MATH70042 Algebraic number theory :: Lecture notes

Lecturer: Margherita Pagano

Last edited: 3rd April 2025

Contents

Week 2, lecture 1, 13th January

Motivation

One of the goal of number theory is to solve Diophantine equations: given $p(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$, we want to describe the set $\{(a_1, \dots, a_n) \in \mathbb{Z}^n : p(a_1, \dots, a_n) = 0\}$.

Theorem 0.0.1 (Fermat's last, Wiles 1994)**.** If $x^n + y^n = z^n$ for $x, y, z \in \mathbb{Z}$ and $n \geq 3$, then $xyz = 0$.

The case $n = 2$ is much easier, and such $x, y, z \in \mathbb{Z}$ are called a Pythagoras triple.

- Reduction 1: observe that to describe these triples, one can assume $x, y, z > 0$ since if one of them is zero, the solutions are of the form $(0, \pm a, \pm a)$ or $(\pm a, 0, \pm a)$, and if (x, y, z) is a solution, then $(\pm x, \pm y, \pm z)$ is a solution.
- Reduction 2: one can also assume that x, y, z are pairwise coprime. first note that if $p \mid x, y, z$ and (x, y, z) is a solution, then $\left(\frac{x}{p}, \frac{y}{p}, \frac{z}{p}\right)$ is a solution. Now if a prime p divides two of x, y, z then it divides also the third one. Suppose $p \mid x, y$, then $z^2 = x^2 + y^2 = p^2a^2 + p^2b^2$, so $p \mid z$.
- Reduction 3: one can further assume that only one of x and y is odd. Suppose both are, then $x^2 = y^2 \equiv 1 \bmod 4$, so $z^2 \equiv 2 \bmod 4$, which is not a square, a contradiction. Hence z is also odd. Suppose WLOG that x is even.

Now rewrite $x^2 + y^2 = z^2$ as $y^2 = z^2 - x^2 = (z - x)(z + x)$. Note that:

- $\gcd(z - x, z + x) = 1$. If $p \mid z - x$ and $p \mid z + x$, then $p \mid z - x + z + x = 2z$ and $p \mid -z + x + z + x = 2x$, but $\gcd(x, z) = 1$, so $p = 2$, but $z - x$ is odd by reduction 3, a contradiction.
- $\exists \alpha, \beta \in \mathbb{Z} : z - x = \alpha^2, z + x = \beta^2$. Write y as its unique prime factorisation $\prod_{i=1}^n p_i^{a_i}$ where p_i are primes and $a_i > 0$. But then $y^2 = \prod_{i=1}^n p_i^{2a_i} = (z - x)(z + x)$ and by the above observation, $p_i \mid z - x \implies p_i^{2a_i} \mid z - x$.
- Now, rewrite
$$\begin{aligned} x &= \frac{z + x - (z - x)}{2} = \frac{\beta^2 - \alpha^2}{2} \\ y &= \alpha^2\beta^2 \\ z &= \frac{z + x + z - x}{2} = \frac{\beta^2 + \alpha^2}{2} \end{aligned}$$
where α, β are both odd and coprime. This parameterises all Pythagoras triples.

Remark 0.0.2. A crucial step that we used is called "separating powers" for $n = 2$ over $\mathbb{Z}$.

Lemma 0.0.3. Let $a, b, c \in \mathbb{Z}\backslash\{0\}$ and $n > 0$ such that $a^n = bc$. If $\gcd(b, c) = 1$, then $\exists b_1, c_1 \in \mathbb{Z} : b = \pm b_1^n, c = \pm c_1^n$.

Proof. The proof is similar to the argument above, using the fact that $\mathbb{Z}$ is a unique factorisation domain. □

Now let's consider the case $n = p$ where p is an odd prime. Then one can write

$$x^p + y^p = (x + y)(x + \xi_p p) \cdots (x + \xi_p^{p-1} y)$$

where ξ_p is the pth root of unity. What happens now is the factors are not the usual integers, but in the larger ring $\mathbb{Z}[\xi_p] = \left\{\sum_{i=0}^{p-1} a_i \xi_p^i : a_i \in \mathbb{Z}\right\} \subset \mathbb{C}$. Does $\mathbb{Z}[\xi_p]$ have unique factorisation? Does the analogue of the lemma above work then? How does it help us solving Diophantine equations? These are the questions we will strive to answer in this course.

Week 2, lecture 2, 14th January

We will see that for a certain class of primes (regular primes), $\mathbb{Z}[\xi_p]$ has the separating power property for $n = p$ and we will show how to use this to prove Fermat's last theorem for these primes.

Another example: suppose $x, y \in \mathbb{Z}$ satisfy $y^2 = x^3 + 16$. If $x = 0$ then $y^2 = 16$ so $y = \pm 4$. We claim these are all the solutions.

- Case 1: $x \neq 0$ and y is odd. Write $(y-4)(y+4) = y^2 - 16 = x^3$. Then $\gcd(y-4, y+4) = 1$, since if $p \mid y-4, y+4$, then $p \mid y+4-y+4 = 8$, so $p = 2$, but y is odd so $y-4, y+4$ are odd. This implies both $y-4, y+4$ are cubes, i.e. $y-4 = \alpha^3, y+4 = \beta^3$ for some $\alpha, \beta \in \mathbb{Z}$, but then $8 = \beta^3 - \alpha^3$, and there are no two cubes different by 8.

- Case 2: $x \neq 0$ and y is even. (Similar)

In general, these $y^2 = x^3 + k$ where $k \in \mathbb{Z}$ are called Mordell equations, and we study the solutions by looking into rings $\mathbb{Z}\left[\sqrt{k}\right]$.

1 Introduction

All rings are commutative with unit.

1.1 Unique factorisation domains

Definition 1.1.1. A ring R is an *integral domain* if $x, y \in R, xy = 0 \implies x = 0$ or $y = 0$.

Definition 1.1.2. The group of *units* of R is $R^\times = \{a \in R : \exists b \in R : ab = 1\}$, which is indeed a group with respect to multiplication.

Definition 1.1.3. For $a, b \in R$, we say *a divides b*, or write $a \mid b$, if $\exists c \in R : ac = b$.

Definition 1.1.4. $a \in R \backslash \{0\}$ is *irreducible* if $a \notin R^\times$ and for every $b, c \in R : a = bc$, either b or c is a unit.

Definition 1.1.5. $a \in R \backslash \{0\}$ is *prime* if $a \notin R^\times$ and $b, c \in R, a \mid bc \implies a \mid b$ or $a \mid c$.

Lemma 1.1.6. If $a \in R$ is prime where R is a domain, then a is irreducible.

Proof. Let a be prime and $b, c \in R : a = bc$. Then $a \mid bc$, so WLOG $a \mid b$, i.e. $\exists u \in R : b = au$, so $a = bc = auc$, i.e. $uc = 1$ since R is a domain, in particular c is a unit. □

Definition 1.1.7. A domain R is a *unique factorisation domain* (UFD) if every $a \in R \backslash \{0\}$ has a factorisation $a = up_1 \cdots p_n$ where $u \in R^\times$ and $p_i \in R$ are irreducible. Moreover, if there is another factorisation $a = vq_1 \cdots q_m$ with $v \in R^\times, q_i \in R$ irreducible, then $n = m$ and after reordering $p_i \sim q_i$ (i.e. $\exists u_i \in R^\times : p_i = uq_i$).

Lemma 1.1.8. In a UFD, every irreducible element is prime.

Proof. Let a be irreducible and $b, c \in R : a \mid bc$, i.e. $\exists d \in R : ad = bc$. Write $d = up_1 \cdots p_m, b = vq_1 \cdots q_n, c = wr_1 \cdots r_t$ where $u, v, w \in R^\times$, p_i, q_j, r_s are irreducible. Then

$$uap_1 \cdots p_m = vwq_1 \cdots q_n r_1 \cdots r_t \implies a \sim q_i \text{ or } a \sim r_s \text{ for some } i \text{ or } s \implies a \mid b \text{ or } a \mid c$$

as desired. □

Definition 1.1.9. A domain R is a *principal ideal domain* (PID) if every ideal of R is principal.

Theorem 1.1.10. Every PID is a UFD.

Example 1.1.11. The ring $\mathbb{Z}\left[i\sqrt{3}\right]$ is not a UFD: note that $4 = 2 \times 2 = \left(1 + i\sqrt{3}\right)\left(1 - i\sqrt{3}\right)$. But how do we know 2 and $1 \pm i\sqrt{3}$ are irreducible and the two factorisations are indeed not equivalent? The idea is to introduce the norm map to use properties of the integers, which we are familiar with, to study unfamiliar ring of integers.

Definition 1.1.12. Define *norm* to be the map

$$N : \mathbb{Z}\left[i\sqrt{k}\right] \to \mathbb{Z}_{\geq 0} : a + i\sqrt{k}b \mapsto a^2 + kb^2 = \left(a + i\sqrt{k}b\right)\left(a - i\sqrt{k}b\right).$$

Proposition 1.1.13. The norm map satisfies $N(\alpha) = 0 \iff \alpha = 0$, $N(\alpha\beta) = N(\alpha)N(\beta)$ and $N(\alpha) = 1 \iff \alpha \in \mathbb{Z}\left[i\sqrt{k}\right]^\times$.

Proof. The first two are clear since $N(\alpha) = \alpha\overline{\alpha}$. Now if $N(\alpha) = 1$ then $\alpha^{-1} = \overline{\alpha}N(\alpha)^{-1} = \overline{\alpha}$, and if $\alpha \in \mathbb{Z}\left[i\sqrt{k}\right]^\times$ then $N(\alpha\alpha^{-1}) = 1 = N(\alpha)N(\alpha^{-1})$, so $N(\alpha) \in \mathbb{Z}^\times = \{\pm 1\}$, hence $N(\alpha) = 1$. □

Lemma 1.1.14. $\alpha \in \mathbb{Z}\left[i\sqrt{3}\right]$ cannot have norm 2.

Proof. Indeed, $N\left(a + i\sqrt{3}b\right) = a^2 + 3b^2 = 2$ has no solutions. □

Example 1.1.15. Continuing the last example, the three elements are indeed irreducible: if $2 = \alpha\beta$ then $N(2) = N(\alpha)N(\beta) = 4$, so by the lemma above one has WLOG $N(\alpha) = 1$ so $\alpha \in \mathbb{Z}\left[i\sqrt{3}\right]^{\times}$. Similar for $1 \pm i\sqrt{3}$. And note that $2 \nmid 1 \pm i\sqrt{3}$.

Week 2, lecture 3, 15th January

1.2 Euclidean domains

Definition 1.2.1. A domain R is an *Euclidean domain* if there is a map $\phi : R\backslash\{0\} \to \mathbb{Z}_{>0}$ such that $\forall a, b \in R\backslash\{0\}$:

1. $\phi(a) \leq \phi(ab)$
2. $\exists q, r \in R$ such that $b = qa + r$ with either $r = 0$ pr $\phi(r) < \phi(a)$.

Remark 1.2.2.

- Sometimes in the definition of Euclidean domains, ϕ is allowed to have value 0, but given such a ϕ, we have $\widetilde{\phi} = n^{\phi}$ for any $n > 1$ satisfying our definition.
- Technically, the first condition was not necessary, since given ϕ satisfying the second, $\widetilde{\phi}$ given by $a \mapsto \min_{b \in R\backslash\{0\}} \phi(ab)$ satisfies the first by construction.

Example 1.2.3.

1. $\mathbb{Z}$ is a Euclidean domain with ϕ given by the absolute value
2. For any field k, the polynomial ring $k[x]$ is a Euclidean domain: fix $n > 1$ and define $\phi = n^{\deg}$ where deg is the usual degree

Definition 1.2.4. The *Gaussian integers* are $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ which is a subring of $\mathbb{C}$.

Theorem 1.2.5. The norm N gives a ϕ satisfying the above definition, so $\mathbb{Z}[i]$ is a Euclidean domain.

Proof. For $a, b \in \mathbb{Z}[i]$, write $z = \frac{b}{a}$. Then $\exists q \in \mathbb{Z}[i] : |z - q| \leq \frac{\sqrt{2}}{2}$. (Think of the lattice). Now let $r = b - qa$, then $N(r) = N(b - qa) = N(a)N(z - q) < N(a)$. □

Theorem 1.2.6. Every Euclidean domain is a PID (hence a UFD).

Proof. Let $I \subset R$ be an ideal of a Euclidean domain R. If $I = 0$ then we're done. If $I \neq 0$, take $a \in I$ such that $\phi(a)$ is minimal. For a contradiction, suppose $\exists b \in I\backslash(a)$, then in particular $a \nmid b$, so $\exists q, r \in R : b = qa + r$ with $\phi(r) < \phi(a)$, but $r = b - qa \in I$. □

Remark 1.2.7. Note that the proof of 1.2.5 relies on the lattice of $\mathbb{Z}[i]$, which makes sure that any point in the ambient complex plane is close enough (to be precise, distance is less than 1) to a point on $\mathbb{Z}[i]$. The maximal such distance on the lattice $\mathbb{Z}\left[i\sqrt{k}\right]$ is $\sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{k}}{2}\right)^2} = \frac{\sqrt{1+k}}{2}$, hence by the same proof, $\mathbb{Z}\left[i\sqrt{k}\right]$ is a Euclidean domain for $k < 3$.

Definition 1.2.8. Let R be a domain with field of fractions K. We say R is *integrally closed* if for every monic $f \in R[x]$ and $\frac{a}{b} \in K$, we have $f\left(\frac{a}{b}\right) = 0 \implies \frac{a}{b} \in R$.

Lemma 1.2.9. Every UFD is integrally closed.

Proof. Let R be a UFD with field of fractions K. Take $\frac{a}{b} \in K$ such that

$$\exists a_0, \ldots, a_{n-1} \in R : \left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 = 0,$$

and (up to unit) a and b have no common factor (we can do this since R is a UFD). Then we have

$$a^n = -b(a_{n-1}a^{n-1} + \cdots + a_0 b^{n-1}),$$

so $b \mid a^n$, hence our assumption forces $b \in R^{\times}$, so $\frac{a}{b} \in R$ as desired. □

Corollary 1.2.10. $\mathbb{Z}\left[i\sqrt{k}\right]$ is not an Euclidean domain for $k > 0$ with $k \equiv 3 \bmod 4$.

Proof. We show that such $\mathbb{Z}\left[i\sqrt{k}\right]$ is not integrally closed, hence not a UFD, so not an Euclidean domain: take $\sqrt{1 + i\sqrt{k}}2 \notin \mathbb{Z}\left[i\sqrt{k}\right]$, which is a root of $x^2 - x + \frac{1+k}{4} \in \mathbb{Z}\left[i\sqrt{k}\right][x]$. □

Week 3, lecture 1, 20th January

2 Algebraic integers

Lemma 2.0.1 (Gauss)**.** If $g, h \in \mathbb{Q}[x]$ are monic polynomials with $gh \in \mathbb{Z}[x]$, then $gh \in \mathbb{Z}[x]$.

Definition 2.0.2. $\alpha \in \mathbb{C}$ is *algebraic* if $\exists f \neq 0 \in \mathbb{Q}[x] : f(\alpha) = 0$.

α is an *algebraic integer* if $\exists$ monic $f \neq 0 \in \mathbb{Z}[x] : f(x) = 0$.

Definition 2.0.3. Given an algebraic element α, consider $I = \{f \in \mathbb{Q}[x] : f(\alpha) = 0\} \subset \mathbb{Q}[x]$. Clearly this is is an ideal, and since $\mathbb{Q}[x]$ is a PID, write $I = (m_\alpha)$ where m_α is monic and called the *minimal polynomial* of α.

Proposition 2.0.4. Let $\alpha \in \mathbb{C}$ be an algebraic element with minimal (monic) polynomial $m_\alpha \in \mathbb{Q}[x]$. Then α is an algebraic integer iff $m_\alpha \in \mathbb{Z}[x]$.

Proof. The $\Longleftarrow$ follows immediately from definition.

Conversely, suppose α is an algebraic integer and let $f \in \mathbb{Z}[x]$ be monic with $f(\alpha) = 0$. By definition of minimal polynomial, $\exists g \in \mathbb{Q}[x] : f = g m_\alpha$. Since f, m_α are monic, g is monic, so by Gauss lemma, $g, m_\alpha \in \mathbb{Z}[x]$. □

Example 2.0.5. Let $\alpha \in \mathbb{Q}$, then $m_\alpha(x) = x - \alpha$, so α is an algebraic integer iff $\alpha \in \mathbb{Z}$, i.e. the algebraic integers of rationals are exactly the (usual) integers.

2.1 Quadratic numbers

Definition 2.1.1. $\alpha \in \mathbb{C}$ is a *quadratic integer* if $m_\alpha \in \mathbb{Z}[x]$ and has degree 2.

Any quadratic integer lies in a quadratic field $\mathbb{Q}\left(\sqrt{d}\right) = \left\{a + b\sqrt{d} : a, b \in \mathbb{Q}\right\}$.

Recall that if $d \in \mathbb{Z}, d \neq 0, 1, -1$ is square free, then $\mathbb{Q}\left(\sqrt{d}\right) \supsetneq \mathbb{Q}$ and if $d_1 \neq d_2$ satisfy the same conditions, then $\mathbb{Q}\left(\sqrt{d}_1\right) \neq \mathbb{Q}\left(\sqrt{d}_2\right)$. We now want to understand algebraic integers in $\mathbb{Q}\left(\sqrt{d}\right)$.

Definition 2.1.2. Define the *trace* function by $\operatorname{tr} : \mathbb{Q}\left(\sqrt{d}\right) \to \mathbb{Q} : \alpha \mapsto \alpha + \overline{\alpha}$.

Note that if $\alpha \in \mathbb{Q}\left(\sqrt{d}\right)$, then $p(x) = x^2 - \operatorname{tr}(\alpha)x + N(\alpha) \in \mathbb{Q}[x]$ is a polynomial that vanishes at α. If $\alpha \notin \mathbb{Q}$, then $p(x) = m_\alpha(x)$, hence α is an algebraic integer iff $\operatorname{tr}(\alpha), N(\alpha) \in \mathbb{Z}$, i.e. if one writes $\alpha = a + \sqrt{d}b$, then the conditio nis $2a, a^2 - db^2 \in \mathbb{Z}$.

