, \delta$ such that $\alpha\delta - \beta\gamma = 1$ such that

$$a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2 = dx^2 + exy + fy^2.$$

Recall also that we say a binary quadratic form is *reduced* if $0 < b \leq a < c$ or $0 \leq b \leq a = c$. Using $\alpha = \delta = 0$ and $\beta = -\gamma = 1$ gives $(a, b, c) \sim (c, -b, a)$. Using $\alpha = \delta = 1, \gamma = 0, \beta = k$ gives us $(a, b, c) \sim (a, b + 2ka, c + bk + ak^2)$.

Example. Consider a binary quadratic form $(7, -8, 3)$. We want to find its reduced form. $(7, -8, 3) \sim (3, 8, 7) \sim (3, 8 - 6, 7 - 8 + 3)$ by letting $k = -1$. Thus we see $(7, -8, 3) \sim (3, 2, 2) \sim (2, -2, 3) = (-2, -2 + 4, 3 + (-2) + 2)$, so $(7, -8, 3) \sim (2, 2, 3)$ which is a reduced form.

Example. How many binary quadratic forms of discriminant -23 are out there? That is, how many triples (a, b, c) are there satisfying $b^2 - 4ac = -23$? We may restrict our count to reduced binary quadratic forms. Notice that $23 = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$. Therefore $a^2 \leq \frac{23}{3}$. Hence $a \leq \sqrt{\frac{23}{3}}$. Hence $a = 1$ or 2. Also, notice that $c = \frac{23+b^2}{4a} \in \mathbb{Z}$. If $a = 1$, then $b = 1$ is the only possible choice. In this case $c = 6$. If $a = 2$ then b can only be $-1, 0$, or 1. If $b = \pm 1$ then $c = 3 \in \mathbb{Z}$. If $b = 0$ or $b = 2$, then $c \notin \mathbb{Z}$. So there are three reduced binary quadratic forms $((1, 1, 6), (2, -1, 3), (2, 1, 3))$. This means (and we will show later) that the class number of $\mathbb{Q}(\sqrt{-23})$ is 3. Hence $\mathrm{Cl}(\mathbb{Q}(\sqrt{-23})) \cong \mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

We now wish to show the connection between binary quadratic forms of discriminant D, and ideals in K with discriminant D. As before let $K = \mathbb{Q}(\sqrt{d}), d < 0$ and squarefree. Then

$$\operatorname{disc}(K) = \begin{cases} d & (d \equiv 1 \pmod 4) \\ 4d & (d \not\equiv 1 \pmod 4) \end{cases}$$

and

$$\tau_D = \begin{cases} \frac{1+\sqrt{D}}{2} & (d \equiv 1 \pmod 4) \\ \frac{\sqrt{D}}{2} & (d \not\equiv 1 \pmod 4). \end{cases}$$

I is of the form $I = \{g(ax + (b + \tau_D)y)\}$. As $I \sim \frac{2}{g} I$ we can assume I is of the form

$$I = \{2ax + (2B + 2\tau_D)y\} = \begin{cases} \{2ax + (2B + 1 + \sqrt{D})y\} & (d \equiv 1 \pmod 4) \\ \{2ax + (2B + \sqrt{D})y\} & (d \not\equiv 1 \pmod 4). \end{cases}$$

Let $b = 2B$ or $2B + 1$.

21. March 16 & 18

Consider the map from an ideal of this form to a binary quadratic form by

$$\begin{aligned} \{2ax + (b + \sqrt{D})y\} \mapsto & (2ax + (b + \sqrt{D})y)(2ax + (b - \sqrt{D})y)/(4a) \\ & = (4a^2x^2 + 4abxy + (b^2 - D)y^2)/(4a). \end{aligned}$$

We claim that $4a \,|\, b^2 - D$, say $4ac = b^2 - D$. To see this, note that $(B + \tau_D')(b + \sqrt{D}) \in I$ where $\tau_D' = -\frac{\sqrt{D}}{2}$ or $\tau_D' = \frac{-\sqrt{D}+1}{2}$ as appropriate. Then $(B + \tau_D')(b + \sqrt{D}) = \frac{1}{2}(b - \sqrt{D})(b + \sqrt{D}) =$

$\frac{b^2-D}{2} \in I$. This gives that $2a \,\Big|\, \frac{b^2-D}{2}$, or $4a \,|\, b^2 - D$ as required. Letting $c = \frac{b^2-D}{4a}$ to argue that $(4a^2x^2 + 4abxy + 4acy^2)/(4a) = ax^2 + bxy + cy^2$.

We need to show that the maps going between equivalent binary quadratic forms (BQF's) correspond to maps between equivalent ideals. Consider the map $(a, b, c) \sim (a, b + 2ak, c + bk + ak^2)$. Consider the ideal $\{2ax + (b + \sqrt{D})y : x, y \in \mathbb{Z}\}$. Note

$$\{2ax + (b + \sqrt{D})y\} = \{2a(x + ky) + (b + \sqrt{D})y\} = \{2ax + (b + 2ak + \sqrt{D})y\},$$

which maps to $(a, b + 2ak, c + bk + ak^2)$. Now consider the relation $(a, b, c) \sim (c, -b, a)$.

$$\begin{aligned}
\{2ax + (b + \sqrt{D})y\} &\sim (b - \sqrt{D})\{2ax + (b + \sqrt{D})y\} \\
&= \{2abx - 2ax\sqrt{D} + (b^2 - D)y\} \\
&= \{2abx - 2ax\sqrt{D} + (b^2 - D)y\} \\
&= \{2abx - 2ax\sqrt{D} + 4acy\} \\
&= 2a\{bx - \sqrt{D} + 2cy\} \\
&= 2a\{2cx + (-b + \sqrt{D})y\}.
\end{aligned}$$

but $\{2cx + (-b + \sqrt{D})y\}$ maps to $(c, -b, a)$ as required. Therefore, each equivalent class of ideals maps to an equivalent class of BQF's from which there is a unique reduced BQF. Hence the number of equivalent classes of ideals (i.e., class number) is equal to the number of reduced BQF's.