Write $a' = 2a, b' = 2b$. Then $a' \in \mathbb{Z}$, and $a'^2 - db'^2 = 4a^2 - d4b^2 \in 4\mathbb{Z}$. But then in particular $db'^2 \in \mathbb{Z}$, and since d is squarefree, $b' \in \mathbb{Z}$. Modulo 4 we have $a'^2 \equiv db'^2 \bmod 4$, so:

1. If a' is even then $db' \equiv 0 \bmod 4$, but d is squarefree, so b' is even as well, hence $a, b \in \mathbb{Z}$, then α is an algebraic integer;
2. or, if a' is odd, then $db' \equiv 1 \bmod 4$ hence b' can't be even, so b' is odd as well and $b'2 \equiv 1 \bmod 4$, hence $d \equiv 1 \bmod 4$.

We therefore found that algebraic integers of $\mathbb{Q}\left(\sqrt{d}\right)$ are

$$\mathcal{O}_d = \begin{cases} \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\} = \mathbb{Z}\left[\sqrt{d}\right] & \text{if } d \neq 1 \bmod 4 \\ \left\{\dfrac{a' + b'\sqrt{d}}{2} : a', b' \in \mathbb{Z}, a' \equiv b' \bmod 2\right\} = \mathbb{Z}\left[\dfrac{1 + \sqrt{d}}{2}\right] & \text{if } d = 1 \bmod 4 \end{cases}$$

2.2 Algebraic integers in $\mathbb{C}$ form a ring

Proposition 2.2.1. Let $\alpha \in \mathbb{C}$. The following are equivalent.

1. α is an algebraic integer
2. $\mathbb{Z}[\alpha]$ is finitely generated as an additive abelian group
3. $\exists$ a nonzero, finitely generated subgroup $M \subset \mathbb{C} : \alpha \cdot M \subset M$.

Remark 2.2.2. 1. We usually say $\mathbb{Z}[\alpha]$ is defined to be the smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and α, but it can also be formally described as $\{f(\alpha) : f \in \mathbb{Z}[x]\}$, or the image of the evaluation map $\mathbb{Z}[x] \to \mathbb{C} : x \mapsto \alpha$.

2. An abelian group M is finitely generated if $\exists m_1, \dots, m_n \in M : \forall m \in M, m = \lambda_1 m_1 + \cdots + \lambda_n m_n, \lambda_i \in \mathbb{Z}$.

Proof of 2.2.1. $1 \implies 2$: let $a_0, \dots, a_{n-1} \in \mathbb{Z}$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0. \tag{$*$}$$

We want to show that $\{1, \alpha, \dots, \alpha^{n-1}\}$ generates $\mathbb{Z}[\alpha]$ as an abelian group. We know $\{\alpha^k : k \in \mathbb{N}\}$ surely generates $\mathbb{Z}[\alpha]$. It now suffices to show α^K can be expressed as a $\mathbb{Z}$-linear combination of $\{1, \dots, \alpha^{n-1}\}$ if $k \geq n$. We prove this by induction on k. If $k = n$ then the desired is immediate from $(*)$. Now suppose $\alpha^k = \sum_{i=0}^{n-1} c_i \alpha^i$, $c_i \in \mathbb{Z}$. Then

$$\alpha^{k+1} = \sum_{i=0}^{n-2} c_i \alpha^{i+1} + c_{n-1}\alpha^n = \sum_{i=0}^{n-2} c_i \alpha^{i+1} + c_{n-1}(-a_{n-1}\alpha^{n-1} - \cdots - a_0).$$

$2 \implies 3$: One has $\alpha\mathbb{Z}[\alpha] \subset \mathbb{Z}[\alpha]$.

$3 \implies 1$: let $m_1, \dots, m_n$ be generators of M and $\alpha M \subset M$. Then $\alpha m_i = \sum_{j=1}^n a_{ij} m_j$, $a_{ij} \in \mathbb{Z}$. Let $A = (a_{ij}) \in M_{n \times n}(\mathbb{Z})$. Then there is a surjective ring morphism $p : \mathbb{Z}^n \to M : \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum_i a_i m_i$ and for every $a \in \mathbb{Z}^n$ we have $\alpha p(a) = \alpha \left(\sum_{i=0}^n a m_i \right) p(Aa)$.

We claim that $\forall f \in \mathbb{Z}[x]$, one has $f(\alpha)p(a) = p(f(\alpha)a)$.

Consider the characteristic (monic) polynomial $\chi_A(x) = \det(xI - A) \in \mathbb{Z}[x]$ of A. By Cayley–Hamilton, $\chi_A(A) = 0$, then $\chi_A(\alpha)M = 0$ since each $m \in M$ is some $p(a)$, so (if we believe the claim) $\chi_A(\alpha)p(a) = p(\chi_A(\alpha)a) = 0$. But since $M \neq 0$, it must be $\chi_A(\alpha) = 0$, so α is an algebraic integer.

Week 3, lecture 2, 21st January

It remains to prove the claim. Note that we do have

$$\alpha p(b) = \sum_{i=1}^n \alpha m_i b_i = \sum_{i,j=1}^n a_{ij} m_j b_i = \sum_{j=1}^n \left(\sum_{i=1}^k a_{ij} b_i \right) m_j = p(Ab).$$

Since p is a ring morphism, we have $\lambda p(b) = p(\lambda b) \forall \lambda \in \mathbb{Z}$, and for any $n \in \mathbb{Z}_{>0}$, we have $\alpha^n p(b) = \alpha^{n-1}\alpha p(b) = \alpha^{n-1} p(Ab) = \cdots = p(A^n b)$, hence the claim is proved. □

Theorem 2.2.3. 1. If α, β are algebraic integers, then so are $\alpha + \beta, \alpha - \beta, \alpha\beta$.

2. If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in \mathbb{C}$ algebraic integers, then every root of f is an algebraic integer.

Remark 2.2.4. 1. Denote the set of algebraic integers of $\mathbb{C}$ by $\overline{\mathbb{Z}}$. 1 is telling us that $\overline{\mathbb{Z}}$ is a ring.

2. 2 is telling us that we don't get anything new if we consider roots of monic polynomials whose coefficients are algebraic integers.

Proof of 2.2.3. 1. Consider $\mathbb{Z}[\alpha, \beta] = \left\{ \sum a_{ij} \alpha^i \beta^j : a_{ij} \in \mathbb{Z} \right\}$, which is generated as an abelian group by $\left\{ \alpha^i, \beta^j : i, j \geq 0 \right\}$. If α satisfies a monic polynomial with integer coefficients of degree n and β of m, then $\left\{ \alpha^i \beta^j : 0 \leq i \leq n, 0 \leq j \leq m \right\}$ generates $\mathbb{Z}[\alpha, \beta]$ by the same argument in the proof of 2.2.1. Now for any $\gamma \in \mathbb{Z}[\alpha, \beta]$, we have $\gamma \mathbb{Z}[\alpha, \beta] \subset \mathbb{Z}[\alpha, \beta]$, so γ is an algebraic integer, so in particular $\alpha + \beta, \alpha - \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$ are algebraic integers.

2. Let $\alpha \in \mathbb{C}$ such that $\exists a_{n-1}, \dots, a_0 \in \mathbb{C}$ algebraic integers such that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. Consider $\mathbb{Z}[a_0, \dots, a_{n-1}, \alpha]$, which is again finitely generated by our familiar argument. Clearly $\alpha \mathbb{Z}[a_0, \dots, a_{n-1}, \alpha] \subset \mathbb{Z}[a_0, \dots, a_{n-1}, \alpha]$, so α is an algebraic integer.

□

2.3 Number fields

Definition 2.3.1. By *number field*, we mean a subfield $K \subset \mathbb{C}$ which is finitely dimensional as a $\mathbb{Q}$-vector space. This dimension is called the *degree* of K and denoted by $[K : \mathbb{Q}]$.

Example 2.3.2. Given an algebraic integer $\alpha \in \mathbb{C}$ we have the number field $\mathbb{Q}(\alpha)$, the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and α. If m_α has a degree n, then $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a basis of K as a $\mathbb{Q}$-vector space, and hence $[K : \mathbb{Q}] = n$. This together with primitive element theorem (see Galois theory) makes things easier.

Definition 2.3.3. Given a number field K, we denote the set of algebraic integers in K by $\mathcal{O}_K$ $(= \overline{\mathbb{Z}} \cap K)$ and call it the *ring of integers* of K.

Remark 2.3.4. Note that the field of fractions of $\mathcal{O}_K$ is precisely K. It's enough to show that $\forall \alpha \in K$, $\exists \lambda \in \mathbb{Z}$: $\lambda\alpha \in \mathcal{O}_K$. This implies $\operatorname{Frac}(\mathcal{O}_K) \supset \mathcal{O}_K$, and the other inclusion is trivial.

Let $\alpha \in K$. Then $\exists a_0, \dots, a_{n-1} \in \mathbb{Q} : \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. Let $\lambda = \operatorname{lcm}(a_{n-1}, a_0)$, then $p(x) = x^b + \lambda(a_{n-1}x^{n-1} + \cdots + a_0) \in \mathbb{Z}[x]$ and $p(\lambda\alpha) = 0$, so $\lambda\alpha$ is an algebraic integer.

Proposition 2.3.5. If K is a number field, then $\mathcal{O}_K$ is integrally closed.

Proof. This follows immediately from 2.2.3.2. □

Corollary 2.3.6. Let K be a number field $\mathcal{O} \subset \mathcal{O}_K$ any subring with $\operatorname{Frac}(\mathcal{O}) = K$. Then $\mathcal{O} \subsetneq \mathcal{O}_K$ is not integrally closed.

Proof. Take $\alpha \in \mathcal{O}_K \backslash \mathcal{O}$, then it satisfies a monic $f \in \mathbb{Z}[x] \subset \mathcal{O}[x]$. □

Definition 2.3.7 (Formal definition of norm and trace)**.** Let K be a number field. For $\alpha \in K$, consider the map $\operatorname{mult}_\alpha : K \to K : x \mapsto \alpha x$ as an endomorphism of $\mathbb{Q}$-vector spaces. Define $N_K(\alpha) = \det \operatorname{mult}_\alpha$ and $\operatorname{tr}_K(\alpha) = \operatorname{tr} \operatorname{mult}_\alpha$.

This doesn't depend on choice of basis of K.

Remark 2.3.8 (Properties of norm and trace that follow from definition)**.** 1. $\forall \lambda \in \mathbb{Q}$, $\operatorname{tr}_K(\lambda a) = \lambda \operatorname{tr}_K(a)$

2. $\forall \alpha, \beta \in K$, $\operatorname{tr}_K(\alpha + \beta) = \operatorname{tr}_K(\alpha) + \operatorname{tr}_K(\beta)$
3. $\forall \alpha, \beta \in K$, $N_K(\alpha\beta) = N_K(\alpha)N_K(\beta)$

Exercise 2.3.9. Verify that this formal definition matches the definitions we gave earlier for $K = \mathbb{Q}\left(\sqrt{d}\right)$.

Example 2.3.10. Let $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$. Compute $\operatorname{tr}_K\left(\sqrt[3]{2}\right)$ and $N_K\left(\sqrt[3]{2}\right)$.

Let $1, \sqrt[3]{2}, \sqrt[3]{4}$ be a basis of K. Then $\operatorname{mult}_{\sqrt[3]{2}}$ corresponds to the matrix $\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ with trace 0 and determinant 2.

Proposition 2.3.11. Let $\alpha \in \mathbb{C}$ be an algebraic number with $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then $\operatorname{tr}_{\mathbb{Q}(\alpha)}(\alpha) = -a_{n-1}$ and $N_{\mathbb{Q}(\alpha)}(\alpha) = (-1)^n a_0$.

Proof. Take the basis $1, \alpha, \dots, \alpha^{n-1}$ for $\mathbb{Q}(\alpha)$ and write $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. Then $\operatorname{mult}_\alpha$ corresponds to the matrix $\begin{pmatrix} 0 & 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & 0 & -a_1 \\ 0 & 1 & 0 & 0 & -a_2 \\ 0 & & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$, from which we can read off the desired result. □

Remark 2.3.12. If α is an algebraic integer, then $m_\alpha \in \mathbb{Z}[x]$ so in particular $\operatorname{tr}_{\mathbb{Q}(\alpha)}(\alpha), N_{\mathbb{Q}(\alpha)}(\alpha) \in \mathbb{Z}$.

Week 3, lecture 3, 22nd January

Lemma 2.3.13 (Tower law)**.** Let $K \subset L \subset M$ be inclusion of fields and suppose $[M : L], [L : K]$ are finite. Then $[M : K] = [M : L][L : K]$. More precisely, if $\alpha_1, \dots, \alpha_n$ is a basis for L as a K-vector space and $\beta_1, \dots, \beta_m$ a basis for M as a L-vector space, then $\alpha_i\beta_j : 1 \le i \le n, 1 \le j \le m$ is a basis for M as a K-vector space.

Proof. Omitted. □

Proposition 2.3.14. Let K be a number field. For $\alpha \in K$, we have $\operatorname{tr}_K(\alpha) = |K : \mathbb{Q}(\alpha)| \operatorname{tr}_{\mathbb{Q}(\alpha)}(\alpha)$ and $N_K(\alpha) = N_{Q(\alpha)}(\alpha)^{|K:\mathbb{Q}(\alpha)|}$.

Proof. Write $n = \deg m_\alpha = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $m = [K : \mathbb{Q}(\alpha)]$. Let $\beta_1, \dots, \beta_m$ be a basis of K as a $\mathbb{Q}(\alpha)$-vector space. By the tower law,

$$\beta_1, \alpha\beta_1, \dots, \alpha^{n-1}\beta_1, \beta_2, \dots, \dots, \dots, \alpha^{n-1}\beta_m$$

is a basis of K as a $\mathbb{Q}$-vector space. Then $\forall i = 1, \dots, m$, the subspace spanned by $\beta_i, \alpha\beta_i, \dots, \alpha^{n-1}\beta_i$ is closed under $\operatorname{mult}_\alpha$, moreover, on these subspaces, the matrix again has the form $\begin{pmatrix} 0 & 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & 0 & -a_1 \\ 0 & 1 & 0 & 0 & -a_2 \\ 0 & & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$, and so the matrix of $\operatorname{mult}_\alpha$ on the whole K has a block diagonal form with m blocks. □

Recall that an abelian group can be alternatively thought as a $\mathbb{Z}$-module, and we say $\mathbb{Z}$-module is free of rank n if it's isomorphic (as $\mathbb{Z}$-modules, or as abelian groups) to $\mathbb{Z}^n$.

Theorem 2.3.15 (Structure theorem, weak form)**.** Let M be a free $\mathbb{Z}$-module of rank n and $M' \subset M$ a submodule. Then M' is free of rank $q \leq n$.

Proof. We prove by induction on n. By assumption $M \cong \mathbb{Z}^n$, so WLOG suppose $M = \mathbb{Z}^n$. For every i, define $p_i : \mathbb{Z}^n \to \mathbb{Z}$ to be the projection into the ith coordinate. If $M' = 0$ then we are done, so suppose $M' \neq 0$, then $\exists i : p_i(M') \neq 0$, so $\exists \beta \in \mathbb{Z} : p_i(M') = \beta$. This means $\exists b \in M' : (\beta) = (p_i(b))$. Write $N = \ker p_i$. We claim $M' = b\mathbb{Z} \oplus M' \cap N$. Note that $M' \cap N \subset N \cong \mathbb{Z}^{n-1}$, so by inductive hypothesis $M' \cap N$ is free of rank $\leq n - 1$. Clearly $b\mathbb{Z}$ is free of rank 1, so it remains to prove the direct sum.

First observe that $b\mathbb{Z} \cap (M' \cap N) = \{0\}$. Indeed, if $m \in b\mathbb{Z}$ then $m = bk$ for $k \in \mathbb{Z}$, but $m \in N$, so $p_i(m) = p_i(bk) = kp_i(b) = 0$, but we assumed $p_i(b) \neq 0$, so $k = 0$ and $m = 0$.

Now let $m \in M'$. Then $p_i(m) \in p_i(M') = (p_i(b))$, so $p_i(m) = kp(b)$ for some $k \in \mathbb{Z}$. Hence $p_i(m - kb) = 0$, i.e. $m - kb \in M' \cap N$. □

Theorem 2.3.16 (Structure theorem, strong form)**.** Let M be a free $\mathbb{Z}$-module of rank n and let $M' \subset M$ be a submodule. If M' is not zero, then there is a basis $\{e_1, \dots, e_n\}$ of M and $a_1, \dots, a_q \in \mathbb{Z} \backslash \{0\}$ with $q \leq n$ such that $\{a_1 e_1, \dots, a_q e_q\}$ is a basis for M' as $\mathbb{Z}$-module and $a_1 \mid a_2 \mid \cdots \mid a_q$.

Theorem 2.3.17 (Smith normal form)**.** Let A be a nonzero $m \times n$ matrix with coefficients in $\mathbb{Z}$. Then $\exists S \in \mathrm{GL}_m(\mathbb{Z}), T \in \mathrm{GL}_n(\mathbb{Z}), r, d_1, \dots, d_r \in \mathbb{Z}_{>0}$ such that $SAT = \begin{pmatrix} \operatorname{diag}(d_1, \dots, d_r) & 0 \\ 0 & 0 \end{pmatrix}$ with $d_1 \mid \cdots \mid d_r$.

Lemma 2.3.18. Let $\alpha_1, \dots, \alpha_n \in K$ be a basis of K as a $\mathbb{Q}$-vector space. Then $\det A \neq 0$ where A is the matrix $(\operatorname{tr}_K(\alpha_i\alpha_j)_{ij})$.