Example. There are three reduced BQF's with disc -23, hence the class number of $\mathbb{Q}(\sqrt{-23})$ is 3.

The BQF method gives us the *exact* class number. Now we discuss some heuristic methods.

21.1. **Class number estimates: analytic method**

Definition 63. Let D be a *negative* discriminant of $\mathbb{Q}(\sqrt{D})$. Define

$$L_D(s) := \sum_{n \geq 1} \left(\frac{D}{n}\right) n^{-s}.$$

This series will converge for all $\mathrm{Re}(s) > 1$, and will converge conditionally at $s = 1$. It has an analytic continuation to the whole complex plane.

Proposition 64. *Let D be as above. Then*

$$L_D(1) = \frac{2\pi h(D)}{\omega(D)\sqrt{|D|}}$$

where $\omega(D)$ is the number of roots of unity in $\mathbb{Q}(\sqrt{D})$.

Example. Let $K = \mathbb{Q}(\sqrt{-31})$. Then $D = -31$. We can show that $\omega(-31) = 2$. Thus,

$$h(-31) = \frac{\sqrt{31}}{\pi} \cdot 2 \sum_{n \geq 1} \left(\frac{D}{n}\right) n^{-1}.$$

Truncating the sum at $n \leq N$ gives us

N	$h(-31)$
10	3.41866
100	2.998259
1000	3.001754
10000	3.000177
100000	3.0000000

An alternate method involves the Euler product

$$L_D(s) = \prod_{p \text{ prime}} \left(1 - \frac{(D/p)}{p^s}\right)^{-1}.$$

With N primes we get

N	$h(-31)$
10	3.0475
100	3.0213
1000	3.0035
10000	3.00188

Theorem 23 (Schoof)**.** *Assuming the ERH, there exists a computable c such that if $N = c \cdot \log^2 |D|$,*

$$\frac{3}{4} \leq \frac{\prod_{p \leq N} \left(1 - \frac{(D/p)}{p}\right)^{-1}}{L_D(1)} \leq \frac{3}{2}.$$

21.2. Shanks's baby step-giant step method

In the previous method we exhaustively found all the BQF's that were reduced to compute the class number. We never took advantage of the fact that $\mathrm{Cl}(K)$ is a groups have structure. This method will use the fact that it is a group. The basic idea is that

1. (1) Pick $a \in \mathrm{Cl}(K)$ at random.
2. (2) Compute the order of a (call it $|a|$).
3. (3) Let $G_1 = \mathrm{Cl}(K)/\langle a \rangle$ and repeat as necessary.
4. (4) If we know that $B < h(D) \leq 2B$ for some B (which we can get from the estimation method), then we repeat until we have the size of the subgroup in this range, when then must equal to $\mathrm{Cl}(K)$.

The first thing we wish to show is how to compute $|a|$, *assuming* we know how to do computations in the group and that we have a bound on the group size. Assume $|G| \leq 2B$. Then $|a| \leq 2B$. Let $d = \left\lfloor \sqrt{2B} \right\rfloor$. We know that $a^r = 1$ for some $1 \leq r \leq 2B = d^2$. Let $r = r_1 d + r_2$ with $r_1, r_2 \in \{0, 1, \ldots, d-1\}$. Then $a^{r_1 d + r_2} = 1$ if and only if $a^{r_2} = a^{-r_1 \cdot d}$. Now we can construct two lists, $\{a^0, a^1, \ldots, a^{d-1}\}$ and $\{a^{-d}, a^{-2d}, \ldots, a^{-(d-1)d}\}$ and see if there is a match. This can be done quickly by sorting the two lists. If (or when) there is a match, construct $r = r_1 d + r_2$ such that $a^r = 1$. Note that $|a| \leq r$, but we only know that $|a| \mid r$. Write $r = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$. We know that $|a| = p_1^{e_1} \cdots p_k^{e_k}$ with $0 \leq e_i \leq d_i$. Further, $p_1^{d_1} \cdots p_k^{d_k} = 1 \neq p_1^{d_1} p_2^{d_2} \cdots p_s^{e_s - 1} \cdots p_k^{d_k}$. Let's say that we wish to test whether $a^s = 1$ for some $s \mid r$. Write $s = s_1 d + s_2$. So $a^s = 1$ if and only if $a^{s_2} = a^{-s_1 d}$ – which we computed already. We know that $|a| \mid |G|$. If $B < |a| \leq 2B$ we are done. Otherwise, we have to repeat this on $G/\langle a \rangle$.

Example. Consider $(\mathbb{Z}/100\mathbb{Z})^* = \{a : \gcd(a, 100) = 1\}$. We know that $|(\mathbb{Z}/100\mathbb{Z})^*| < 45$. Take $d = \lceil\sqrt{45}\rceil = 7$. Pick a random element – say, $a = 11$. We see that $\{a^i\}_{i=1}^{49} = \langle a\rangle$. Now note that

$$\{a^i\}_{i=1}^{49} = \{a^{7i+j}\}_{1\leq i,j\leq 7} = \{a^i\}_{i=8}^{56}.$$

Hence if $a^{7i+j} = 1$ then $a^j = a^{-7i}$. Since we have multiple matches, we can pick any (the smaller the better). Thus, for instance, we see that $a^5 = 51 = a^{-35}$. Thus $a^{40} = 1$. Note that $40 = 2^3 \cdot 5$, and that $a^{20} = 1 \Rightarrow a^6 = a^{-14}$; $a^{10} = 1 \Rightarrow a^3 = a^{-7}$. But $a^5 \neq 1$.

$$\begin{aligned}
a^1 &= 11 & a^{-7} &= 31\\
a^2 &= 21 & a^{-14} &= 61\\
a^3 &= 31 & a^{-21} &= 91\\
a^4 &= 41 & a^{-28} &= 21\\
a^5 &= 51 & a^{-35} &= 51\\
a^6 &= 61 & a^{-42} &= 81\\
a^7 &= 71 & a^{-49} &= 11.
\end{aligned}$$

Thus, the order has 2^1 as a factor. But since $a^8 \neq 1$, or $a^1 \neq a^{-7}$, the order is 10. Hence $\langle a\rangle = \{a^i\}_{i=1}^{10} = \{a^{4i+j}\}_{1\leq j\leq 4, 1\leq i\leq 3}$. Now let

$$\begin{aligned}
S_a &= \{a^j\}_{j=1}^4 = \{11, 21, 31, 41\}\\
S_a^{-1} &= \{a^{-j}\}_{j=1}^4 = \{91, 81, 71, 61\}\\
T_a &= \{a^{4i}\}_{i=1}^3 = \{41, 81, 21\}\\
T_a^{-1} &= \{a^{-4i}\}_{i=1}^3 = \{61, 21, 81\}.
\end{aligned}$$

It is not hard to see that $\langle a\rangle = S_a \cdot T_a$. Pick $b \in G$ at random. If $G \neq \langle a\rangle$ then b has less than 50% chance of being in $\langle a\rangle$. So the chance that this happens for n random choices of b is at most $1/2^n$. So if we try this twenty times, then we always lie in $\langle a\rangle$. Either we are caught in an unlucky event ($\approx 10^{-6}$), or $\langle a\rangle = G$.

Pick $b \in G$ random, say $b = 7$. If $b \in \langle a\rangle$ then $b \in S_aT_a$. Thus $bS_a^{-1} \cap T_a \neq \emptyset$. Thus $b \in \langle a\rangle$. We wish to find the order of b in $(\mathbb{Z}/100\mathbb{Z})^*/\langle a\rangle$, or equivalently a power of b such that $b^k \in \langle a\rangle$. As $|(\mathbb{Z}/100\mathbb{Z})^*| < 45$ and $|a| = 10$, we have $|(\mathbb{Z}/100\mathbb{Z})^*/\langle a\rangle| < 4.5$. Thus we only need to look at b^k for $k = 1, 2, 3, 4$. That is, we need to find k and l such that $b^{2k+l} \in \langle a\rangle, k, l \in \{1, 2\}$. Hence $b^{2k+l} \in S_aT_a$ so $b^lS_a^{-1} \cap b^{-2k}T_a \neq \emptyset$.

Now note

$$\begin{aligned}
bS_a^{-1} &= \{37, 67, 97, 27\}\\
b^2S_a^{-1} &= \{59, 69, 79, 89\}\\
b^{-2}T_a &= \{89, 29, 39\}\\
b^{-4}T_a &= \{61, 21, 81\}.
\end{aligned}$$

This gives us $b^4 \in \langle a\rangle$ since $89 \in b^2S_a^{-1} \cap b^{-2}T_a$. Notice now that $b^2 \in \langle a\rangle \Leftrightarrow b^2S_a^{-1} \cap T_a \neq \emptyset$. But since $b^2S_a^{-1} \cap T_a = \emptyset$ it follows that $b^2 \in \langle a\rangle$. So $|(\mathbb{Z}/100\mathbb{Z})^*|$ is divisible by $|\langle a\rangle| = 10$; and we see that $|(\mathbb{Z}/100\mathbb{Z})^*/\langle a\rangle|$ is divisible by 4. Thus $|(\mathbb{Z}/100\mathbb{Z})^*|$ is divisible by 40, so $|(\mathbb{Z}/100\mathbb{Z})^*| = 40$ since $|(\mathbb{Z}/100\mathbb{Z})^*| < 45$. We now know that there are three finite abelian groups of size 40, namely $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ and $(\mathbb{Z}/100\mathbb{Z})^* = \langle 7, 11\rangle$.

Remark. We now make a few comments regarding the above example.

(1) In general, we can continue in this fashion, constructing $S_{a,b} = \{a^i b^j\}$, where $|S_{a,b}|$ is approximately the square root of the size of the subgroup.
(2) Here computing $S_a, S_a^{-1}, T_a, T_a^{-1}$ is excessive. We could go with just S_a and T_a^{-1} for example. This requires more book-keeping. Taking the inverse of a BQF is easy, i.e., $(a,b,c)^{-1} = (a,-b,c)$.
(3) Here the choice of indices, a^{di+j}, is somewhat flexible. So long as $\{di+j\} \bmod |G| = \{0,1,\ldots,|G|-1\}$, we are fine. There are advantages to using negative i and j.
(4) If we have upper bound *and* lower bound for $|G|$, then we can compute fewer terms for giant steps, i.e., no need to start at a^{-d}, start at a^{-kd} for some kd greater than that lower bound.
(5) If we don't know the size of G then it is harder to pick d. If we pick d randomly and have no collisions, then $|G| > d^2$, so we need to increase d.
(6) In the other direction, if lots of random choices for b all have $b \in \langle a\rangle$, chances are that G is in this subgroup.

We now need to look at how to do this for BQF's, i.e., how to multiply and how to find a random element.