Proof. Consider the linear transformation $A : \mathbb{Q}^n \to \mathbb{Q}^n$ associated to the matrix A. It's enough to show that A is injective by the rank–nullity theorem. Let $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in \ker A$, i.e. $Ac = 0$. The ith entry of Ac is

$$\sum_{j=1}^{n} \operatorname{tr}_K(\alpha_i\alpha_j)c_j = \sum_{j=1}^{n} \operatorname{tr}_K(\alpha_i\alpha_j c_j) = \operatorname{tr}_K\left(\sum_{j=1}^{n} c_j\alpha_i\alpha_j\right) = 0 \quad \forall i = 1, \dots, n$$

Denote $\sum_{j=1}^{n} c_j\alpha_j$ by α, then the above is $\operatorname{tr}_K(\alpha\alpha_i) = 0$. Let $\beta \in K$, then $\beta = d_1\alpha_1 + \cdots + d_n\alpha_n$, so $\operatorname{tr}_K(\alpha\beta) = \sum_{i=1}^{n} d_i \operatorname{tr}(\alpha\alpha_i) = 0$. But now take $\beta = \alpha^{-1}$, then $\operatorname{tr}_K(\alpha\beta) = \operatorname{tr}_K(1) = n$, a contradiction. So $\alpha = 0$ and hence $c_j = 0$ $\forall j = 1, \dots, n$ since α_j is linearly independent, i.e. $c = 0$. □

Theorem 2.3.19. Let K be a number field. Then as a group under addition, $\mathcal{O}_K$ is free of rank $[K : \mathbb{Q}]$.

Proof. Let $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ be a basis of K as a $\mathbb{Q}$-vector space. (We can do this by $\mathrm{Frac}(\mathcal{O}_K) = K$ so we can keep multiplying a basis of K by integers to make them in $\mathcal{O}_K$). Then every element $\alpha \in \mathcal{O}_K$ can be written as $c_1\alpha_1 + \dots + c_n\alpha_n$ for some $c_i \in \mathbb{Q}$. We want to bound denominators of c_i's. If we can do it then

$$\mathbb{Z}^n \subset \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n \subset \mathcal{O}_K \subset \mathbb{Z}\frac{\alpha_1}{d} \oplus \dots \oplus \mathbb{Z}\frac{\alpha_n}{d} \cong \mathbb{Z}^n,$$

so by the weak form of structure theorem, $\mathcal{O}_K$ is free of rank $\geq n$ and $\leq n$, so n.

By 2.3.18, $A = (\mathrm{tr}_K(\alpha_i\alpha_j)_{ij})$ is invertible, hence write $A\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$, i.e. $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A^{-1}\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$. Pick $d \in \mathbb{Z}$ such that $dA^{-1} \in M_n(\mathbb{Z})$. □

Week 4, lecture 1, 27th January: problem class (sheet 1)

Exercise 2.3.20. 1. Find all irreducible elements of $\mathbb{Z}\left[i\sqrt{2}\right]$. Characterise all integers n of the form $n = a^2 + 2b^2$.

Solution. We know that $\mathbb{Z}\left[i\sqrt{2}\right]$ is a Euclidean domain, so primes are precisely irreducibles. The main idea is to use the norm function $N : \mathbb{Z}\left[i\sqrt{2}\right] \to \mathbb{Z}_{\geq 0}$.

Recall that $\mathbb{Z}\left[i\sqrt{2}\right]^\times = \left\{\alpha \in \mathbb{Z}\left[i\sqrt{2}\right] : N(\alpha) = 1\right\} = \left\{a + i\sqrt{2}b : a, b \in \mathbb{Z}, a^2 + 2b^2 = 1\right\} = \{\pm 1\}$, and that N is multiplicative. We claim that (a) if $\alpha \in \mathbb{Z}\left[i\sqrt{2}\right]$ has $N(\alpha) = p$ for some prime p, then α is irreducible, and (b) $p \in \mathbb{Z}$ prime is reducible in $\mathbb{Z}\left[i\sqrt{2}\right] \iff \exists \alpha \in \mathbb{Z}\left[i\sqrt{2}\right] : N(\alpha) = p$.

(a): Write $\alpha = \beta\gamma$ where $\beta, \gamma \in \mathbb{Z}\left[i\sqrt{2}\right]$, then $p = N(\alpha) = N(\beta)N(\gamma) \in \mathbb{Z}$, so either $N(\beta)$ or $N(\gamma) = 1$, hence either β or γ is a unit, i.e. α is irreducible.

(b): Suppose p is reducible, then write $p = \beta\gamma$ where $N(\beta), N(\gamma) \neq 1$, but then $p^2 = N(p) = N(\beta)N(\gamma)$, so $N(\beta) = N(\gamma) = p$. Now suppose $N(\alpha) = p$, then $p = \alpha\overline{\alpha}$ where $N(\overline{\alpha}) = N(\alpha) = p$, hence p is reducible.

Now $\exists \alpha : N(\alpha) = p \iff \exists a, b \in \mathbb{Z} : a^2 + 2b^2 = p$. Note that p cannot divide a and b both since if so then $p^2 \mid a^2 + 2b^2 = p$, a contradiction, hence we have $a^2 + 2b^2 \equiv 0 \bmod p$, i.e. $-2 \equiv \left(\frac{a}{b}\right)^2 \bmod p$. This only happens if $p \equiv 1, 3 \bmod 8$. Conversely, suppose $p \equiv 1, 3 \bmod 8$, then -2 is a square mod p, i.e. $\exists x \in \mathbb{Z} : -2 \equiv x^2 \bmod p$, so $x^2 + 2 \equiv 0 \bmod p$, hence $p \mid x^2 + 2 = \left(x + i\sqrt{2}\right)\left(x - i\sqrt{2}\right)$, and clearly $p \nmid x \pm i\sqrt{2}$ since $\frac{x + i\sqrt{2}}{p} \notin \mathbb{Z}\left[i\sqrt{2}\right]$, so p is not prime, thus p is reducible.

From the above we can make a list of irreducibles of $\mathbb{Z}\left[i\sqrt{2}\right]$:

- $p = 2$, then $p = N(i\sqrt{2})$, so $i\sqrt{2}$ is irreducible
- p is an odd prime and $p \equiv 5, 7 \bmod 8$, then p is irreducible
- p is an odd prime and $p \equiv 1, 3 \bmod 8$, then $\exists \alpha \in \mathbb{Z}\left[i\sqrt{2}\right] : N(\alpha) = N(\overline{\alpha}) = p = \alpha\overline{\alpha}$, so $\alpha, \overline{\alpha}$ are irreducible

We just proved that an odd prime p can be written as $p = a^2 + 2b^2$ iff $p =\equiv 1, 3 \bmod 8$, and if $p \equiv 5, 7 \bmod 8$ then p^2 can be written in the same form. But using that the norm is multiplicative, we conclude that n can be written in the same form iff $\forall p \mid n$ with $p \equiv 5, 7 \bmod 8$, we have $p^2 \mid n$.

2. Show that $\mathcal{O} = \mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$ is not Euclidean by these steps:

(a) Assume that a Euclidean norm $\lambda : \mathcal{O}\backslash\{0\} \to \mathbb{Z}_{>0}$ such that $\lambda(a) \leq \lambda(ab)$ $\forall a, b \in \mathcal{O}$ exists. Describe the set of elements in $\mathcal{O}\backslash\{0\}$ for which λ is minimal.

(b) Compute $\mathcal{O}^\times$.

(c) Show that 2 and 3 are irreducible.

(d) For $a \in \mathcal{O}\backslash\{0\}$ such that $\lambda(a)$ is the second smallest value, describe $\mathcal{O}/a\mathcal{O}$.

(e) Deduce $a \mid 2$ or $a \mid 3$ a reach a contradiction.

Solution.

(a) We claim this is precisely $\mathcal{O}^\times$. Note that $1a = a$, so $\lambda(1) \leq \lambda(a)$ $\forall a \in \mathcal{O}$, and $\lambda(1) = 1$, but $\lambda(u) = 1 \iff u \in \mathcal{O}^\times$.

(b) One has

$$\mathcal{O}^\times = \{\alpha \in \mathcal{O} : N(\alpha) = 1\} = \left\{\frac{a + bi\sqrt{19}}{2} : a, b \in \mathbb{Z}, \frac{a^2 + 19b^2}{4} = 1\right\} = \{\pm 1\}.$$

(c) If 2 is not irreducible, then $\exists \alpha \in \mathcal{O} : N(\alpha) = 2$, but $a^2 + 19b^2 = 2$ has no integer solutions. Same for 3.

(d) Take $b \in \mathcal{O}$ and write $b = aq + r$ with the condition: either $r = 0$ or $\lambda(r) < \lambda(a)$ (possible by definition of Euclidean norm), but then by definition of a we have $\lambda(r) = 1$, so $\mathcal{O}/a\mathcal{O} = \{0, \pm 1\}$, hence $\mathcal{O}/a\mathcal{O}$ is either $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}$.

(e) If $\mathcal{O}/a\mathcal{O} = \mathbb{Z}/2\mathbb{Z}$, then $2 \mid a$, and if $\mathcal{O}/a\mathcal{O} = \mathbb{Z}/3\mathbb{Z}$ then $3 \mid a$. But we claim $\mathcal{O}/2\mathcal{O}$ has 4 elements, contradicting that $\mathcal{O}/a\mathcal{O} \twoheadrightarrow \mathcal{O}/2\mathcal{O}$ surjectively. Consider $\mathcal{O}$ as $\mathbb{Z}[x]/(x^2 - x - 5)$. But then $\mathcal{O}/2\mathcal{O} = \mathbb{Z}[x]/(x^2 - x - 5, 2) = \mathbb{Z}[x]/(x^2 + x + 1, 2) = \{c + dx : c, d \in \mathbb{Z}/2\mathbb{Z}\}$, which has 4 elements as claimed. Same for $\mathcal{O}/3\mathcal{O}$.

Week 4, lecture 2, 28th January

Definition 2.3.21. Let K be a number field. An *embedding* of K is a ring homomorphism $\tau : K \to \mathbb{C}$. Write Σ_K for the set of embeddings of K.

Remark 2.3.22. 1. Recall that homomorphisms of fields are automatically injective.

2. We defined number fields as subfields $K \subset \mathbb{C}$ finitely generated over $\mathbb{Q}$. Hence $\mathrm{incl} : K \hookrightarrow \mathbb{C}$ is an embedding.

Proposition 2.3.23. Let α be algebraic with $m_\alpha(x)$ of degree n. Then $\left|\Sigma_{\mathbb{Q}(\alpha)}\right| = n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Moreover, for each distinct roots $\alpha_1, \ldots, \alpha_n$ of $m_\alpha(x)$, there is an embedding $\tau_i : \mathbb{Q}(\alpha) \to \mathbb{C} : \alpha \mapsto \alpha_i$.

Proof. Recall that $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(m_\alpha(x))$, and since m_α is by definition irreducible, it's separable, i.e. it has $\deg m_\alpha = n$ distinct roots.

To give a ring homomorphism from $\mathbb{Q}(\alpha)$ to $\mathbb{C}$ is precisely giving the image of x of the map $\mathbb{Q}[x]/(m_\alpha(x)) \xrightarrow{\phi} \mathbb{C}$ (since it must map 1 to 1, it's identity on $\mathbb{Q}$). But since $\ker \phi = (m_\alpha(x))$, it follows that $\phi(m_\alpha(x))$, and since ϕ is a homomorphism, $m_(\alpha)(\phi(x)) = 0$, hence $\phi(x)$ can only be one of the n roots of m_α. □

Example 2.3.24. If $K = \mathbb{Q}\left(\sqrt{d}\right)$, then $m_{\sqrt{d}}(x) = x^2 - d$ which has roots $\pm\sqrt{d}$, hence

$$\Sigma_{\mathbb{Q}(\sqrt{d})} = \left\{\tau_1 : \mathbb{Q}\left(\sqrt{d}\right) \to \mathbb{C} : \sqrt{d} \mapsto \sqrt{d}, \quad \tau_2 : \mathbb{Q}\left(\sqrt{d}\right) \to \mathbb{C} : \sqrt{d} \mapsto -\sqrt{d}\right\}.$$

Remark 2.3.25. Recall that if $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then $\mathrm{tr}_{\mathbb{Q}(\alpha)}(\alpha) = -a_{n-1}$ and $N_{\mathbb{Q}(\alpha)}(\alpha) = (-1)^n a_0$, but if we factorise $m_\alpha(x)$ and write it as $\prod_{i=1}^n (x - \alpha_i)$, then

$$\mathrm{tr}_{\mathbb{Q}(\alpha)}(\alpha) = \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \tau_i(\alpha), \quad N_{\mathbb{Q}(\alpha)}(\alpha) = \prod_{i=1}^n \alpha_i = \prod_{i=1}^n \tau_i(\alpha).$$

We now want to do this for a general number field K instead of $\mathbb{Q}(\alpha)$.

Lemma 2.3.26. Let K be a number field and fix an embedding $\tau_0 : K \to \mathbb{C}$. Let α be algebraic, then there are $[K(\alpha) : K]$ embeddings $\tau : K(\alpha) \to \mathbb{C}$ that restrict to τ_0.

Proof. Omitted; very similar to proof of 2.3.23. □

Corollary 2.3.27. Let $K \subset L$ be number fields and $\tau_0 : K \to \mathbb{C}$ be an embedding. Then there are $|L : K|$ embeddings $\tau : L \to \mathbb{C}$ that restrict to τ_0.

Proof. We prove by induction on $[L : K]|$. If $[L : K] = 1$ then $L = K$ and there's nothing to prove. Now if $[L : K] > 1$, pick $\alpha \in L \backslash K$, then $K \subsetneq K(\alpha) \subset L$ and by the tower law, $[L : K(\alpha)] < [L : K]$. Then τ_0 extends to $[K(\alpha) : K]$ embeddings $\tau_1 : K(\alpha)) \to \mathbb{C}$ by 2.3.26, each of which extends to $[L : K(\alpha)]$ embeddings by the inductive hypothesis. □

Theorem 2.3.28. Let K be a number field. Then for $\alpha \in K$ we have

$$\mathrm{tr}_K(\alpha) = \sum_{\tau \in \Sigma_K} \tau(\alpha), \quad N_K(\alpha) = \prod_{\tau \in \Sigma_K} \tau(\alpha).$$

Proof. We already have $\mathrm{tr}_K(\alpha) = [K : \mathbb{Q}(\alpha)] \, \mathrm{tr}_{\mathbb{Q}(\alpha)}(\alpha)$, so

$$\mathrm{tr}_K(\alpha) = [K : \mathbb{Q}(\alpha)] \sum_{\tau_0 \in \Sigma_{\mathbb{Q}(\alpha)}} \tau_0(\alpha) = \sum_{\tau \in \Sigma_K} \sigma(\alpha)$$

since each $\tau_0 \in \Sigma_{\mathbb{Q}(\alpha)}$ extends to $[K : \mathbb{Q}(\alpha)]$ embeddings that agree with τ_0 on $\mathbb{Q}(\alpha)$, in particular on α, and K does have $[K : \mathbb{Q}(\alpha)] \left|\Sigma_{\mathbb{Q}(\alpha)}\right|$ by the primitive element theorem, tower law and 2.3.23.

Similarly for the norm. □

Proposition 2.3.29. Let K be a number field and $\alpha \in \mathcal{O}_K$. Then $\alpha \in \mathcal{O}_K^\times \iff N(\alpha) \in \mathbb{Z}^\times = \{\pm 1\}$.

Proof. If $\alpha \in \mathcal{O}_K^\times$, $\exists \beta \in \mathcal{O}_K : \alpha\beta = 1$, so $N(\alpha)N(\beta) = 1$ where $N(\alpha) \in \mathbb{Z}$ by 2.3.12, so $N(\alpha) = \pm 1$. (We didn't need the embeddings for this direction.)
Now if $N(\alpha) = \pm 1$, then

$$\prod_{\tau \in \Sigma_K} \tau(\alpha) = \alpha \prod_{\tau \in \Sigma_K \setminus \{\mathrm{id}\}} \tau(\alpha).$$

Now define $\beta = N(\alpha) \prod_{\tau \in \Sigma_K \setminus \{\mathrm{id}\}} \tau(\alpha) \in \mathcal{O}_K$ (since $\tau(\alpha)$ satisfy the minimal polynomial of α, which is an algebraic integer), then $\alpha\beta = N(\alpha)^1 = 1$. □

Week 4, lecture 3, 29th January

2.4 Discriminant and basis

Definition 2.4.1. Let K be a number field of degree $n = [K : \mathbb{Q}]$. Define the *discriminant* of $\alpha_1, \dots, \alpha_n \in K$ as

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(\operatorname{tr}_K(\alpha_i \alpha_j)_{ij}) \in \mathbb{Q}.$$

Example 2.4.2. Consider $K = \mathbb{Q}\left(\sqrt{d}\right)$ with $d \not\equiv 1 \bmod 4$. We calculate the discriminant of integral basis $\{1, \sqrt{d}\}$ of $\mathbb{Z}\left[\sqrt{d}\right]$:

$$\operatorname{disc}\left(1, \sqrt{d}\right) = \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Now $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ has integral basis $1, \frac{1+\sqrt{d}}{2}$. We calculate

$$\operatorname{disc}\left(1, \frac{1+\sqrt{d}}{2}\right) = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

Remark 2.4.3. We have seen (2.3.18) that if $\alpha_1, \dots, \alpha_n$ is a $\mathbb{Q}$-basis of a number field K then $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$, and clearly if $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ then $\operatorname{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.

Lemma 2.4.4. Suppose $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in K$ such that

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = S \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \quad S \in M_n(\mathbb{Q}),$$

then $\operatorname{disc}(\beta_1, \dots, \beta_n) = (\det S)^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n)$.

Proof. Write $A = (\operatorname{tr}_K(\alpha_i\alpha_j)_{ij})$, $B = (\operatorname{tr}_K(\beta_i\beta_j)_{ij})$ and $S = (s_ij)$, then

$$\operatorname{tr}_K(\beta_i\beta_j) = \sum_{k,l=1}^{n} s_{ik} \operatorname{tr}_K(\alpha_k\alpha_l) s_{jl},$$

i.e. $B = SAS^t$, so taking determinants on both sides gives the desired. □

Corollary 2.4.5. If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ and $\beta_1, \dots, \beta_n \in \mathcal{O}_K$ are $\mathbb{Z}$-basis of $\mathcal{O}_K$ as an abelian group, then $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \operatorname{disc}(\beta_1, \dots, \beta_n)$.