Example. Let $K = \mathbb{Q}(\sqrt{-14})$. This has discriminant -56. We see that $(3,2,5)$ is reduced BQF with discriminant $2^2 - 4\cdot 3\cdot 5 = -56$. Recall the correspondence

$$\begin{aligned}(a,b,c) &\leftarrow \{2ax + (b+\sqrt{D})y : x,y\in\mathbb{Z}\}\\ (3,2,5) &\to \{6x + (2+\sqrt{-56})y\} \sim \{3x + (1+\sqrt{-14})y\} =: I.\end{aligned}$$

We can compute $(3,2,5)^2$ by looking at I^2. Here, I has Hermite normal form

$$\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}.$$

Thus I^2 has Hermite normal form

$$\begin{pmatrix} 2 & -14+1 \\ 3 & 3 \\ 3 & 3 \\ 0 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 16 \\ 2 & 5 \\ 0 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 7 \\ 0 & 9 \end{pmatrix}.$$

Hence $I^2 = \{9x + (7+\sqrt{-14})y\} \sim \{18x + (14+\sqrt{D})y\} \to (9,14,c)$. Note that $14 - 4\cdot 9\cdot c = -56$, or $c = 7$. So $(3,2,5)^2 = (9,14,7) \sim (7,-14,9) \sim (7,0,2) \sim (2,0,7)$. Similarly,

$$(3,2,5)\cdot(2,0,7) \to \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & -14 \\ 3 & 0 \\ 2 & 2 \\ 0 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 4 \\ 0 & 6 \end{pmatrix},$$

which corresponds to the BQF $(6,8,5) \sim (3,-2,5)$. Doing this for each BQF with discriminant -56 gives us the following multiplication table:

$\cdot$	$(1,0,14)$	$(3,2,5)$	$(2,0,7)$	$(3,-2,5)$
$(1,0,14)$	$(1,0,14)$	$(3,2,5)$	$(2,0,7)$	$(3,-2,5)$
$(3,2,5)$	$(3,2,5)$	$(2,0,7)$	$(3,-2,5)$	$(1,0,14)$
$(2,0,7)$	$(2,0,7)$	$(3,-2,5)$	$(1,0,14)$	$(3,2,5)$
$(3,-2,5)$	$(3,-2,5)$	$(1,0,14)$	$(3,2,5)$	$(2,0,7)$

22. March 23

There is a way to multiply BQF directly without going into ideals. It is faster but not that intuitive. If $(a_3, b_3, c_3) = (a_1, b_1, c_1) \cdot (a_2, b_2, c_2)$, then

(1) $g = \gcd(a_1, a_2, (b_1 + b_2)/2)$
(2) $g = a_1\alpha + a_2\beta + \gamma(b_1 + b_2)/2$
(3) $r = \beta = \beta \cdot (b_1 - b_2)/2 + \gamma c_2$.
(4) $a_3 = a_1 \cdot a_2/g$
(5) $b_3 = b_2 + 2a_2r/g$
(6) $c_3 = (b^2 + D)/(4a_3)$, where $D = b_1^2 - 4a_1c_1$.

If $\gcd(a_1, a_2) = 1$, then this simplifies into

(1) $g = 1$
(2) $g = 1 = \alpha a_1 + \beta b_2$ (i.e., $\gamma = 0$)
(3) $r = \beta(b_1 - b_2)/2$
(4) $a_3 = a_1 \cdot a_2$
(5) $b_3 = b_2 + 2a_2r \equiv b_2 \bmod a_2$
(6) $b_3 \equiv b_2 + 2a_2\beta(b_1 - b_2)/2 \equiv b_2 + b_1 - b_2 \equiv b_1 \bmod a_1$

Thus $a_3 = a_1a_2, b_3 \equiv b_1 \pmod{a_1}, b_2 \pmod{a_2}, c_3 = (b_3^2+D)/(4a_3)$. The last step of Shanks's baby step, giant step is the following: how do we find random group elements?

Lemma 12. *Let $\left(\frac{D}{p}\right) \neq -1$. Then there exist $|b_p| \leq p$ and c_p such that (p, b_p, c_p) is a BQF with discriminant D.*

Proof. Assume that $\left(\frac{D}{p}\right) = 1$. This tells us that there exists b such that $b^2 \equiv D \pmod{p}$. Clearly there exists b_2 such that $b_2^2 \equiv D \pmod{4}$. So by the Chinese remainder theorem, there exists b_p such that $b_p^2 \equiv D \pmod{4p}$. As there are two choices for b_2 we can enuser that b_p is from an interval of length $2p$, i.e., $-p \leq b_p \leq p$. Note that $b_p^2 \equiv D \pmod{4p}$ so $b_p^2 - D = 4p \cdot c_p$ for some c_p. We claim both $(p, \pm b_p, c_p)$ have the desired property as $b_p^2 - 4pc_p = D$ as required. □

Remark. We have lots of p such that $(D/p) \neq -1$ pre-computed by doing analytic estimates. Finding b such that $b^2 \equiv D$ is easy. This is so because we know how to factor $x^2 - D$ mod p. We can just start at the last of the three steps. Since $b^2 - 4pc = D$, we have that

$$c = \frac{b^2 - D}{4p} \leq \frac{p^2 - D}{4p} \approx 4p - \frac{D}{4p}.$$

If p is relatively small ($\sim \sqrt{D}/4$) then $a < c$; and this is very close to being reduced.

Example. We try to find some non-trivial BQF of discriminant $-4 \cdot 14 = -56$. Note that $\left(\frac{-56}{3}\right) = \left(\frac{-56}{5}\right) = 1$ while $\left(\frac{-56}{7}\right) = 0$. So $b^2 \equiv -56 \equiv 1 \pmod{3}$ and $b_3 \equiv 1$ or $2 \pmod{3}$.

Also need $b_3^2 \equiv -56 \equiv 0 \pmod 4$ and $b_3 \equiv 0$ or $2 \pmod 4$. Thus $b_3 = -2$ so $(3, -2, \frac{4+56}{12}) = (3, -2, 5)$.

Similarly, $b_5^2 \equiv 4 \pmod 5), b_5 \equiv 2$ or $3 \pmod 5), b_5^2 \equiv 0 \pmod 2$ and $b_5 \equiv 0$ or $2 \pmod 4$. In this case $b_5 = 2$ works. So $(5, 2, 3)$ works. The same thing can be done to get $(7, 0, 2)$.

Example. We want to compute $(7, 0, 2)\cdot(3, -2, 5)$. Then $(7, 0, 2)\cdot(3, -2, 5) = (21, 28, \frac{28^2+56}{84}) = (21, 28, 10)$.