Proof. In this case, the change of basis matrix $S \in \mathrm{GL}_n(\mathbb{Z})$, so $\det S = \pm 1$. □

Definition 2.4.6. Define the *discriminant* of a number field K to be $D_K = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n$ is any $\mathbb{Z}$-basis of $\mathcal{O}_K$. More generally, for a free abelian subgroup G of $\mathcal{O}_K$, define $\operatorname{disc}(G)$ to be the discriminant of any of G's $\mathbb{Z}$-basis (allowed by 2.3.16).

Proposition 2.4.7. Suppose $M \subset N$ are free abelian subgroups of $\mathcal{O}_K$ of rank n. Then

$$\operatorname{disc}(M) = [N : M]^2 \operatorname{disc}(N).$$

(Note that $[N : M]$ denotes the index of M as a subgroup of N, and not degree of field extension).

Proof. Let $\alpha_1, \dots, \alpha_n$ be a basis of N and $d_1\alpha_1, \dots, d_n\alpha_n$ be a basis of M where $d_1, \dots, d_n \in \mathbb{Z}$. Then

$$\operatorname{disc}(M) = \det(\operatorname{tr}_K(d_i\alpha_i d_j\alpha_j))_{ij} = (d_i \cdots d_n)^2 \operatorname{disc}(N),$$

and since

$$N/M = \frac{\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n}{\mathbb{Z}d_1\alpha_1 \oplus \cdots \oplus \mathbb{Z}d_n\alpha_n} \cong \mathbb{Z}/d_n\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z},$$

one has $[N : M] = d_1 \cdots d_n$. □

Remark 2.4.8. In particular, if $M \subset \mathcal{O}_K$ is free of rank n, then $D_K \mid \operatorname{disc}(M)$. Also, if $p \mid [\mathcal{O}_K : M]$, then $p^2 \mid \operatorname{disc}(M)$. Most importantly, if $\operatorname{disc}(M)$ is squarefree, then $M = \mathcal{O}_K$. Hence, if $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ satisfies that $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$ is squareefree, then it is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

For example, we know that $1, \sqrt{d}$ is not a $\mathbb{Z}$-basis of $\mathbb{Z}\left[\sqrt{d}\right]$ if $d \equiv 3 \bmod 4$, and indeed as calculated before, $\operatorname{disc}\left(1, \sqrt{d}\right) = 4d$ is not squarefree.

Proposition 2.4.9. Let K be a number field with $\Sigma_K = \{\tau_1, \dots, \tau_n\}$. Then for $\alpha_1, \dots, \alpha_n \in K$,

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(\tau_i(\alpha_j)_{ij})^2.$$

Proof. Let $A = (\operatorname{tr}_K(\alpha_i\alpha_j)_{ij})$ and $T = (\tau_i(\alpha_j)_{ij})$. We have

$$\operatorname{tr}_K(\alpha_i\alpha_j) = \sum_{l=1}^{n} \tau_l(\alpha_i\alpha_j) = \sum_{l=1}^{n} \tau_l(\alpha_i)\tau_l(\alpha_j),$$

which is the i, jth entry of T^tT. □

Remark 2.4.10. Consider $K = \mathbb{Q}(\alpha)$ with $m_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. Take $1, \alpha, \dots, \alpha^{n-1}$ to be a $\mathbb{Q}$-basis of K. Then $\tau_1, \dots, \tau_n$ satisfy $\tau_i(\alpha) = \alpha_i$. Now suppose $\alpha = \alpha_1$, then

$$\operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) = \det \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix}^2 = \prod_{1 \le i, j \le n} (\alpha_i - \alpha_j)^2,$$

(recall the Vandermonde matrix).

Proposition 2.4.11.

$$\operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}(\alpha)}(m'_\alpha(\alpha)).$$

Proof. Note that

$$N_{\mathbb{Q}(\alpha)}(m'_\alpha(\alpha)) = \prod_{i=1}^{n} \tau_i(m'_\alpha(\alpha)) = \prod_{i=1}^{n} m'_\alpha(\tau_i(\alpha)) = \prod_{i=1}^{n} m'_\alpha(\alpha_i),$$

and the desired is clear if we write $m_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. □

3 Unique ideal factorisation

3.1 Prime ideals in $\mathcal{O}_K$

Definition 3.1.1. Let R be a ring. A subgroup under addition $I \subset R$ is an *ideal* if $ra \in I \ \forall r \in R, a \in I$.

Remark 3.1.2. Given an ideal $I \subset R$ we can form the quotient ring R/I. Denote the coset $r + I$ by $[r]$.

Definition 3.1.3. Given $S \subset R$, denote by (S) the smallest ideal containing S, or the ideal *generated* by S. Explicitly,

$$(S) = \left\{ \sum_i r_i s_i : r_i \in R, s_i \in S \right\}.$$

An ideal I is *principal* if one can write $I = (S)$ where $|S| = 1$.

Definition 3.1.4. Given $I, J \in R$ ideals, define $I + J = \{a + b : a \in I, b \in J\}$ and $IJ = \left\{\sum_i a_ib_i : a_i \in I, b_i \in J\right\} = (\{ab : a \in I, b \in J\})$. These two with $I \cap J$ are all ideals.

Definition 3.1.5. An ideal $I \subset R$ is *prime* if $ab \in I \implies a$ or $b \in I$.

Proposition 3.1.6. An ideal $I \subset R$ is prime $\iff R/I$ is a domain.

Example 3.1.7. Recall that $R = \mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD since $6 = 2 \times 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$. Now let $\mathfrak{p}_2 = \left(2, 1+\sqrt{-5}\right)$, $\mathfrak{p}_3 = \left(3, 1+\sqrt{-5}\right)$, $\overline{\mathfrak{p}_3} = \left(3, 1-\sqrt{-5}\right)$. We will see that $\mathfrak{p}_2^2 = (2)$ and $\mathfrak{p}_3\overline{\mathfrak{p}_3} = (3)$, and $\mathfrak{p}_2$ is a prime ideal. Also, $\mathfrak{p}_2$ is not principal; indeed, assume $\mathfrak{p}_2 = (\alpha)$ where $\alpha \in \mathbb{Z}\left[\sqrt{-5}\right]$, but then $\mathfrak{p}_2^2 = (\alpha^2) = (2)$, so $N(\alpha)^2 = N(2) = 4$, hence $N(\alpha) = 2$, but $a^2 + 5b^2 = 2$ has no $\mathbb{Z}$ solutions.

$\mathfrak{p}_2$ is prime: consider $\mathbb{Z}\left[\sqrt{-5}\right]$ as $\mathbb{Z}[t]/(t^2+5)$ by $\sqrt{-5} \to t$, then $\mathfrak{p}_2$ is $(2, 1+t)$ and so $\mathbb{Z}\left[\sqrt{-5}\right]/\mathfrak{p}_2$ is

$$\mathbb{Z}[t]/(t^2+5, 2, 1+t) = \mathbb{Z}/2\mathbb{Z}[t]/(t^2-1, t+1) = \mathbb{Z}/2\mathbb{Z}[t]/(t+1) = \mathbb{Z}/2\mathbb{Z},$$

which is a domain.

$\mathfrak{p}_3\overline{\mathfrak{p}_3} = (3)$: we prove the equality

$$\left(9, 3-3\sqrt{5}, 3+3\sqrt{6}\right) = (3).$$

Clearly $\left(9, 3-3\sqrt{5}, 3+3\sqrt{6}\right) \subset (3)$ since $9, 3-3\sqrt{5}, 3+3\sqrt{6} \in (3)$, and since $9-6=3$ we also have the other inclusion.

Week 5, lecture 1, 3rd February

Remark 3.1.8. Denote the ideal generated by $a_1, \ldots, a_n \in R$ by $(a_1, \ldots, a_n) \subset R$. Then note that

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_m) = (a_1, \ldots, a_n, b_1, \ldots, b_m)$$

and

$$(a_1, \ldots, a_n)(b_1, \ldots, b_m) = \left(\{a_i b_j\} : i = 1, \ldots, n, b = 1, \ldots, m\right).$$

3.2 Dedekind domains

Definition 3.2.1. A domain R is a *Dedekind domain* if

1. R is integrally closed;
2. Every nonzero prime ideal is maximal;
3. R is noetherian.

Lemma 3.2.2. Let $I \subset \mathcal{O}_K$ be a nonzero ideal. Then I has finite index in $\mathcal{O}_K$, i.e. $[\mathcal{O}_K : I] = |\mathcal{O}_K/I|$ is finite.

Proof. Let $0 \neq \alpha \in I$. Then $(N_K(\alpha)) \subset (\alpha) \subset I$. Indeed, we have $N_K(\alpha) = \alpha \prod_{\tau \neq \mathrm{id}} \tau(\alpha)$, so it suffices to show $\beta := \prod_{\tau \neq \mathrm{id}} \tau(\alpha) \in \mathcal{O}_K$, i.e. $\beta \in K$ and it's an algebraic integer. But this is clear since $\beta = \frac{N_K(\alpha)}{\alpha} \in K$ and it's a product of algebraic integers (homomorphisms preserve algebraic integers).

In particular, we now have $[\mathcal{O}_K : I] \leq [\mathcal{O}_K : (N_K(\alpha))]$. It suffices to show $\mathcal{O}_K/N$ is finite for any $N \neq 0 \in \mathbb{Z}$, but by 2.3.19 one has $\mathcal{O}_K \cong \mathbb{Z}^n$ so $\mathcal{O}_K/N \cong \mathbb{Z}^n/N \cong (\mathbb{Z}/N\mathbb{Z})^n$ which has size N^n, in particular finite. □

Proposition 3.2.3. If K is a number field, then $\mathcal{O}_K$ is a Dedekind domain.

Proof.

1. This follows immediately from definition of ring of integers: it's precisely roots of monic integer polynomials.
2. If $\mathfrak{p} \subset \mathcal{O}_K$ be a nonzero prime ideal, then $\mathcal{O}_K/\mathfrak{p}$ is a finite domain, hence a field, thus $\mathfrak{p}$ is maximal.
3. Let $I_1 \subsetneq I_2 \subsetneq \cdots$ be an ascending chain of ideals in $\mathcal{O}_K$. Then $[\mathcal{O}_K : I_1] > [\mathcal{O}_K : I_2] > \cdots$, where all $[\mathcal{O}_K : I_i]$ by previous lemma are positive integers, hence there is a least $[\mathcal{O}_K : I_i]$ by well-ordering principle, so the chain stabilises at I_i.

□

Proposition 3.2.4. Every PID is a Dedekind domain.

Proof.

1. This follows from 1.1.10 and 1.2.9.

2. Let $(a) \subset R$ be a nonzero prime ideal, then a is prime, so by 1.1.6 a is irreducible, so (a) is maximal; indeed, assume $(a) \subset (c) \subset R$, then $a = cb$ for some $b \in R$, so c is either a unit (then $(c) = R$) or $c \sim a$ (then $(c) = (a)$).
3. Every ideal is generated by one element, in particular by finite number of elements.

□

Remark 3.2.5. Dedekind domains also arise from algebraic geometry: the coordinate ring (ring of regular functions) of smooth affine curves are Dedekind domains, e.g. $\mathbb{C}[x,y]/(x^n + y^n - 1)$. On the other hand, $\mathbb{C}[x,y]/(y^2 - x^3)$ where the curve $y^2 - x^3$ is singular is not integrally closed, which is analogous to that $\mathbb{Z}\left[\sqrt{d}\right]$ where $d \equiv 1 \bmod 4$ is not integrally closed.

Week 5, lecture 2, 4th February

Theorem 3.2.6. Let R be a Dedekind domain. Then any nonzero ideal $I \subsetneq R$ can be written in the form $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where $\mathfrak{p}_i \subset R$ are prime ideals. Moreover, this decomposition is unique up to permutation.

Proof. We prepare the proof by three lemmas for a Dedekind domain R which we will prove later:

1. If $\mathfrak{p}$ is a prime ideal and $I, J \subset R$ are ideals, then $IJ \subset \mathfrak{p} \implies I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$.
2. If $I, J, K \subset R$ are nonzero ideals, then $IK = JK \implies I = J$.
3. If $I, J \subset R$ are nonzero ideals, then $I \subset J \iff \exists K \subset R : I = JK$.

Now the proof of theorem has two parts:

1. *Existence of factorisation*. Let S be the set of ideals which are not products of prime ideals. For a contradiction, suppose $S \neq \varnothing$. Since R is noetherian, let I be a maximal element of S. Pick $\mathfrak{p}$ to be a maximal ideal of R such that $I \subsetneq \mathfrak{p}$ (if $I = \mathfrak{p}$ then I is maximal so prime so in particular a product of prime ideals, then $I \notin S$). By lemma 3, $\exists J \in R : I = \mathfrak{p}J$. Then $I \subset J$, but $I \neq J$ since if $I = J$ then $\mathfrak{p} = R$. This implies $J \notin S$, so J is a product of prime ideals, but then $I = \mathfrak{p}J$ is too.
2. *Uniqueness*. If $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ where $\mathfrak{p}_i, \mathfrak{q}_i$'s are prime, then we can prove by induction that $r = s$ and $\mathfrak{p} = \mathfrak{q}$ up to reordering. Indeed, we have $\mathfrak{q}_1 \cdots \mathfrak{q}_s = \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{p}_1$, so by lemma 1 and after necessary reordering we have $\mathfrak{q}_1 \subset \mathfrak{p}_1$. But they are both prime, so both maximal, hence $\mathfrak{q}_1 = \mathfrak{p}_1$. Cancel them from the equation by lemma 2 and proceed inductively.

□

Lemma 3.2.7. Let $I \subset R$ be an ideal of a Dedekind domain R and $\alpha \in \mathrm{Frac}(R)$. If $\alpha I \subset I$ then $\alpha \in R$.

Proof. Since R is Noetherian, write $I = (a_1, \ldots, a_n)$ where $a_i \in R$. Then $\alpha a_j = \sum_{i=1}^n c_{ij} a_i$ where $c_i j \in R$. Consider the matrix $A = (c_{ij})$ and its characteristic polynomial $\chi_A(t) \in R[t]$. Then $\chi_A(\alpha) I = \chi_A(A) I = 0$, so $\chi_A(\alpha) = 0$. Finally, since χ_A is monic and R is integrally closed, we have $\alpha \in R$. □

Lemma 3.2.8. Let $I \subset R$ be a nonzero ideal of a Dedekind domain R. Then there are nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset R$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset I$.

Proof. Let S be the set of nonzero ideals such that the statement of the lemma fails. Again, for a contradiction, suppose $S \neq \varnothing$ and let $I \in S$ be a maximal element. I is not prime by construction, so let $a, b \in R$ satisfy that $ab \in I$ and $a, b \notin I$. Then $I \subsetneq (a) + I$ and $I \subsetneq (b) + I$, so the lemma applies to $(a) + I$ and $(b) + I$. Write $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset (a) + I$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subset (b) + I$ where $\mathfrak{p}_i, \mathfrak{q}_i$'s are nonzero and prime. But then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m \subset ((a) + I)((b) + I) = (ab) + (a)I + (b)I + I^2 \subset I,$$

a contradiction. □

Lemma 3.2.9. Lemma 1 in proof of 3.2.6.

Proof. Suppose $I \not\subset \mathfrak{p}$, i.e. $\exists a \in I : a \notin \mathfrak{p}$. Then $ab \in IJ \subset \mathfrak{p}\ \forall b \in J$, so $b \in \mathfrak{p}\ \forall b \in J$ since $\mathfrak{p}$ is prime and $a \notin \mathfrak{p}$, i.e. $J \subset \mathfrak{p}$. □

Lemma 3.2.10. Let $I \subsetneq R$ be a nonzero proper ideal of a Dedekind domain R. Then $\exists x \in \text{Frac}(R) : x \notin R$ and $xI \subset R$.

Proof. Let $0 \neq \alpha \in I$. Then by 3.2.8, one can write $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (\alpha)$ where $\mathfrak{p}_i$'s are nonzero and prime and r is minimal (i.e. if we remove one $\mathfrak{p}_i$ then the inclusion fails). Let $\mathfrak{m}$ be a maximal ideal such that $(\alpha) \subset I \subset \mathfrak{m}$. Then by previous lemma, WLOG $\mathfrak{p}_1 \subset \mathfrak{m}$, but $\mathfrak{p}_1$ is prime so it's maximal as well, hence $\mathfrak{p}_1 = \mathfrak{m}$. Since r is minimal, $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (\alpha)$, so let $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \backslash (\alpha)$, then $bI \subset b\mathfrak{m} = b\mathfrak{p}_1 \subset \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (\alpha)$, so $\frac{b}{\alpha} I \subset R$, where $\frac{b}{\alpha}$ is the desired x. Indeed $\frac{b}{\alpha} \notin R$ since $b \in (\alpha)$ by construction. □

Lemma 3.2.11. Let $I \subset R$ be a nonzero ideal and $0 \neq a \in I$. Then $\exists$ ideal $J \subset R : IJ = (a)$.

Proof. We claim $J = \{b \in R : bI \subset (a)\}$ is the ideal we want. First this is indeed an ideal since (a) is. Also by construction $IJ \subset (a)$, so it remains to see $(a) \subset IJ$. For a contradiction, suppose $IJ \subsetneq (a)$, then $K = \frac{1}{a} IJ \subsetneq R$ is a nonzero proper ideal. By previous lemma, let $x \in \text{Frac}(R) \backslash R$ satisfy $xK \subset R$, so $xIJ = xaK \subset (a)$. Now since $a \in I$, we have $aJ \subset IJ$, so $J \subset K$ and $xJ \subset xK \subset R$. Let $b \in J$. Then $xb \in R$ and $xbI \subset xJI \subset (a)$, so $xb \in J$ by definition of J. This implies $xJ \subset J$, so by 3.2.7 $x \in R$, a contradiction. □

Lemma 3.2.12. Lemma 2 in proof of 3.2.6.