22.1. McCurley's subexponential method

With the baby-step, giant-step algorithm, if we are very unlucky, we find some $H < \mathrm{Cl}(K)$ and find a divisor of $h(D)$. This method attacks the problem from the other direction. And if we are unlucky we get a multiple of $h(D)$. Let $\mathcal{P} = \{(p_1, b_{p_1}, c_{p_1}), (p_2, b_{p_2}, c_{p_2}), \dots\}$ with $|\mathcal{P}| = n$. We can find a bound so that if n is larger than this bound then $\mathcal{P}$ generates $\mathrm{Cl}(K)$.

Define $\varphi : \mathbb{Z}^n \to \mathrm{Cl}(K)$ by $\varphi(x_1, \dots, x_n) = (p_1, b_{p_1}, c_{p_1})^{x_1} \cdots (p_n, b_{p_n}, c_{p_n})^{x_n}$. This is a surjective group homomorphism. The kernel of this map, say Λ is a group. Further, $\mathbb{Z}^n/\Lambda \cong \mathrm{Cl}(K)$. Hence $|\mathbb{Z}^n/\Lambda| = [\mathbb{Z}^n : \Lambda] = |\mathrm{Cl}(K)| = h(D)$. Assume that Λ has a basis $\{\bar{x}_1, \dots, \bar{x}_n\}$ with $\bar{x}_1 = (x_1^{(1)}, \dots, x_n^{(1)})$, and so forth. In this case, $[\mathbb{Z}^n : \Lambda] = |\det(x_j^{(i)})_{1\le i,j\le n}|$. This would be great if we could find Λ. If we can find a set of vectors $\bar{x}_1, \dots, \bar{x}_n \in \Lambda$ then we set Λ_0 the lattice from $\bar{x}_1, \dots, \bar{x}_n$. This has the property that $[\mathbb{Z}^n : \Lambda_0] = [\mathbb{Z}^n : \Lambda][\Lambda : \Lambda_0] = h(D) \cdot [\Lambda : \Lambda_0] = h(D) \cdot a$ for some random number a. Thus the basic algorithm looks like the following:

(1) $g := 0$
(2) Find random relations $\bar{x}_1, \dots, \bar{x}_n$
(3) Let $g := \gcd(g, \det((\bar{x}_1, \dots, \bar{x}_n)^T))$
(4) Repeat the (2)-(3) loop as desired.

Remark. The probability that $\gcd(a, b) = 1$ for random a, b is $6/\pi^2$. So after n steps, the chance of not having $h(D)$ is $(1 - \frac{6}{\pi^2})^n$, which converges to 0 as $n \to \infty$ (and quickly). We want $\gcd(a, b) = 1$ since $\gcd(h(D) \cdot a, h(D) \cdot b) = h(D) \cdot \gcd(a, b)$ (with $h(D) \cdot a$ and $h(D) \cdot b$ coming from the determinants) and we don't want the extraneous $\gcd(a, b)$ so we want $\gcd(a, b)$ to be 1.

However we don't know how to find this random relation. One can try the naïve method, but the chance of success is low should $h(D)$ turn out to be large. Thus, this is not a good way to do it.

23. March 30: McCurley's subexponential algorithm, continued

Consider the map $\varphi : \mathbb{Z}^n \to \mathrm{Cl}(K)$ by

$$\varphi(e_1, \dots, e_n) = (p_1, b_{p_1}, c_{p_1})^{e_1}(p_2, b_{p_2}, c_{p_2})^{e_2} \cdots (p_n, b_{p_n}, c_{p_n})^{e_n}$$

and $\Lambda = \ker \varphi$. Here, $[\mathbb{Z}^n : \Lambda] = |\mathrm{Cl}(K)|$. So our goal is to find $\Lambda_i \subseteq \Lambda$ by *finding random elements in* Λ. This gives us $h(K) \mid [\mathbb{Z}^n : \Lambda_i]$ for all $\Lambda_i \subseteq \Lambda$. Taking enough Λ_i gives a good estimate for $|\mathrm{Cl}(K)|$.

Lemma 13. *Let (a, b, c) be a BQF with discriminant D. Further, let $a = p_1^{e_1} \cdots p_k^{e_k}$. Then*

$$(a, b, c) \sim \prod_{i=1}^{k} (p_i, \pm b_{p_i}, c_{p_i})^{e_i}.$$

Moreover, $b \equiv \pm b_{p_i} \pmod{p_i}$.

Proof. Recall that if (a,b,c) and (d,e,f) had $\gcd(a,d)=1$ then $(a,b,c)\cdot(d,e,f)=\left(ad,B,\frac{B^2-D}{4ad}\right)$ where $B\equiv b\pmod{2a}$ and $B\equiv e\pmod{2d}$. In a similar way we can show $(p,b_p,c_p)^e=(p^e,B,\frac{B^2-D}{4p^e})$ with $B\equiv b\pmod p$ (and $B^2\equiv D\pmod{p^e}$). □

Example. We want to find a,b,c,d such that $(15,-4,67)=(3,a,b)\cdot(5,c,d)$. Note that $a=2$ and $c=-4$. Using Lemma 13 we see that $b=\frac{4+4004}{6}$ and $d=\frac{16+4004}{20}=201$ since $16-4\cdot15\cdot67=-4004$. The same type of approach gives us $(25,14,42)=(5,4,201)^2=(5,-4,201)^{-2}$.

23.1. How to find a relation

(1) Step 1: Randomly multiply some generators together (with various exponents), say $(p_1,b_{p_1},c_{p_1})^{e_1},\dots,(p_n,b_{p_n},c_{p_n})^{e_n}$.
(2) Step 2: Reduce this binary quadratic form to some (a,b,c).
(3) Step 3: If we are lucky, then $a\neq p_1^{|e_1|}\cdots p_n^{|e_n|}$ but $a=p_1^{f_1}p_2^{f_2}\cdots p_n^{f_n}$.
(4) Step 4: Now factor the BQF $(a,b,c)=(p_1,b_{p_1},c_{p_1})^{\pm f_1}\cdots(p_n,b_{p_n},c_{p_n})^{\pm f_n}$. As this equals $(p_1,b_{p_1},c_{p_1})^{e_1}\cdots$, this gives us a relation in Λ. That is, we have $(e_1\mp f_1,e_2\mp f_2,\dots,e_n\mp f_n)\in\Lambda$.
(5) Do Steps 1–4 a number of times to get an independent set in Λ.

Example. Find a relation between $(2,2,501),(3,2,334),(5,-4,201),(7,0,143)$. We will try $[1,0,1,1]$. So let

$$(2,2,501)\cdot(5,-4,201)\cdot(7,0,143)=(70,b,c).$$

Note that $b\equiv2\bmod 4$, $-4\bmod 10$, and $\equiv0\bmod 14$. We see that $b=-14$ works, by the Chinese remainder theorem. So $(b,c)=(-14,15)$. But $(70,b,c)$ is not reduced. But we have $(70,-14,15)\sim(15,14,70)=(3,2,334)\cdot(5,4,201)=(3,2,334)\cdot(5,-4,201)^{-1}$. This gives us that $[1,0,1,1]-[0,1,-1,0]=[1,-1,2,1]\in\Lambda$. Repeating this three more times gives $[3,3,4,-5],[-2,-4,-2,2],[-4,0,0,4]\in\Lambda$. It turns out that the discriminant of this matrix is 160. Keep going on with different vectors and you will get $200,240,-80,\dots$. This gives us $h(-4004)\,|\,40$ by gcd's.

23.2. Binary quadratic forms of real quadratic fields

We have the same connection as before ideals between $\mathbb{Z}_K$ where $K=\mathbb{Q}(\sqrt d)$ and binary quadratic forms of $\operatorname{disc}(K)$. We did not require d to be negative.

Example. For example, $I=\{4x+(3+\sqrt{17})y : x,y\in\mathbb{Z}\}$. This gives us the binary quadratic form $(2,3,\frac{3^2-17}{8})=(2,3,-1)$.

We have the same idea of equivalents, i.e., $(a,b,c)\sim(c,-b,a)\sim(a,b+2ak+c+bk+ak^2)$. We also use the equivalent $(a,b,c)\sim(-a,b,-c)$. This comes from looking at the ideal and noticing that they are the same. This wasn't needed in the imaginary case. As before, we can define what it means for a BQF to be reduced. In the case of BQF's with positive discriminant, a BQF is reduced if $\left|\sqrt D-2|a|\right|<b\le\sqrt D$.

Example. $(2,3,-1)$ is reduced, since $|\sqrt{17}-4|=0.123\cdots<b=3<\sqrt D=4.123\dots$.

Unfortunately, reduced forms are not unique within the same equivalence class. For instance, note that $(2,3,-1)\sim(-1,-3,2)\sim(-1,3,2)$, and both $(2,3,-1)$ and $(-1,3,2)$ are reduced. In fact, $(-1,3,2)\sim(2,1,-2)$ and $(2,1,-2)$ is also reduced. Thus, equivalent reduced BQF's are not necessarily equal. There do exist two functions ρ and $(a, b, c) \leftrightarrow (-a, b, -c)$ such that all equivalent reduced BQF's lie in the orbit of these two functions.

Our goal will be to show how to reduce a BQF and to find its orbit. Consider a reduced BQF $(a, b, c) = (2, 3, -1) \sim (-1, -3, 2) \sim (-1, 3, 2) = (a', b', c')$. We note that we choose $a' = c$ (clearly). We next choose b' such that $b \equiv -b \pmod{2a'}$ or $\pmod{2c}$. b' needs to be in the correct range i.e., $\left|\sqrt{D} - 2|c|\right| < b' < \sqrt{D}$. Clearly there can only be the unique choice for b'. Lastly, $c' = \frac{b^2-D}{4a'} = \frac{b^2-D}{4c}$. In fact, this works if $c < \sqrt{D}$. So we define $\rho(a, b, c) = (a', b', c')$ if $|c| < \sqrt{D}$, $a' = c$, and b' as explained in our dicsussion, and $c' = \frac{b'^2-D}{4a'}$.

Lemma 14. *Let (a, b, c) be a reduced BQF with $D > 0$. Then $|a|, b, |c| < \sqrt{D}$ and $ac < 0$.*

Proof. $b^2 - 4ac = D$ and $b < \sqrt{D}$ and $b < \sqrt{D}$. Thus $-4ac = D - b^2 > 0$ so $ac < 0$. We claim that $|a| + |c| - \sqrt{D} < 0$ which implies $|a|, |c| < \sqrt{D}$. Since

$$\begin{aligned}
|a| + |c| - \sqrt{D} &= \frac{4|a|^2 + 4|ac| - 4|a|\sqrt{D}}{4|a|} \\
&= \frac{4|a| - 4ac - 4|a|\sqrt{D}}{4|a|} \\
&= \frac{4|a| + D - b^2 - 4|a|\sqrt{D}}{4|a|} \\
&= \frac{(\sqrt{D} - 2|a|)^2 - b^2}{4|a|}.
\end{aligned}$$

Since $\left|\sqrt{D} - 2|a|\right| < b$ we have that this expression is negative. Hence $|a| + |c| - \sqrt{D} < 0$ and $|a|, b, |c| < \sqrt{D}$. □

Corollary 11. *ρ maps reduced forms to reduced forms.*

24. April 1

The ρ we defined last time will not work if $|c| > \sqrt{D}$. In this case, we use the same map, except that the restriction placed on b' will be different. Rather than using $\left|\sqrt{D} - 2|c|\right| < b' < \sqrt{D}$, we use $-|c| < b' \leq |c|$ instead.