Proof. By 3.2.11, let K' be an ideal such that $KK' = (a)$ for some $a \in K$. Then $I(a) = IKK' = JKK' = J(a)$, so $I = J$ by the usual cancellation since R is a domain. □

Corollary 3.2.13. Lemma 3 in proof of 3.2.6.

Proof. $\Longleftarrow$ Clearly $I = JK \subset J$.

$\Longrightarrow$ By 3.2.11, write $JJ' = (b)$ where $b \in J$, so $IJ' \subset JJ' = (b)$, then take $K = b^{-1}IJ'$, and indeed $JK = b^{-1}JJ'I = I$.

□

Week 5, lecture 3, 5th February

3.3 Class groups, or how far is my Dedekind domain from a UFD?

Definition 3.3.1. Let R be a Dedekind domain. Two nonzero ideals $I, J \subset R$ are in the same *class*, denoted by $I \sim J$, if $\exists \alpha \in \text{Frac}(R)^\times : \alpha I = J$. The set of equivalences classes of ideals of R, denoted by $\text{Cl}(R)$, is called the *class group* of R, and the class of $I \subset R$ is denoted by $[I]$.

Remark 3.3.2.

- By definition $[I] = [R] \iff I = \alpha R \iff I$ is principal, so all principal ideals are in the same class (as the whole ring).
- Define an operation on $\text{Cl}(K)$ by $[I] \cdot [J] = [IJ]$. Check this is well-defined, commutative and associative.

Proposition 3.3.3. The class group is indeed a group (and an abelian one too).

Proof. Note that the class $[R]$ serves as the identity: $[I][R] = [IR] = [I]$. Then inverses exists by 3.2.11. □

Example 3.3.4. Let $\mathfrak{p}_2 = \left(2, 1 + \sqrt{-5}\right)$ and $\mathfrak{p}_3 = \left(3, 1 + \sqrt{-5}\right)$ again be ideals of $\mathbb{Z}\left[\sqrt{-5}\right]$. Then

$$\mathfrak{p}_3\mathfrak{p}_2 = \left(6, 3 + 3\sqrt{-5}, 2 + 2\sqrt{-5}, \left(1 + \sqrt{-5}\right)^2\right) = \left(1 + \sqrt{-5}\right)$$

(since $6 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$. In particular $[\mathfrak{p}_2\mathfrak{p}_3] = 1$, i.e. $[\mathfrak{p}_2] = [\mathfrak{p}_3]$. Similarly $\mathfrak{p}_2^2 = (2)$ is principal, so $[\mathfrak{p}_2]$ has order 2 in $\text{Cl}(R)$. We will eventually see that this is the whole group: $\text{Cl}(R) = \{1, [\mathbb{P}_2]\} \cong \mathbb{Z}/2\mathbb{Z}$.

Proposition 3.3.5. Let R be a Dedekind domain. The following are equivalent:

1. $\text{Cl}(R) = \{1\}$.
2. R is a PID.
3. R is a UFD.

Proof. Clearly $1 \iff 2$.

$2 \implies 3$ is 1.1.10.

It remains to show $3 \implies 2$. To prove R is a PID, it suffices to show that every prime ideal is principal since then every ideal is a product of prime ideals and hence principal as well. Let $\mathfrak{p} \subset R$ be a nonzero ideal ad $0 \neq \alpha \in \mathfrak{p}$. Since R is a UFD, write $\alpha = i\pi_1 \cdots \pi_r$ where $u \in R^\times$ and π_i's are irreducible/prime. Then some $(\pi_i) \subset \mathfrak{p}$, but both are maximal so $(\pi_i) = \mathfrak{p}$, in particular $\mathfrak{p}$ is principal. □

Proposition 3.3.6 (Computations with ideals)**.** Let R be a Dedekind domain and $I, J \subset R$ nonzero ideals. Write $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ and $J = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}$ where a_i, b_i's could be 0 and $\mathfrak{p}_i$'s are distinct prime ideals. Then

1. $IJ = \mathfrak{p}_1^{a_1+b_1} \cdots \mathfrak{p}_r^{a_r+b_r}$
2. $I \subset J \iff a_i \geq b_i \ \forall i$
3. $I + J = \mathfrak{p}_1^{\min\{a_i,b_i\}} \cdots \mathfrak{p}_r^{\min\{a_r,b_r\}}$
4. $I \cap J = \mathfrak{p}_1^{\max\{a_i,b_i\}} \cdots \mathfrak{p}_r^{\max\{a_r,b_r\}}$

Proof.

1. This follows from commutativity and $\mathfrak{p}^a\mathfrak{p}^b = \mathfrak{p}^{a+b}$.
2. Recall that $I \subset J \iff \exists$ ideal $K \subset R : I = JK$. Write $K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} K'$ for some ideal $K' \subset R$. Using unique factorisation, $a_i = b_i + e_i \ \forall i$ and $K' = R$.
3. Write $I+J = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_r^{c_r}$. Then $I, J \subset I+J$, so $c_i \leq a_i, b_i$, i.e. $c_i \leq \min\{a_i, b_i\}$, hence $\mathfrak{p}_1^{\min\{a_i,b_i\}} \cdots \mathfrak{p}_r^{\min\{a_r,b_r\}} \subset I + J$ by 2. But $I, J \subset \mathfrak{p}_1^{\min\{a_i,b_i\}} \cdots \mathfrak{p}_r^{\min\{a_r,b_r\}}$ again by 2 so $I + J \subset \mathfrak{p}_1^{\min\{a_i,b_i\}} \cdots \mathfrak{p}_r^{\min\{a_r,b_r\}}$, hence equality.
4. Again write $I + J = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_r^{c_r}$. Since $I \cap J \subset I, J$, by 2 $a_i, b_i \leq c_i$, in particular $c_i \geq \max\{a_i, b_i\}$, hence $I \cap J \subset \mathfrak{p}_1^{\max\{a_i,b_i\}} \cdots \mathfrak{p}_r^{\max\{a_r,b_r\}}$. But $\mathfrak{p}_1^{\max\{a_i,b_i\}} \cdots \mathfrak{p}_r^{\max\{a_r,b_r\}} \subset I, J$, so $\mathfrak{p}_1^{\max\{a_i,b_i\}} \cdots \mathfrak{p}_r^{\max\{a_r,b_r\}} \subset I \cap J$.

□

Theorem 3.3.7 (Chinese remainder theorem)**.** Let R be a commutative ring and $I, J \subset R$ ideals. If $I + J = R$ then $I \cap J = IJ$ and there is an isomorphism of rings $R/IJ \to R/I \times R/J$ via $a + IJ \mapsto (a + I, a + J)$.

In general if ideals $I_1, \dots, I_r \subset R$ satisfy $I_i + I_j = R \ \forall i, j$ then $\bigcap I_i = \prod I_i$ and $R/I_1 \cdots I_r \cong R/I_1 \times \cdots \times R/I_r$.

In particular on Dedekind domains, if $\mathfrak{p}_1, \mathfrak{p}_2$ are distinct prime ideals then necessarily $\mathfrak{p}_1^{a_1} + \mathfrak{p}_2^{a_2} = R$ for all $a_1, a_2 \geq 0$ by 3.3.6. It follows that for a Dedekind domain R,

$$R/\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} \cong R/\mathfrak{p}_1^{a_1} \times \cdots \times R/\mathfrak{p}_r^{a_r}$$

for any collection $\mathfrak{p}_1, \dots \mathfrak{p}_r$ of distinct prime ideals. We will most often use particularly surjection; namely the system of equations

$$\begin{cases} x \equiv x_1 \bmod \mathfrak{p}_1^{a_1} \\ \vdots \\ x \equiv x_r \bmod \mathfrak{p}_r^{a_r} \end{cases}$$

is solvable.

Proposition 3.3.8. Let R be a Dedekind domain and $I \subset R$ a nonzero ideal with $0 \neq \alpha \in I$. Then $\exists \beta \in I : I = (\alpha, \beta)$. In particular, every ideal in R can be generated by two elements.

Proof. Write the prime factorisation $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$. Then $(a) = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r} \mathfrak{q}_1^{c_1} \cdots \mathfrak{q}_s^{c_s}$ for some distinct prime ideals q_j's. Since $(a) \subset I$ we have $b_i \geq a_i$. For $i = 1, \dots, r$ clearly $\mathfrak{p}_i^{a_i+1} \subsetneq \mathfrak{p}_i^{a_i}$, so let $x_i \in \mathfrak{p}_i^{a_i} \backslash \mathfrak{p}_i^{a_i+1}$. And since $\mathfrak{q}_j \subsetneq R$, let $x_j \in R \backslash \mathfrak{q}_j$. Now use CRT to find $\beta \in R$ such that

$$\begin{cases} \beta \equiv x_i \bmod \mathfrak{p}_i^{a_i+1} \\ \vdots \\ \beta \equiv x_j \bmod \mathfrak{q}_j, \end{cases}$$

in particular $\beta \notin \mathfrak{p}_i^{a_i+1}$, $\beta \in \mathfrak{p}_i^{a_i}$ and $\beta \notin \mathfrak{q}_j$. This implies in the prime factorisation of (β) we won't see $\mathfrak{q}_j$'s and $\mathfrak{p}_i$'s are of order exactly a_i, i.e. $(\beta) = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} \tau_1^{d_1} \cdots \tau_l^{d_k}$ where τ_j's are different from $\mathfrak{p}_i$'s and $\mathfrak{q}_j$'s. Then $(\alpha, \beta) = (\alpha) + (\beta) = \mathfrak{p}_1^{\min\{a_i,b_i\}} \cdots \mathfrak{p}_r^{\min\{a_r,b_r\}} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} = I$. □

Exercise 3.3.9. 3. Let $\mathcal{O}_{-5} = \mathbb{Z}\left[\sqrt{5}\right]$, $\mathfrak{p}_2 = \left(2, 1+\sqrt{-5}\right)$, $\mathfrak{p}_3 = \left(3, 1+\sqrt{-5}\right)$ and $\overline{\mathfrak{p}_3} = \left(3, 1-\sqrt{-5}\right)$.

(b) Check $(2) = \mathfrak{p}_2^2$, $(3) = \mathfrak{p}_3\overline{\mathfrak{p}_3}$.

(c) Show that $\mathfrak{p}_3^2$ is principal and find a generator.

(d) What is $\mathcal{O}_{-5}/\mathfrak{p}_2$?

(e) Prove that (7) is not prime.

Solution.

(b) Showed in class.

(c) We can do this by hand by multiplying generators, but there is a trick. We already know $\mathfrak{p}_2\mathfrak{p}_3 = \left(1+\sqrt{-5}\right)$ by 3.3.4. Write $2\mathfrak{p}_3^2 = \mathfrak{p}_2^2\mathfrak{p}_3^2 = (\mathfrak{p}_2\mathfrak{p}_3)^2 = \left(1+\sqrt{-5}\right)^2 = \left(-4+2\sqrt{5}\right) = (2)\left(-2+\sqrt{-5}\right)$. The trick is useful when we have enough information of other ideals in the class group.

(d) Similarly to before, write $\mathcal{O}_{-5} = \mathbb{Z}[t]/(t^2+5)$ and hence $\mathcal{O}_{-5}/\mathfrak{p}_2 = \mathbb{Z}[t]/(t^2+5, 2, 1+t) = \mathbb{Z}/2\mathbb{Z}[t]/(t^2-1, 1+t) = \mathbb{Z}/2\mathbb{Z}[t]/(1+t) = \mathbb{Z}/2\mathbb{Z}$.

(e) We can prove this in two ways.

i. Again, write $\mathcal{O}_{-5}/(7) = \mathbb{Z}[t]/(t^2+5, 7) = \mathbb{Z}/7\mathbb{Z}[t]/(t^2+5) = \mathbb{Z}/7\mathbb{Z}[t]/((t-3)(t+3))$, which is not a domain.

ii. $21 = \left(4+\sqrt{-5}\right)\left(4-\sqrt{-5}\right) \in (7)$ but $\left(4+\sqrt{-5}\right), \left(4-\sqrt{-5}\right) \notin (7)$. We can get these two elements by mapping $t-3, t+3$ back to $\mathcal{O}_{-5}$.

4. Give examples of a ring that has two of the following properties but not third one: Noetherian, integrally closed, and every nonzero prime ideal is maximal (i.e. definition of a Dedekind domain).

Solution.

(a) $\mathbb{Z}[x]$ is Noetherian by Hilbert, it's a UFD by Gauss hence integrally closed by 1.2.9, but (x) is prime and not maximal ($(x) \subsetneq (x, 2)$ for example).

(b) $\mathbb{Z}\left[\sqrt{-3}\right]$ is Noetherian since it's a quotient of $\mathbb{Z}[x]$. For the third property, the argument used in proof of 3.2.3 still applies. But it's not integrally closed since $\frac{1+\sqrt{-3}}{2}$ is a solution of x^2-x+1.

(c) $\overline{\mathbb{Z}}$, the set of all algebraic integers in $\mathbb{C}$, is clearly integrally closed. For the third property, we need the following lemma.

Lemma 3.3.10. Let $\phi : A \to B$ be a ring morphism. Then $\forall$ prime ideals $\mathfrak{p} \subset B$, $\phi^{-1}\mathfrak{p} = \{a \in A : \phi(a) \in \mathfrak{p}\}$ is prime. In particular if ϕ is an embedding, denote $\mathfrak{p} \cap A = \phi^{-1}(\mathfrak{p})$.

Now take $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be a nonzero prime ideal and assume $\mathfrak{p} \subsetneq \mathfrak{q}$ for some other prime ideal $\mathfrak{q} \subset \overline{\mathbb{Z}}$. Then $\mathfrak{p} \cap \mathbb{Z}, \mathfrak{q} \cap \mathbb{Z}$ are both nonzero prime ideals, so $\mathfrak{p} \cap \mathbb{Z}, \mathfrak{q} \cap \mathbb{Z}$ are maximal hence equal to some (p) with p prime. Now take $\beta \in \mathfrak{q}\backslash\mathfrak{p}$, then $\exists b_{n-1}, \dots, b_0 \in \mathbb{Z} : \beta^n + b_{n-1}\beta^{n-1} + \dots + \beta_0 = 0$. Assume j is the minimal integer such that $b_j \notin (p)$. Then $\beta^{n-j}(\beta^j + \dots + b_j) = -\left(b_{j+1}\beta^{j+1} + \dots + b_0\right) \in (p)$, so $\beta^j + \dots + b_j \in (p) \subset \mathfrak{q}$, hence $\beta_j \in \mathfrak{q}$, a contradiction. Hence $\mathfrak{p} = \mathfrak{q}$ and $\mathfrak{p}$ is maximal.
But $\overline{\mathbb{Z}}$ is not Noetherian: the chain

$$(2) \subsetneq \left(\sqrt{2}\right) \subsetneq \left(\sqrt[4]{2}\right) \subsetneq \dots \subsetneq \left(2^{\frac{1}{2n}}\right) \subsetneq \cdots$$

doesn't stabilise.

Week 6, lecture 2, 11th February

Proof of 3.3.10. It's clear that $\phi^{-1}(\mathfrak{p})$ is indeed an ideal. Now $ab \in \phi^{-1}(\mathfrak{p}) \implies \phi(ab) = \phi(a)\phi(b) \in \mathfrak{p} \implies \phi(a)$ or $\phi(b) \in \mathfrak{p} \implies a$ or $b \in \phi^{-1}(\mathfrak{p})$. □

In particular, given a number field K we always have a natural inclusion $\iota : \mathbb{Z} \hookrightarrow \mathcal{O}_K$, so given a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ we have $\mathfrak{p} \cap \mathbb{Z} = \iota^{-1}(\mathfrak{p}) \subset \mathbb{Z}$ is a prime ideal.

Lemma 3.3.11. Let K be a number field and $\mathfrak{p} \subset \mathcal{O}_K$ a nonzero prime ideal. Then there is a unique prime number $p \in \mathbb{Z}$ such that $p \in \mathfrak{p}$.

Proof. Two ways to see this:

1. We have just seen that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal, so since $\mathbb{Z}$ is a PID, if we can prove this is nonzero we are done. Take $0 \neq \alpha \in \mathfrak{p}$. Then $N_K(\alpha) = \alpha \prod_{\tau \neq \mathrm{id}} \tau(\alpha)\mathfrak{p}$. Also $N_K(\alpha) \in \mathbb{Z}$ since $\alpha \in \overline{\mathbb{Z}}$. Hence $N_K(\alpha) \in \mathfrak{p} \cap \mathbb{Z}$.

2. We know $\mathcal{O}_K/\mathfrak{p}$ is finite, so $\mathcal{O}_K/\mathfrak{p}$ is a field of characteristic $p > 0$, so $p = 0$ in $\mathcal{O}_K/\mathfrak{p}$, hence $p \in \mathfrak{p}$.

□

3.4 Factorisation of prime ideals into Dedekind domain prime factors

Definition 3.4.1. A nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ *lies above* the prime $p \in \mathbb{Z}$ if $p \in \mathfrak{p}$ (or equivalently $\mathfrak{p} \cap \mathbb{Z} = (p)$.)

Proposition 3.4.2. Let $p \in \mathbb{Z}$ be prime and suppose $\mathcal{O}_K \supset (p) = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ distinct prime ideals using 3.2.6. Then they are exactly the prime ideals that lie above p.

Proof. $(p) = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} \subset \mathfrak{p}_i \ \forall i$, so $p \in \mathfrak{p}_i \ \forall i$. Conversely, if $\mathfrak{p} \subset \mathcal{O}_K$ and $p \in \mathfrak{p}$, then $(p) \subset \mathfrak{p}$, so $\exists$ ideal $I \subset \mathcal{O}_K$ such that $(p) = \mathfrak{p}I$, The desired then follows from 3.2.6. □

Example 3.4.3. $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$. First note that $\mathbb{Z}[i]$ is a Euclidean domain, so every prime ideal $\mathfrak{p}$ is generated by a irreducible element.