Lemma 15. *If $|c| > \sqrt{D}$ and $\rho(a, b, c) = (a', b', c')$ then $|c'| \leq |c|/2$.*

Proof. Clearly $b' \leq |a'| = |c|$ by construction, since $a' = c$ here. Thus

$$|c'| = \left|\frac{b'^2 - D}{4a'}\right| \leq \frac{|c|^2 + |c|^2}{4|c|} = \frac{|c|}{2},$$

as required. □

Example. Consider the non-reduced BQF $(2, 8, 5)$. Find a reduced form equivalent to it. This one has discriminant $24 = 4 \cdot 6$. Then $\rho(2, 8, 5) = (5, b', c')$. We need $b' \equiv -8 \pmod{10}$. Since $|c| > \sqrt{24}$, we need $-5 \leq b' \leq 5$. Thus $b' = 2$. So $\rho(2, 8, 5) = (5, 2, -1)$. Upon iteration, ρ takes a non-reduced BQF to a reduced BQF, and a reduced BQF to a reduced BQF. We state the following theorem without proof.

Theorem 24. *Let (a,b,c) and (d,e,f) be two equivalent BQF's with positive discriminant. Let $A = \{\rho^n(a,b,c)\}$ and $E = \{\rho^n(d,e,f)\}$. Then either $A \cap E$ is the set of reduced forms equivalent to (a,b,c) or $A \cap \sigma(E)$ is the set of reduced forms equivalent to (a,b,c) hewer $\sigma(a,b,c) = (-a,b,-c)$.*

Example. Find all reduced BQFs with discriminant 17. Recall that $|a|, b, |c| \leq \sqrt{17}$ and $\left|\sqrt{17} - 2|a|\right| < b < \sqrt{17}$. Thus $a = \pm 4, \pm 3, \pm 2, \pm 1$. If $a = -4$, then $\left|\sqrt{D} - 2|a|\right| \approx 3.87\cdots < b < 4.123\ldots$. Thus $b = 4$ but $c = -1/8 \notin \mathbb{Z}$ so not a reduced form. Keep going $a = -3, -2, -1, \ldots$. Once you go through all the cases you will find out all the forms. We get six forms: $(-2,1,2), (-2,3,1), (-1,3,2), (1,3,-2), (2,1,-2), (2,3,-1)$. It turns out that all the six BQFs are in the same orbit. Hence there is only one thing in the class group. This tells us that $\mathbb{Z}_K$ with $K = \mathbb{Q}(\sqrt{-17})$ is a unique factorization domain and that the class number of K is 1.

Example. We want to find the class number of $\mathbb{Q}(\sqrt{15})$, which has discriminant 60. Using the theorem above we get the reduced forms $(-6,6,1), (-1,6,6), (1,6,-6), (6,6,-1), (-3,6,2), (-2,6,3), (2,6,-3), (3,6,-2)$. Here, $\rho(-6,6,1) = (1,6,-6)$ and $\rho(1,6,-6) = (-6,6,1)$. We also have $\sigma(-6,6,1) = (6,6,-1)$ and $\rho(1,6,-6) = (-1,6,6)$. So here the first four are all in one orbit.

24.1. Analytic methods

Before discussing the analytic methods, we need to discuss the unit group.

Definition 65. We say that $x \in \mathbb{Z}_M$ is a unit if $x^{-1} \in \mathbb{Z}_K$, or equivalent $\mathrm{N}(x) = \pm 1$. As norms and algebraic integers are closed under multiplication, so is the set of units. This this rise to an abelian group with the identity $1 \in \mathbb{Z}_K$.

Theorem 25. *The unit group looks like $U \times \mathbb{Z}^{r_1+r_2-1}$, where r_1 and r_2 denote the number of real embeddings, r_3 the number of pairs of imaginary embeddings (or number of imaginary conjugate embeddings) and U a finite cyclic group.*

Corollary 12. *If $K = \mathbb{Q}(\sqrt{d})$ and $d < 0$, then the unit group is finite since $r_1 = 0, r_2 = 1$. Note that $\mathbb{Z}_K^* \cong U \times \mathbb{Z}^0 = U$. If $K = \mathbb{Q}(\sqrt{d})$ and $d > 0$, then the unit group is of the form $U \times \mathbb{Z}$, since $r_1 = 2, r_2 = 0$.*

Let u be a generator for the "$\mathbb{Z}$" portion. So the unit group looks like $U \times \langle u \rangle$ where $|u| = \infty$.

Definition 66. Let $K = \mathbb{Q}(\sqrt{d})$ and $D > 0$. Then the u above is called a *fundamental unit*. The *regulator of K* is $\log |u|$.

Example. $2 + \frac{1+\sqrt{21}}{2}$ is a unit in $\mathbb{Z}_K$, where $K = \mathbb{Q}(\sqrt{21})$. Note that $\mathrm{N}\left(2 + \frac{1+\sqrt{21}}{2}\right) = \left(\frac{5+\sqrt{21}}{2}\right)\left(\frac{5-\sqrt{21}}{2}\right) = 1$. This is in fact a fundamental unit. In fact there exist $u_n, v_n \in Z$ such that

$$u_n + v_n\left(\frac{1+\sqrt{21}}{2}\right) = \left(2 + \frac{1+\sqrt{21}}{2}\right)^n.$$

As before, we define

$$L_D(s) = \sum_{n\geq 1} \left(\frac{D}{n}\right) n^{-s}.$$

Theorem 26. *Let $K = \mathbb{Q}(\sqrt{d})$ with discriminant $D > 0$. Then*

$$L_D(1) = \frac{2h(D)r(D)}{\sqrt{D}},$$

where $r(D)$ is the regulator of K. Thus

$$h(D) = \frac{\sqrt{D}L_D(1)}{2r(D)}.$$

24.2. **Computing regulators**

The study of fundamental units is connected to Pell equations and continued fractions.

Definition 67. $[a_0, a_1, \dots, a_n] = a_0 + \frac{1}{a_1+\frac{1}{a_2+\frac{1}{\ddots_{a_{n-1}+\frac{1}{a_n}}}}}$. And we define $[a_0, a_1, \dots] := \lim_{n\to\infty}[a_0, a_1, \dots, a_n]$. Also, we say that $p_n/q_n = [a_0, \dots, a_n]$ is a convergent of $[a_0, a_1, \dots]$.

We have a nice algorithm to find the continued fraction of $\alpha \in \mathbb{R}$. As $\alpha = a_0 + b$ where $b \in (0,1)$, we can let $a_0 = \lfloor \alpha \rfloor$. Set $\alpha_0 = \alpha$. So $\alpha_0 = a_0 + \frac{1}{a_1+(*)}$. Then let $\alpha_1 = \frac{1}{\alpha_0 - a_0} = a_1 + b'$ where $b/ \in (0,1)$. Write $a_1 = \lfloor \alpha_1 \rfloor$. Keep going. In general, $\alpha_n = \frac{1}{\alpha_{n-1} - a_{n-1}}$, $a_n = \lfloor \alpha_n \rfloor$.

Theorem 27. *A continued fraction terminates at some point (i.e., a continued fraction is finite) if and only if x is rational. The continued fraction of x is eventually periodic if and only if x is the root of some quadratic polynomial.*

Let

$$\frac{p_n}{q_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}.$$

We will continue next Monday on this topic.

25. April 4

Let $K = \mathbb{Q}(\sqrt{d})$ with d squarefree, $d \equiv 2, 3 \pmod 4$ and $d > 0$. In this case we know that all algebraic integers are of the form $x + y\sqrt{d}$ and have $\mathrm{N}(x + y\sqrt{d}) = x^2 - dy^2$. If these are units, we then want the norm to be ± 1. We may assume without loss of generality that $x, y > 0$. Letting $u_n + v_n\sqrt{d} = (x + y\sqrt{d})^n$, we again see that $u_n + v_n\sqrt{d}$ is a unit. Further, $u_n = xu_{n-1} + dyv_{n-1} \geq u_{n-1}$ and $v_n = xv_{n-1} + yu_{n-1} \geq v_{n-1}$ ($u_n + v_n\sqrt{d} = (x + \sqrt{d}y)(u_{n-1} + \sqrt{d}v_{n-1})$). In particular, this sequence is growing. This allows us to say that the smallest x, y such that $x^2 - dy^2 = \pm 1$ is a *fundamental unit.* Notice that if $x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y) = \pm 1$, then

$$|x - \sqrt{d}y| = \frac{1}{x + \sqrt{d}y} \leq \frac{1}{2y}$$

(assume without loss of generality that $d \geq 6$). So

$$\left|\frac{x}{y} - \sqrt{d}\right| \leq \frac{1}{2y^2}.$$

Theorem 28. *If $\frac{p}{q}$ is such that $\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{2q^2}$ then p/q is a convergent of α. This means that it suffices to look for the first (i.e., the smallest) convergent of $\sqrt{d}$, say $\frac{p_n}{q_n}$, such that $\mathrm{N}(p_n + q_n\sqrt{d}) = \pm 1$.*

Example. We find the regulator of $K = \mathbb{Q}(\sqrt{6})$. We can compute the continued fraction of $\sqrt{6}$ as $[2, 2, 4, 2, 4, \ldots]$. This has convergents $\frac{2}{1}, \frac{5}{2}, \frac{22}{9}, \frac{49}{20}, \ldots$. But $\mathrm{N}(2 + \sqrt{6}) = 2^2 - 6 \neq 1$ while $\mathrm{N}(5 + 2\sqrt{6}) = 5^2 - 4 \cdot 6 = 1$. Therefore $5 + 2\sqrt{6}$ is a fundamental unit. The regulator is thus $\log(5 + 2\sqrt{6}) = 2.2924\ldots$.

Assume now that $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 1 \pmod 4), d > 1$, and d squarefree. In this case, all the algebraic integers are of the form $x + y\left(\frac{1+\sqrt{d}}{2}\right)$. If y is even, say $y = 2y'$, then we can rewrite this as $x + 2y'\left(\frac{1+\sqrt{d}}{2}\right) = (x + 1) + y'\sqrt{d} = x' + y'\sqrt{d}$ where $x' = x + 1$. We now have $\mathrm{N}(x' + y'\sqrt{d}) = \pm 1$. If instead y is odd, we write this as $x + y\left(\frac{1+\sqrt{d}}{2}\right) = \frac{1}{2}(2x + y + y\sqrt{d}) = \frac{1}{2}(x' + y\sqrt{d})$. Here, we let $x' = 2x + y, y' = y, x', y'$ both odd. Hence $\mathrm{N}\left(\frac{1}{2}(x' + y'\sqrt{d})\right) = \pm 1$ so $\mathrm{N}(x' + y'\sqrt{d}) = \pm 4$. Similar to before, we look for convergent such that either $p_n^2 - dq_n^2 = pm1$ or p_n, q_n odd and $p_n^2 - dq_n^2 = \pm 4$.

Example. Find the fundamental unit in $K = \mathbb{Q}(\sqrt{21})$. This has continued fraction $[4, 1, 1, 2, 1, 1, 8, 1, 1, 2, 1$. This has convergents $\frac{4}{1}, \frac{5}{1}, \frac{9}{2}, \frac{23}{5}, \frac{32}{7}, \ldots$. Write $\beta := \frac{1+\sqrt{21}}{2}$. But $\mathrm{N}(4 + \beta) = 4^2 - 21 = -5$ while $\mathrm{N}(5 + \beta) = 5^2 - 21 = 4$. Also, 5 and 1 are both odd, thus a fundamental unit is

$$\frac{5}{2} + \frac{21}{2} = 2 + \frac{1 + \sqrt{21}}{2}$$

is a fundamental unit.

Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, Canada N2L 3G1

E-mail address: hsyang@uwaterloo.ca