- If $p \equiv 3 \bmod 4$, then p is irreducible, so (p) is prime.
- If $p \equiv 1 \bmod 4$ then $p = \pi_p \overline{\pi_p}$ for some irreducible π_p, and $N_{\mathbb{Q}(i)}(\pi_p) = N_{\mathbb{Q}(i)}(\overline{\pi_p}) = p$. Hence $(p) = (\pi_p)(\overline{\pi_p}) =: \mathfrak{p}_1\mathfrak{p}_2$. Moreover, $\mathfrak{p}_1 \neq \mathfrak{p}_2$; if $\mathfrak{p}_1 = \mathfrak{p}_2$ then $\exists u \in \mathbb{Z}[i]^\times : \pi_p = u\overline{\pi_p}$. But we know $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, and if we write $\pi_p = x + iy$ with $N_{\mathbb{Q}(i)}(x + iy) = x^2 + y^2 = p$, we now that $x, y \neq 0$ and $x \neq y \bmod 2$. Now no u satisfies these two conditions, so a contradiction.
- If $p = 2$ then $p = (1+i)(1-i)$ where $1+i, 1-i$ are irreducible, so $(2) = (1+i)(1-i)$, but $1 + i = i(1-i)$, so $(2) = \mathfrak{p}^2$ for a prime ideal $\mathfrak{p}$.

Definition 3.4.4. Let K be a number field and $\mathfrak{p} \subset \mathcal{O}_K$ a nonzero prime ideal lying above p. The *ramification index* $e(\mathfrak{p})$ of $\mathfrak{p}$ is the multiplicity with which $\mathfrak{p}$ occurs in the factorisation of (p).

For example, in the above example, $(1+i)$ has ramification index 2, but π_p has ramification index 1.

Definition 3.4.5. The *inertia degree* of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is $f(\mathfrak{p}) = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$.

Example 3.4.6. $K = \mathbb{Q}\left(\sqrt{-5}\right)$, $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-5}\right]$ with $\mathfrak{p}_2$ being as usual. Then $(2) = \mathfrak{p}_2^2$ so $e(\mathfrak{p}_2) = 2$, and $(3) = \mathfrak{p}_3\overline{\mathfrak{p}_3}$ so $e(\mathfrak{p}_3) = 1$. Clearly $(5) = \left(\sqrt{-5}\right)^2 := \mathfrak{p}_5^2$ so $e(\mathfrak{p}_5) = 2$. One can check that $(7) = \left(7, 3 + \sqrt{-5}\right)\left(7, 3 - \sqrt{-5}\right)$.

Theorem 3.4.7. Let K be a number field fix $p \in \mathbb{Z}$ prime. Then

$$\sum_{\mathfrak{p} \subset \mathcal{O}_K, p \in \mathfrak{p}} e(\mathfrak{p}) f(\mathfrak{p}) = \deg_{\mathbb{Q}}(K).$$

Remark 3.4.8. What is the theorem saying above $K = \mathbb{Q}\left(\sqrt{d}\right)$? One of the following 3 possibilities happen:

1. There is just one prime $\mathfrak{p} \subset \mathcal{O}_K$ lying above $p \in \mathbb{Z}$ with $e(p) = 2$ and $f(p) = 1$.
2. There is just one prime $\mathfrak{p} \subset \mathcal{O}_K$ lying above $p \in \mathbb{Z}$ with $e(p) = 1$ and $f(p) = 2$.
3. There are two distinct prime $\mathfrak{p}_1 \neq \mathfrak{p}_2$ with $e(\mathfrak{p}_1) = e(\mathfrak{p}_2) = 1$ and $f(\mathfrak{p}_1) = f(\mathfrak{p}_2) = 1$.

The main we are using to prove the theorem is the following notion.

Definition 3.4.9. Let $I \subset \mathcal{O}_K$ be a nonzero ideal. The *norm* of I, denoted by $N_K(I)$, is the index $[\mathcal{O}_K : I]$.

Remark 3.4.10.

1. If $p \subset \mathcal{O}_K$ is a prime ideal, then $[\mathcal{O}_K : \mathfrak{p}] = p^{f(p)}$.
2. If $n \in \mathbb{Z}$ and $N_K((n)) = |n|^{\deg_{\mathbb{Q}}(K)} = |N_K(n)|$ (we will see that $\forall \alpha \in \mathcal{O}_K$ we have $N_K(\alpha\mathcal{O}_K) = |N_K(\alpha)|$); indeed, recall (after fixing an integral basis of $\mathcal{O}_K$) that $\mathcal{O}_K \cong \mathbb{Z}^{\deg_{\mathbb{Q}}^K}$, so $\mathcal{O}_K/n\mathcal{O}_K \cong (\mathbb{Z}/n\mathbb{Z})^{\deg_{\mathbb{Q}} K}$.

Week 6, lecture 3, 12th February

Proposition 3.4.11. If I, J are nonzero ideals of $\mathcal{O}_K$, then $N_K(IJ) = N_K(I)N_K(J)$.

Proof. By 3.2.6, it suffices to show $N_K(\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r}) = N_K(\mathfrak{p}_1)^{a_r}\cdots N_K(\mathfrak{p}_r)^{a_r}$ where $\mathfrak{p}_i$ are prime ideals. Chinese remainder theorem says, $\mathcal{O}_K/\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r} \cong \mathcal{O}_K/\mathfrak{p}_1^{a_1}\times\cdots\times\mathcal{O}_K/\mathfrak{p}_r^{a_r}$, so it remains to see $N_K(\mathfrak{p}^a) = N_K(\mathfrak{p})^a$ for a prime ideal $\mathfrak{p}$. We prove it by induction on a. The base case $a = 1$ is tautological. Now by Lagrange and 3rd isomorphism theorem (in particular for abelian groups $A \subset B \subset C$, we have $[C : A] = [B : A][(C/A) : (B/A)] = [B : A][C : B]$),

$$N_K(\mathfrak{p}^{a+1}) = [\mathcal{O}_K : \mathfrak{p}^{a+1}] = [\mathcal{O}_K : \mathfrak{p}^a][\mathfrak{p}^a : \mathfrak{p}^{a+1}] = N_K(\mathfrak{p})^a[\mathfrak{p}^a : \mathfrak{p}^{a+1}],$$

now it suffices to show $[\mathfrak{p}^a : \mathfrak{p}^{a+1}] = N_K(\mathfrak{p})$. We build a isomorphism of abelian groups $\mathcal{O}_K/\mathfrak{p} \to \mathfrak{p}^a/\mathfrak{p}^{a+1}$. Take $b \in \mathfrak{p}^a\backslash\mathfrak{p}^{a+1}$ and define the map by $y + \mathfrak{p} \mapsto yb + \mathfrak{p}^{a+1}$. The map is

1. well-defined: suppose $y' - y \in \mathfrak{p}$, i.e. $y' = y + x$ for some $x \in \mathfrak{p}$. Then $y' + \mathfrak{p} \mapsto y'b + \mathfrak{p}^{a+1} = yb + xb + \mathfrak{p}^{a+1}$, but $x \in \mathfrak{p}, b \in \mathfrak{p}^a \implies xb \in \mathfrak{p}^{a+1}$;
2. injective: recall that in Dedekind domains every nonzero prime ideal is maximal, so $\mathfrak{p}$ is maximal, so for any nonzero $x \notin \mathfrak{p}$ we have $\mathfrak{p} + (x) = \mathcal{O}_K$. Hence $1 = y + xx'$ for some $y \in \mathfrak{p}$ and $x' \in \mathcal{O}_K$. If $x + \mathfrak{p} \mapsto 0$, then $xb \in \mathfrak{p}^{a+1}$. Write $b = b(y + xx') = by + bxx'$ Then $b \in \mathfrak{p}^a, y \in \mathfrak{p} \implies by \in \mathfrak{p}^{a+1}$, $xb \in \mathfrak{p}^{a+1} \implies bxx' \in \mathfrak{p}^{a+1}$, so $b \in \mathfrak{p}^{a+1}$, contradicting our assumption of b;
3. surjective: note that $(b) = \mathfrak{p}^a I$ with I coprime to $\mathfrak{p}$ by 3.2.6 since $b \notin \mathfrak{p}^{a+1}$. Then $(b) + \mathfrak{p}^{a+1} = \mathfrak{p}^a$ by 3.3.6.3. Now let $x \in \mathfrak{p}^a$ write $x = yb + y'$ where $y \in \mathcal{O}_K$, $y' \in \mathfrak{p}^{a+1}$. Then $y + \mathfrak{p} \mapsto yb + \mathfrak{p}^{p+1} = yb + y' + \mathfrak{p}^{a+1}$.

□

Proof of 3.4.7. By definition, $p\mathcal{O}_K = \mathfrak{p}_1^{e(\mathfrak{p}_1)}\cdots\mathfrak{p}_r^{e(\mathfrak{p}_r)}$, and $N_K = p^{\deg_{\mathbb{Q}} K} = N_K(\mathfrak{p}_1)^{e(\mathfrak{p}_1)}\cdots N_K(\mathfrak{p}_r)^{e(\mathfrak{p}_r)}$ by 3.4.11. But by definition $N_K(\mathfrak{p}_i) = [\mathcal{O}_K : \mathfrak{p}_i] = p^{f(\mathfrak{p}_i)}$, hence $p^{\deg_{\mathbb{Q}} K} = p^{e(\mathfrak{p}_1)f(\mathfrak{p}_1)}\cdots p^{e(\mathfrak{p}_r)f(\mathfrak{p}_r)}$, giving us the desired. □

Remark 3.4.12. An implication is if $I \subset \mathcal{O}_K$ is an ideal and $N_K(I) = p \in \mathbb{Z}$ is prime, then I is a prime ideal.

Proposition 3.4.13. Let $0 \neq \alpha \in \mathcal{O}_K$, then $N_K(\alpha\mathcal{O}_K) = |N_K(\alpha)|$.

Proof. Recall that $N_K(\alpha) = \det A$ where A is the matrix associated to $\mathrm{mult}_\alpha : \mathcal{O}_K \to \mathcal{O}_K$. But then $[\mathcal{O}_K : \alpha\mathcal{O}_K] = [\mathbb{Z}^n : A\mathbb{Z}^n] = |\det A|$ by 2.3.19 and linear algebra (in particular Smith normal form). □

Remark 3.4.14. If $\alpha \in \mathcal{O}_K$ and $N_K(\alpha) = p$, then $N_K(\alpha\mathcal{O}_K) = p$ by above so $\alpha\mathcal{O}_K$ is a prime ideal, hence α is a prime element. But before introducing norm of ideals, we only know that $N_K(\alpha) = \pm p \implies \alpha$ is irreducible.

Theorem 3.4.15. Let $d \neq 0, 1$ be a squarefree integer and $p \in \mathbb{Z}$ an odd prime. Then $p\mathcal{O}_K$ splits in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathcal{O}_K$ as follows.

1. If $p \mid d$ then p ramifies as $p\mathcal{O}_K = \left(p, \sqrt{d}\right)^2$.
2. If $p \nmid d$ and $\exists a \in \mathbb{Z} : a^2 \equiv d \bmod p$, then $p\mathcal{O}_K = \left(p, a + \sqrt{d}\right)\left(p, a - \sqrt{d}\right)$.
3. If $p \nmid d$ and $\nexists a \in \mathbb{Z} : a^2 \equiv d \bmod p$, then $p\mathcal{O}_K$ is a prime ideal.

Proof. 1. One has $\left(p, \sqrt{d}\right)^2 = \left(p^2, p\sqrt{d}, d\right) \subset (p)$. But then $p^2, d \in \left(p^2, p\sqrt{d}, d\right)$ and $\gcd(p^2, d) = p$ so by Bézout $p \in \left(p^2, p\sqrt{d}, d\right)$. It remains to show $\left(p, \sqrt{d}\right) := \mathfrak{p}$ is prime. Indeed, $N_K(p\mathcal{O}_K) = |p|^{\deg_{\mathbb{Q}} \mathbb{Q}(\sqrt{d})} = p^2$, so $N_K(\mathfrak{p}) = p$.

2. One has
$$\left(p, a + \sqrt{d}\right)\left(p, a - \sqrt{d}\right) = \left(p^2, p\left(a + \sqrt{d}\right), p\left(a - \sqrt{d}\right), a^2 - d\right) \subset (p)$$
since $p \mid a^2 - d$. Now $p\left(a + \sqrt{d}\right) + p\left(a - \sqrt{d}\right) = 2pa \in \left(p^2, p\left(a + \sqrt{d}\right), p\left(a - \sqrt{d}\right), a^2 - d\right)$ and $\gcd(2pa, p^2) = p$ ($p \nmid a$ since $a^2 \equiv d \bmod p$ and $p \nmid d$), so one has equality.

Week 7, lecture 1, 17th February

3. Suppose for a contradiction that $p\mathcal{O}_K$ is not prime, then $\exists \mathfrak{p} \subset \mathcal{O}_K$ prime such that $p\mathcal{O}_K \subsetneq \mathfrak{p}$. Then $N_K(\mathfrak{p}) = p$; indeed, $N_K(\mathfrak{p}) \mid N_K(p\mathcal{O}_K) = p^2$, so $N_K(\mathfrak{p}) = 1, p$ or p^2. But $\mathfrak{p}$ is prime so not 1, and the inclusion is strict so not p^2. This means $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$. Moreover, $\left(\sqrt{d} + \mathfrak{p}\right)^2 = d + \mathfrak{p} \in \mathcal{O}_K/\mathfrak{p}$, but this is saying d is a quadratic residue modulo p, a contradiction.

□

Theorem 3.4.16. If $p = 2$, then

1. If $d \not\equiv 1 \bmod 4$ then 2 ramifies in $\mathcal{O}_K$ as follows:
   (a) If $2 \mid d$ then $(2) = \left(2, \sqrt{d}\right)^2$
   (b) If $2 \nmid d$, then $d \equiv 3 \bmod 4$ and $(2) = \left(2, \sqrt{d} + 1\right)^2$
2. If $d \equiv 1 \bmod 4$, then
   (a) If $d \equiv 1 \bmod 8$, then
   $$(2) = \left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right).$$
   (b) If $d \equiv 5 \bmod 8$ then (2) is prime.

Proof. Let's see the proof of 2(a). If $d \equiv 1 \bmod 8$ then in particular $d \equiv 1 \bmod 4$ so $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Write $\mathfrak{p}_1 = \left(2, \frac{1+\sqrt{d}}{2}\right)$ and $\mathfrak{p}_2 = \left(2, \frac{1-\sqrt{d}}{2}\right)$. Then

$$\mathfrak{p}_1\mathfrak{p}_2 = \left(4, 1+\sqrt{d}, 1-\sqrt{d}, \frac{1-d}{4}\right) \subset (2)$$

since d is assumed to be 1 mod 8. The other inclusion follows from

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

To see $\mathfrak{p}_1, \mathfrak{p}_2$ are prime, note that $N_K(\mathfrak{p}_1\mathfrak{p}_2) = N_K(2) = 4 = N_K(\mathfrak{p}_1)N_K(\mathfrak{p}_2)$, but $\mathfrak{p}_1, \mathfrak{p}_2$ are both proper so don't have norm 1, hence $N_K(\mathfrak{p}_1) = N_K(\mathfrak{p}_2) = 2$, so prime.

It remains to see $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Suppose $\mathfrak{p}_1 = \mathfrak{p}_2$, then $\frac{1+\sqrt{d}}{2} \in \mathfrak{p}_2$, so $\frac{1+\sqrt{d}}{2} + \frac{1-\sqrt{d}}{2} = 1 \in \mathfrak{p}_2$, i.e. $\mathfrak{p}_2 = \mathcal{O}_K$, a contradiction.

Proofs for other cases employ similar strategies and are omitted. □

We have seen that the discriminant $D_{\mathbb{Q}(\sqrt{d})}$ of $\mathbb{Q}\left(\sqrt{d}\right)$ is $4d$ if $d \equiv 1 \bmod 4$ and d if $d \equiv 1 \bmod 4$. With the theorems above this gives

Corollary 3.4.17. A prime p ramifies in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \iff p \mid D_{\mathbb{Q}(\sqrt{d})}$.

We now take inspiration from this and investigate ramification more generally.

Definition 3.4.18. We say a prime $p \in \mathbb{Z}$ *ramifies* in a number field K if in the factorisation of $p\mathcal{O}_K$ there is at least one repeated factor, i.e. for $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ with $\mathfrak{p}_i$ distinct prime ideals, $\exists i : e_i > 1$.

The aim of this week is to partially prove the following theorem for $K = \mathbb{Q}(\alpha)$. By primitive element theorem from Galois theory, this is actually for all number fields.

Theorem 3.4.19. Let K be a number field. Then a prime number $p \in \mathbb{Z}$ ramifies in $\mathcal{O}_K \iff p \mid D_K$.

We used several times that $\mathbb{Z}\left[\sqrt{d}\right] = \mathbb{Z}[t]/\left(t^2 - d\right)$. In general,

Lemma 3.4.20. Let $\alpha \in \mathbb{C}$ be a nonzero algebraic integer and $m_\alpha \in \mathbb{Z}[x]$ be its minimal polynomial. Then there is an isomorphism $\mathbb{Z}[\alpha] \to \mathbb{Z}[x]/(m_\alpha)$.

Proof. We see that $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\alpha] : x \mapsto \alpha$ is a surjective morphism (by definition of $\mathbb{Z}[\alpha]$) with kernel (m_α); this is a bit subtle since we can't just use Definition 2.0.3. Clearly $(m_\alpha) \subset \ker \phi$. If $f \in \mathbb{Z}[x] : \phi(f) = f(\alpha) = 0$, write $f(x) = g(x)m_\alpha(x)$, which is only true over $\mathbb{Q}[x]$. If $\deg f < \deg m_\alpha$ then $f = 0$ and $f \in (m_\alpha)$ trivially. If $\deg f \geq \deg m_\alpha$, write

$$f(x) = a_n x^n + \cdots + a_0 = a_n x^{n-\deg m_\alpha} m\alpha + h$$

where h is some polynomial with $\deg h < \deg f$. Moreover, $f(\alpha) \implies h(\alpha)$, so by induction we are done. □

Moreover, if an ideal $I \subset \mathbb{Z}[x]$ is generated by $f_1, \ldots, f_r$ then $\mathbb{Z}[\alpha]/I = \mathbb{Z}[x]/(m_\alpha, f_1, \ldots, f_r)$.

Week 7, lecture 2, 18th February

Theorem 3.4.21 (Dedekind's factorisation criteria)**.** Let $K = \mathbb{Q}(\alpha)$ where $\alpha \in \mathbb{C}$ is a nonzero algebraic integer with minimal polynomial m_α. Let p be a prime number such that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. If $\overline{m_\alpha} = \overline{g_1}^{e_1} \cdots \overline{g_r}^{e_r}$ is the factorisation of m_α modulo p with g_i's being distinct monic irreducible polynomials, then $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ where $\mathfrak{p}_i = (p, g_i(\alpha))$ with g_i being any lift in $\mathbb{Z}[x]$ at $\overline{g_i} \in \mathbb{F}_p[x]$. Moreover, $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_K$ and $f(\mathfrak{p}_i) = \deg(\overline{g_i})$.

Remark 3.4.22. $\mathfrak{p}_i$ indeed doesn't depend on choice of the lift: let $g_i, \widetilde{g}_i \in \mathbb{Z}[x]$ be two different lifts of $\overline{g_i} \in \mathbb{F}_p[x]$. Then $g_i - \widetilde{g}_i \in (p)$, so $(p, g_i(\alpha)) = (p, \widetilde{g}_i(\alpha))$.

Example 3.4.23. Let's convince ourselves that the theorem is true using the previous two theorems. Consider the quadratic case $K = \mathbb{Q}\left(\sqrt{d}\right)$ with $d \not\equiv 1 \bmod 4$ so $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{d}\right]$. Now $\overline{m_\alpha}(x) = x^2 - \overline{d} \in \mathbb{F}_p[x]$. We have following possibilities:

1. If $\overline{m_\alpha}(x) = (x-a)(x-b)$ for some $a, b \in \mathbb{F}_p$ and $a \neq b$, then $p \nmid d$ and a is a root of $\overline{m_\alpha}$ so d is a quadratic residue, so we are in case 2 of 3.4.15, hence $p\mathcal{O}_K = \left(p, a - \sqrt{d}\right)\left(p, a + \sqrt{d}\right)$ which is indeed $\left(p, g_1\left(\sqrt{d}\right)\right)\left(p, g_2\left(\sqrt{d}\right)\right)$; we only need to see that $b = -a$, but this is forced by $(x-a)(x-b) = x^2 - (a+b)x + ab = x^2 - d$. Also note that
$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[x]/(p, x^2 - d) = \mathbb{F}_p[x]/(x^2 - \overline{d}) = \mathbb{F}_p[x]/(x-a)(x-b) = \mathbb{F}_p[x]/(x-a) \times \mathbb{F}_p[x]/(x-b).$$
2. If $\overline{m_\alpha}(x) = (x-a)^2$ for some $a \in \mathbb{F}_p$, then if $p \neq 2$, $x^2 - \overline{d} = (x-a)^2 \implies 2a = 0 \implies a = 0$, and $\overline{m_\alpha}(x) = x^2$. If $p = 2$ then a can be either 0 or 1, i.e. $\overline{m_\alpha}(x)$ is either x^2 or $(x-1)^2$.
   (a) If $p \neq 2$ then $a = 0 \implies \overline{d} = 0 \implies p \nmid d$, so we are in case 1 of 3.4.15, i.e. $p\mathcal{O}_K = \left(p, \sqrt{d}\right)^2$ which is indeed $\left(p, g_1\left(\sqrt{d}\right)\right)^2$.
   (b) If $p = 2$ then we are either in case 1(a) or 2(b) of 3.4.16, and the rest reasoning is similar.

Example 3.4.24. Let's now observe how the theorem applies to a higher degree case. Let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt[3]{2}$ with $m_\alpha(x) = x^3 - 2$. From coursework 1 we know $\mathrm{disc}(\mathbb{Z}[\alpha]) = -27 \cdot 4$, so Dedekind can be applied for any $p \neq 2, 3$ (since $\mathrm{disc}(\mathbb{Z}[\alpha]) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 D_K$). Take $p = 5$. Then $x^3 - \overline{2} = (x-3)(x^2 + 3x - 1)$ which tells us $5\mathcal{O}_K = \left(5, \sqrt[3]{2} - 3\right)\left(5, \left(\sqrt[3]{2}\right)^2 + 3\sqrt[3]{2} - 1\right)$. If $p = 7$ then $x^3 - 2$ is irreducible (check there's no roots), so $7\mathcal{O}_K$ is prime.

Lemma 3.4.25. If $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, then the map $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \to \mathcal{O}_K/p\mathcal{O}_K$ induced by the inclusion $\mathbb{Z}[\alpha] \hookrightarrow \mathcal{O}_K$ is an isomorphism.

Proof. Surjectivity: by Lagrange, $[\mathcal{O}_K : \mathbb{Z}[\alpha]]\mathcal{O}_K \subset \mathbb{Z}[\alpha]$. Moreover, $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ implies that $\exists a, b \in \mathbb{Z} : a[\mathcal{O}_K : \mathbb{Z}[\alpha]] + bp = 1$. Take $x \in \mathcal{O}_K$. Then

$$x + p\mathcal{O}_K = (a[\mathcal{O}_K : \mathbb{Z}[\alpha]] + bp)x + p\mathcal{O}_K = a[\mathcal{O}_K : \mathbb{Z}[\alpha]]x + p\mathcal{O}_K$$

where $a[\mathcal{O}_K : \mathbb{Z}[\alpha]]x \in \mathbb{Z}[\alpha]$.
Injectivity is proved similarly. □

Proof of 3.4.21. From $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(m_\alpha)$ and previous lemma we have

$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(p, m_\alpha) = \mathbb{F}_p[]x]/(\overline{m_\alpha}).$$

Suppose $\overline{m_\alpha}(x) = \overline{g_1}(x)^{e_1} \cdots \overline{g_r}(x)^{e_r}$ where $\overline{g_i}$'s are monic, irreducible and distinct. We first show that $\mathfrak{p}_i = (p, g_i(\alpha))$ is prime by showing $\mathcal{O}_K/\mathfrak{p}_i$ is a field. By above this is $\mathbb{F}_p[x]/(\overline{m_\alpha}, \overline{g_i})$ but $g_i \mid \overline{m_\alpha}$ so it's $\mathbb{F}_p[x]/(\overline{g_i})$ which is a field since $\overline{g_i}$ is assumed to be irreducible. Moreover, $p^{f(\mathfrak{p}_i)} = |\mathcal{O}_K/\mathfrak{p}_i| = |\mathbb{F}_p[x]/(\overline{g_i})| = p^{\deg \overline{g_i}}$, so $f(\mathfrak{p}_i) = \deg \overline{g_i}$.

We now show that $\mathfrak{p}_i$'s are pairwise distinct. Indeed, for $i \neq j$,

$$\mathcal{O}_K(\mathfrak{p}_i + \mathfrak{p}_j) = \mathcal{O}_K/(p, g_i, g_j) = \mathbb{F}_p[x](\overline{g_i}, \overline{g_j}) = 0$$

since $\overline{g_i}, \overline{g_j}$ are monic, irreducible and distinct.

Finally it remains to show $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Clearly $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subset (p, g_1^{e_1}, \dots, g_r^{e_r})$, and by construction $g_1^{e_1} \cdots g_r^{e_r} \equiv m_\alpha \bmod p$, hence

$$g_1^{e_1} \cdots g_r^{e_r}(\alpha) = \underbrace{m_\alpha(\alpha)}_{0} + \underbrace{(g_1^{e_1} \cdots g_r^{e_r} - m_\alpha)(\alpha)}_{\in p\mathcal{O}_K} \in p\mathcal{O}_K,$$

in particular $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subset p\mathcal{O}_K$. But $N_K(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = p^{\deg \overline{g_1}} \cdots p^{\deg \overline{g_r}} = p^{\deg m_\alpha} = N_K(p\mathcal{O}_K)$, so we have equality. □

Week 7, lecture 3, 19th February

Remark 3.4.26. Note that an immediate consequence of 3.4.19 is that only finitely many primes ramify. By partially, we mean we are going to show:

1. If $K = \mathbb{Q}(\alpha)$ then finitely many primes ramify.
2. If a prime p ramifies, then $p \mid D_K$.

Proposition 3.4.27. Let $f \in \mathbb{Z}[x]$ be irreducible and monic. Then for all but finitely many primes p, $\overline{f} \in \mathbb{F}_p[x]$ has no repeated irreducible factors.

Proof. Note that if F is any field and $h \in F[x]$ has $g^2 \mid h$ for $g \in F[x]$, then $g \mid h'$ since if we write $h = g^2 h_1$ then $h' = 2gg'h_1 + g^2 h_1'$. This means if $\gcd(h, h') = 1$, i.e. if $(h) + (h') = F[x]$, then h cannot have any repeated factors.

In our setting, since $f \in \mathbb{Z}[x]$ is irreducible, $(f) + (f') = \mathbb{Q}[x]$, i.e. $\exists g_1, g_2 \in \mathbb{Q}[x] : g_1 f + g_2 f' = 1$. Clear denominators and write $dg_1 f + dg_2 f' = d$ for some $d \in \mathbb{Z}$ and we have $dg_1, dg_2 \in \mathbb{Z}[x]$. But now for all primes p with $p \nmid d$, one has $\overline{dg_1 f} + \overline{dg_2 f} = \overline{d} \in \mathbb{F}_p^\times$, hence $(\overline{f}) + (\overline{f}') = \mathbb{F}_p[x]$, i.e. $\overline{f}$ has no repeated irreducible factors. □

Taking d to be the discriminant of f with 3.4.21, we have proved the first claim in previous remark.

For the second claim, we give a sketch of proof. Suppose p ramifies, i.e. $p\mathcal{O}_K = \mathfrak{p}^1 \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some prime ideal $\mathfrak{p}$. Note that $\mathfrak{p}_i$'s are not necessarily distinct. Take $x \in \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r \backslash p\mathcal{O}_K$. Then $[x]$ in $\mathcal{O}_K/p\mathcal{O}_K$ is nilpotent, since $x^2 \in \mathfrak{p}^2 \mathfrak{p}_1^2 \cdots \mathfrak{p}_r^2 \subset p\mathcal{O}_K$. Take an integral basis $\alpha_1, \dots, \alpha_n$ of $\mathcal{O}_K$ such that $[\alpha_1]$ is nilpotent. But then each $\alpha_1 \alpha_i$ is nilpotent, so $p \mid \mathrm{tr}(\alpha_1 \alpha_i)$. Hence $p \mid D_K$ by definition of discriminant.

4 Cyclotomic fields

Let p be an odd prime and consider $\mathbb{Q}(\zeta_p)$ where ζ_p is a primitive pth root of unity. Explicitly one can have $\zeta_p = e^{\frac{2\pi i}{p}}$. The minimal polynomial of ζ_p is $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$, the cyclotomic polynomial. Recall that using Eisenstein's criteria and the shift $\Phi_p(x+1)$ we can show Φ_p is irreducible.

Proposition 4.0.1. Let $K = \mathbb{Q}(\alpha)$ where α is an algebraic integer and suppose that m_α is Eisenstein at p. Then $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ and $p\mathcal{O}_K = (p, \alpha)^{[K:\mathbb{Q}]}$.

Proof. Write $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. For a contradiction, suppose $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, then $\exists y \in \mathcal{O}_K : y \notin \mathbb{Z}[\alpha], py \in \mathbb{Z}[\alpha]$. Write $py = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$ and so $y = \frac{c_0}{p} + \frac{c_1}{p}\alpha + \cdots + \frac{c_{n-1}}{p}\alpha^{n-1}$. Let i be the minimal such that $c_i \notin p\mathbb{Z}$. Then $\frac{c_i}{p}\alpha^i + \cdots + \frac{c_{n-1}}{p}\alpha^{n-1} \in \mathcal{O}_K$. Multiplying by α^{n-1-i} gives

$$\frac{c_i}{p}\alpha^{n-1} + \frac{\alpha^n}{p}\left(c_{i+1} + \cdots + c_{n-1}\alpha^{n-i-2}\right) \in \mathcal{O}_K,$$

but $\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_0) \in p\mathcal{O}_K$ since m_α is Eisenstein at p, so $\frac{c_i}{p}\alpha^{n-1} \in \mathcal{O}_K$. But

$$N_K\left(\frac{c_i}{p}\alpha^{n-1}\right) = \left(\frac{c_i}{p}\right)^n N_K(\alpha)^{n-1} = \left(\frac{c_i}{p}\right)^n ((-1)^n a_0)^{n-1} = \pm\left(\frac{c_i}{p}\right)^n a_0^{n-1},$$

but since $p^2 \nmid a_0$ (again since m_α is Eisenstein at p), $p^n \nmid a_0^{n-1}$, so $N_K\left(\frac{c_i}{p}\alpha^{n-1}\right) \notin \mathbb{Z}$, a contradiction.

To see the last part, use 3.4.21 on $\overline{m_\alpha} = x^n$. □

Week 8, lecture 1, 24th February: problem class (sheet 3)

Exercise 4.0.2. 5. Let α be a root of x^3+x+1 and let $K=\mathbb{Q}(\alpha)$. We've seen $\operatorname{disc}(\mathbb{Z}[\alpha])=-31$ which implies $\mathcal{O}_K=\mathbb{Z}[\alpha]$. Use Dedekind's criteria to factor $2,3,5$ in $\mathcal{O}_K$.

Solution. First observe that we can apply Dedekind to primes not dividing $[\mathcal{O}_K:\mathbb{Z}[\alpha]]=1$, hence all primes can be factorised, in particular $2,3,5$. Since x^3+x+1 is irreducible it must be the minimal polynomial of α

- Modulo 2 the polynomial looks the same has no roots over $\mathbb{F}_2$, so irreducible and 2 is thus prime.
- Modulo 3 the polynomial looks again the same but has root 1, and indeed can be factorised as $(x-1)(x^2+x-1)$, so $3\mathcal{O}_K=(\alpha,\alpha-1)(\alpha,\alpha^2+\alpha-1)$.
- Modulo 5 the polynomial is again irreducible, so 5 is prime.

Bonus: what about $p=31$? It divides $\mathcal{O}_K$, and we've seen 3.4.19 which in this case says 31 ramifies. Hence we expect $\overline{m_\alpha} \bmod 31$ to have multiple roots, which are roots shared with $\overline{m'_\alpha}=3x^2+1$, which has root 14. We find that $\overline{m_\alpha}=(x-14)^2(x-3)$, and therefore $31\mathcal{O}_K=(\alpha,\alpha-14)^2(\alpha,\alpha-3)$.

6. We give an example of a number field K such that $\mathcal{O}_K\neq\mathbb{Z}[\alpha]$ $\alpha\in\mathcal{O}_K$.

(a) Prove that if $[K:\mathbb{Q}]=3$ and $(2)=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ where $\mathfrak{p}_i$'s are distinct, then $\mathcal{O}_K\neq\mathbb{Z}[\alpha]$ $\forall\alpha\in\mathcal{O}_K$. In fact, $2\mid[\mathcal{O}_K:\mathbb{Z}[\alpha]]$.

(b) Prove that x^3-x^2-2x-8 is irreducible. Let θ be a root of it and denote $K=\mathbb{Q}(\theta)$ and $\theta'=\frac{4}{\theta}$. Prove that $\theta'\in\mathcal{O}_K$.

(c) By showing $\theta^2=\theta+2+2\theta'$ and $(\theta')^2=-\theta'-2+2\theta$, prove that $\mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta'\subset\mathcal{O}_K$ is a subring.

(d) Compute $\operatorname{disc}(1,\theta,\theta')$ and deduce $1,\theta,\theta'$ is an integral basis for $\mathcal{O}_K$.

(e) Prove that as rings, $\mathcal{O}_K/2\mathcal{O}_K\cong\mathbb{F}_2\times\mathbb{F}_2\times\mathbb{F}_2$.

(f) Deduce that $\mathcal{O}_K\neq\mathbb{Z}[\alpha]$ $\forall\alpha\in\mathcal{O}_K$.

Solution.

(a) Since $\mathbb{F}_2$ has only two elements, a degree 3 polynomial cannot factor as three distinct linear polynomials. This doesn't contradict Dedekind only if $2\mid[\mathcal{O}_K:\mathbb{Z}[\alpha]]$ $\forall\alpha\in\mathcal{O}_K$.

(b) Modulo 3 the polynomial has no roots, so irreducible. Note that $\theta^3-\theta^2-2\theta-8=0$ gives

$$1-\frac{1}{\theta}-\frac{2}{\theta^2}-\frac{8}{\theta^3}=0\implies\frac{64}{\theta^3}+\frac{16}{\theta^2}+\frac{8}{\theta}+8=0\implies\frac{4}{\theta}\text{ is a root of }x^3+x^2+2x+8,$$

hence $\theta'\in\mathcal{O}_K$.

(c) The two desired equations can be obtained by multiplying $\theta^3-\theta^2-2\theta-8=0$ by θ^{-1} and $\theta'^3+\theta'^2-2\theta'+8$ by $2\theta^{-2}$.

(d) We find $\operatorname{disc}(1,\theta,\theta')=-503$ is squarefree.

(e) By (c) and (d), $\mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta'\hookrightarrow\mathcal{O}_K$ is in fact a ring isomorphism, so $\mathcal{O}_K/2\mathcal{O}_K\cong\mathbb{F}_2\times\mathbb{F}_2\theta\times\mathbb{F}_2\theta'$. Note that $1+\theta+\theta',\theta,\theta'$ is a full system of orthogonal idempotents; indeed by (c), $\theta\theta'=4\equiv 0 \bmod 2$, $\theta+\theta^2+4=2\theta+2+2\theta'+4\equiv 0 \bmod 2$ and $\theta'+\theta'^2+4=-2+2\theta+4\equiv 0 \bmod 2$, with $\theta^2\equiv\theta \bmod 2$, $\theta'^2=\theta' \bmod 2$ and $(1+\theta+\theta')^2\equiv 1+\theta^2+\theta'^2\equiv 1+\theta+\theta' \bmod 2$.

(f) If (2) ramifies then $\mathcal{O}_K/2\mathcal{O}_K$ has a nilpotent element, contradicting (e) since any product of fields doesn't have nilpotent elements. But if $(2)=\mathfrak{p}\mathfrak{q}$ where $\mathfrak{p}\neq\mathfrak{q}$ are distinct, then $e(\mathfrak{p})f(\mathfrak{p})+e(\mathfrak{q})f(\mathfrak{q})=f(\mathfrak{p})+f(\mathfrak{q})=3$, hence either $f(\mathfrak{p})$ or $f(\mathfrak{q})=2$, so $\mathcal{O}/2\mathcal{O}_K=\mathcal{O}_K/\mathfrak{p}\times\mathcal{O}_K/\mathfrak{q}=\mathbb{F}_4\times\mathbb{F}_2$, again contradicting (e).

Week 8, lecture 2, 25th February

Example 4.0.3. Let $\alpha=\sqrt[3]{2}$ and $K=\mathbb{Q}(\alpha)$. We want to show $\mathcal{O}_K=\mathbb{Z}[\alpha]$. Recall $\operatorname{disc}\mathbb{Z}[\alpha]=-3^2\cdot 2^2$. We claim it is enough to prove $2,3\nmid[\mathcal{O}_K:\mathbb{Z}[\alpha]]$, since together with $\operatorname{disc}\mathbb{Z}[\alpha]=[\mathcal{O}_K:\mathbb{Z}[\alpha]]^2D_K$ it follows that $[\mathcal{O}_K:\mathbb{Z}[\alpha]]=1$, i.e. $\mathcal{O}_K=\mathbb{Z}[\alpha]$. Now $m_\alpha(x)=x^3-2$ which ie Eisenstein at $p=2$, so by 4.0.1 $2\mid[\mathcal{O}_K:\mathbb{Z}[\alpha]]$. For 3, we instead consider the minimal polynomial of $\alpha+\lambda$ where $\lambda\in\mathbb{Z}$. This is indeed valid since $\mathbb{Z}[\alpha]=\mathbb{Z}[\alpha+\lambda]$, and so $m_{\alpha+\lambda}$ Eisenstein at 3 would imply $3\nmid[\mathcal{O}_K:\mathbb{Z}[\alpha]]$ again by 4.0.1. We find that $\lambda=-2$ does the job since $m_{\alpha-2}(x)=m_\alpha(x+2)=(x+2)^3-2=x^3+6x^2+12x+6$.

Exercise 4.0.4. Now in general, let $d \neq \pm 1$ and squarefree, and $K = \mathbb{Q}\left(\sqrt[3]{d}\right)$. First show that $\operatorname{disc}\mathbb{Z}\left[\sqrt[3]{d}\right] = -27d^2$. Is $\mathcal{O}_K = \mathbb{Z}\left[\sqrt[3]{d}\right]$? To show equality, again it's enough to show no prime dividing $-27d^2$ divides $\left[\mathcal{O}_K : \mathbb{Z}\left[\sqrt[3]{d}\right]\right]$. Such prime is either 3 or not 3.

If $p \neq 3$ then $p \mid d$ but then $m_{\sqrt[3]{d}} = x^3 - d$ is Eisenstein at p so by 4.0.1 the equality follows.

If $p = 3$ and $d \not\equiv \pm 1 \bmod 9$, then $m_{\sqrt[3]{d}-d} = (x+d)^3 - d = x^3 + 3dx^2 + 3d^2x + d(d+1)(d-1)$ is Eisenstein at 3, and the equality follows similarly.

But if $p = 3$ and $d \equiv \pm 1 \bmod 9$ then one can check $\frac{\left(\sqrt[3]{d}-d\right)^2}{3} \in \mathcal{O}_K \backslash \mathbb{Z}\left[\sqrt[3]{d}\right]$.

Theorem 4.0.5. $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$ and $D_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{p-1}{2}} p^{p-2}$. Also, $p\mathcal{O}_{\mathbb{Q}(\zeta_p)} = (\zeta_p - 1)^{p-1}$ is principal and totally ramified.

Proof. We first compute $\Phi_p'(\zeta_p)$. Note that $(x-1)\Phi_p(x) = x^p - 1$, so $\Phi_p(x) + (x-1)\Phi_p'(x) = px^{p-1}$, i.e.

$$\Phi_p'(\zeta_p) = \frac{p\zeta_p^{p-1}}{\zeta_p - 1} = \frac{p\zeta_p^{-1}}{\zeta_p - 1},$$

so

$$N_{\mathbb{Q}(\zeta_p)}(\Phi_p'(\zeta_p)) = \frac{N_{\mathbb{Q}(\zeta_p)}(p)}{N_{\mathbb{Q}(\zeta_p)}(\zeta_p)N_{\mathbb{Q}(\zeta_p)}(\zeta_p - 1)} = \frac{p^{[\mathbb{Q}(\zeta_p):\mathbb{Q}]}}{1 \cdot p} = \frac{p^{p-1}}{p} = p^{p-2}.$$

Now since p is odd, $(-1)^p = -1$ and $1^p = 1$, hence $(-1)^{\frac{p(p-1)}{2}} = (-1)^{\frac{p-1}{2}}$, so by 2.4.11, $\operatorname{disc}\mathbb{Z}[\zeta_p] = (-1)^{\frac{p-1}{2}} p^{p-2}$. Now again, to show $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$ and $D_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{p-1}{2}} p^{p-2}$, since $\operatorname{disc}\mathbb{Z}[\zeta_p] = \left[\mathcal{O}_{\zeta_p} : \mathbb{Z}[\zeta_p]\right]^2 D_{\mathbb{Q}(\zeta_p)}$, it suffices to show any prime dividing $\operatorname{disc}\mathbb{Z}[\zeta_p] = (-1)^{\frac{p-1}{2}} p^{p-2}$ (which would be p) does not divide $\left[\mathcal{O}_{\zeta_p} : \mathbb{Z}[\zeta_p]\right]$, but this follows precisely from 4.0.1, that $\Phi_P(x+1)$ is Eisenstein at p and $\mathbb{Z}[\zeta_p] = \mathbb{Z}[\zeta_p - 1]$. Now again by 4.0.1, $p\mathcal{O}_{\mathbb{Q}(\zeta_p)} = p\mathcal{O}_{\mathbb{Q}(\zeta_p - 1)} = (p, \zeta_p - 1)^{p-1}$, but as calculated before, $N_{\mathbb{Q}(\zeta_p)}(\zeta_p - 1) = p$, hence $p \in (\zeta_p - 1)$ and $p\mathcal{O}_{\mathbb{Q}(\zeta_p)} = (\zeta_p - 1)^{p-1}$ as desired. □

We've now seen how p ramifies in the pth cyclotomic field, now let's fix p and see how a general prime q behaves in the pth cyclotomic field.

Theorem 4.0.6. Let $q \in \mathbb{Z}$ be prime and $q \neq p$. Let f be the order of $[q]$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ and $r = \frac{p-1}{f}$. Then $q\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ where $\mathfrak{q}_i$'s are distinct prime ideals with $f(\mathfrak{q}_i) = f$.

Proof. Write $h(x) = x^p - 1$. Then $h'(x) = px^{p-1}$ and note that $-ph(x) + xh'(x) = -px^p + p - px^p = p$. This means h and h' cannot have common roots mod q. Otherwise, if α is a common root, then $0 \equiv p \bmod q$ which contradicts our assumption for q. This means h doesn't have multiple roots mod q, so $\Phi_p(x) = \frac{h(x)}{x-1}$ doesn't either, i.e. $\overline{\Phi_p(x)} = g_1 \cdots g_r$ in $\mathbb{F}_q[x]$ for some r where g_i's are distinct irreducible polynomials.

Now $\mathbb{F}_q[x]/(g_i) = F_i$ has cardinality $q^{\deg g_i}$, hence for any $a \in F_i^\times$, by Lagrange, $a^{q^{\deg g_i}-1} = 1$. In particular, take $a = [x] \in F_i^\times$, and $[x]^p = 1$ since $g_i(x) \mid x^p - 1$. This means $p \mid q^{\deg g_i} - 1$, i.e. $q^{\deg g_i} \equiv 1 \bmod p$. By our construction of f, this implies $f \mid \deg g_i$. To prove the theorem, it now suffices to show $f = \deg g_i$, which would imply $\deg g_i$'s are the same and hence $p - 1 = \deg g_i r = fr$, thus r is indeed the $r = \frac{p-1}{f}$ we constructed.

Consider the subfield $\widetilde{F_i} = \{b \in F_i : b^{q^f} = b\}$ of F_i. Then $\widetilde{F_i}$ contains $[x]$: indeed, $a \in \widetilde{F_i} \impliedby a(a^{q^f-1} - 1) = 0 \impliedby a^{q^f-1} = 1 \impliedby a^{p\lambda} - 1 = 0$ for some $\lambda \in \mathbb{Z}$ (since $qf = 1 \bmod p$ by construction), and we saw that $[x]^p = 1$. Hence $\widetilde{F_i} = F_i$, so $q^{\deg g_i} = |F_i| = |\widetilde{F_i}| \leq q^f$, i.e. $\deg g_i \leq f$, but $f \mid \deg g_i$ in particular implies $f \leq \deg g_i$, hence $f = \deg g_i$ as desired. □

Week 8, lecture 3, 26th February

4.1 Quadratic reciprocity

If a quadratic field K lives inside a cyclotomic field $\mathbb{Q}(\zeta_p)$, that we may be able to read information on splitting in K from $\mathbb{Q}(\zeta_p)$. In fact one can always find such an embedding:

Lemma 4.1.1. $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right) \subset \mathbb{Q}(\zeta_p)$.

Proof. The roots of $\Phi_p(x)$ are $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$, so the embeddings $\tau_1, \dots, \tau_p : \mathbb{Q}(\zeta_p) \to \mathbb{C}$ are given by $\tau_i : \zeta_p \mapsto \zeta_p^i$. Also, by 4.0.5, $\left\{\zeta_p, \dots, \zeta_p^{p-1}\right\}$ is an integral basis of $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$. Again according to 4.0.5,

$$D_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{p-1}{2}} p^{p-2} = \det(\tau_i(\zeta_p^j))_{ij}^2 = \det\left(\zeta_p^{ij}{}_{ij}\right)^2,$$

and dividing both sides by p^{p-3} gives $(-1)^{\frac{p-1}{2}} p = \left(\frac{\det\left(\zeta_p^{ij}{}_{ij}\right)}{p^{\frac{p-3}{2}}}\right)^2$ where $\frac{\det\left(\zeta_p^{ij}{}_{ij}\right)}{p^{\frac{p-3}{2}}} \in \mathbb{Q}(\zeta_p)$, hence $\sqrt{(-1)^{\frac{p-1}{2}} p} \in \mathbb{Q}(\zeta_p)$, so $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right) \subset \mathbb{Q}(\zeta_p)$ as desired. □

Exercise 4.1.2. Show that this is the only thing we can do: if $K \subset \mathbb{Q}(\zeta_p)$ is a quadratic field, then the only prime that can ramifies in K is p and $K = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$.

From now on, for an odd prime p, we denote $p^* = \sqrt{(-1)^{\frac{p-1}{2}} p}$. Note that $p^* \equiv 1 \bmod 4$: if $p \equiv 1 \bmod 4$ then $\frac{p-1}{2}$ is even and $p^* = p$, and if $p \equiv 3 \bmod 4$ then $\frac{p-1}{4}$ is odd and $p^* = -p$.

Lemma 4.1.3. Let $q \in \mathbb{Z}$ be prime and $q \neq p$. Let f be the order of $[q]$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ and $r = \frac{p-1}{f}$, which we now know is the number of prime factors of $q\mathbb{Z}[\zeta_p]$. Then

1. If q splits in $\mathbb{Q}(\sqrt{p^*})$ then r is even.
2. If $p \equiv 3 \bmod 4$ then the converse also holds.

Remark 4.1.4. Since $p^* \equiv 1 \bmod 4$, $D_{\mathbb{Q}(\sqrt{p^*})} = p^*$, so if $q \neq p$ then $q \nmid D_{\mathbb{Q}(\sqrt{p^*})}$, hence q does not ramify in $D_{\mathbb{Q}(\sqrt{p^*})}$. So this lemma does almost describe everything about behaviour of q in the quadratic field (knowing about the ambient cyclotomic field).

Proof.
1. q splits means $q\mathcal{O}_{\mathbb{Q}(\sqrt{p^*})} = \mathfrak{q}\overline{\mathfrak{q}}$, hence $q\mathbb{Z}[\zeta_p] = (\mathfrak{q}\mathbb{Z}[\zeta_p])(\overline{\mathfrak{q}}\mathbb{Z}[\zeta_p])$. We prove that $\mathfrak{q}\mathbb{Z}[\zeta_p]$ and $\overline{\mathfrak{q}}\mathbb{Z}[\zeta_p]$ have the same number of factors. Take $\tau_0 : \mathbb{Q}(\sqrt{p^*}) \to \mathbb{C} : x \mapsto \overline{x}$. By 2.3.26, there is an embedding $\tau : \mathbb{Q}(\zeta_p) \to \mathbb{C}$ that restricts to τ_0. Note that τ is of the form $\zeta_p \mapsto \zeta_p^i$ for some i; $\tau(\mathbb{Q}(\zeta_p)) = \mathbb{Q}(\zeta_p)$; and $\tau(\mathbb{Z}[\zeta_p]) = \mathbb{Z}[\zeta_p]$. Then $\tau(\mathfrak{q}\mathbb{Z}[\zeta_p]) = \tau(\mathfrak{q})\mathbb{Z}[\zeta_p]$, but $\mathfrak{q}$ is an ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{p^*})}$, so this is $\tau_0(\mathfrak{q})\mathbb{Z}[\zeta_p] = \overline{\mathfrak{q}}\mathbb{Z}[\zeta_p]$. Hence $\{\mathfrak{q}\mathbb{Z}[\zeta_p]\}$ and $\{\overline{\mathfrak{q}}\mathbb{Z}[\zeta_p]\}$ are in bijection, so in particular have the same number of factors.
2. For a contradiction, suppose q does not split. Recall 3.4.8 which says this means $f = f(q) = 2$, in particular even. But $rf = p - 1$ and since $p \equiv 3 \bmod 4$, this implies r is odd.

□

Lemma 4.1.5. Let p be an odd prime. Then

1. $\forall a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,
2. $\left(\frac{a}{p}\right) = 1 \iff r = \frac{p-1}{f}$ is even where f is the order of $[a] \in (\mathbb{Z}/p\mathbb{Z})^\times$,
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Theorem 4.1.6 (Gauss' reciprocity law)**.** Let p, q be distinct odd primes, then

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Equivalently,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. If $\left(\frac{D_{\mathbb{Q}(\sqrt{p^*})}}{q}\right) = \left(\frac{p^*}{q}\right) = 1$, by 3.4.15 q splits, so by 4.1.3 r is even, hence by 4.1.5 $\left(\frac{q}{p}\right) = 1$. □

Week 9, lecture 1, 3rd March

5 Class groups, reprise

5.1 Finiteness of class groups

Theorem 5.1.1. The class group $\mathrm{Cl}(\mathcal{O}_K)$ of a number field K is finite.

Lemma 5.1.2. For any $c \in \mathbb{R}_{>0}$, the number of ideals $I \subset \mathcal{O}_K$ with $N_K(I) \leq c$ is finite.

Proof. Let $I \subset \mathcal{O}_K$ and write $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ where $\mathfrak{p}_i$'s are distinct prime ideals and $e_i \geq 1$. We prove the finiteness by first bounding r and then bounding the number of primes $p \in \mathbb{Z} \cap I$.

The only ideal with norm one is the whole ring $\mathcal{O}_K$ since $[\mathcal{O}_K : I] = 1 \iff I = \mathcal{O}_K$, so assume $N_K(\mathfrak{p}_i) \geq 2$, hence $2^{e_1+\cdots+e_r} \leq N_K(I) \leq c$, i.e. $r \leq e_1 + \cdots + e_r \leq \log_2(c)$.

Now each $\mathfrak{p}_i$ lies above some $p \in \mathbb{Z}$, so $c \geq N_K(I) \geq N_K(\mathfrak{p}_i) = p^{f(\mathfrak{p}_i)} \geq p$, hence the number of possible such p's is finite. But then by 3.4.2, for each such p, the number of prime ideals lying above p is also finite. □

Lemma 5.1.3. Let K be a number field and suppose there is a constant $c \in \mathbb{R}_{>0}$ such that $\forall$ nonzero ideal $I \subset \mathcal{O}_K$, $\exists 0 \neq \alpha \in I : |N_K(\alpha)| \leq cN_K(I)$, then $\forall [I] \in \mathrm{Cl}(\mathcal{O}_K)$, $\exists I' \subset \mathcal{O}_K : [I] = [I']$ and $N_K(I') \leq c$.

If we can find such a constant for K then together with 5.1.2, the lemma implies the desired 5.1.1.

Proof. Suppose $[I]^{-1} = [J]$. Then $\exists 0 \neq \alpha \in J : |N_K(\alpha)| \leq cN_K(J)$, and by 3.2.13 we have ideal I' with $JI' = (\alpha)$. Now $[I'] = [J]^{-1} = [I]$ by definition of class groups, and $N_K(J)N_K(I') = N_K(JI') = N_K((\alpha)) = |N_K(\alpha)| \leq N_K(J)$ by 3.4.10, so $N_K(I') \leq c$. □

Definition 5.1.4. An embedding $\tau : K \hookrightarrow \mathbb{C}$ of a number field K is *real* if $\tau(K) \subset \mathbb{R}$. Denote by r the number of real embeddings. If $\tau : K \hookrightarrow \mathbb{C}$ is not real then it's *complex*, and $\overline{\tau} : \alpha \mapsto \overline{\tau(\alpha)}$ is a different embedding, so complex embeddings always come in pairs. Denote by s the number of pairs of complex embeddings. By 2.3.26, one can write $n = [K : \mathbb{Q}] = |\sigma_K| = r + 2s$.

Theorem 5.1.5 (Minkowski's bound)**.** For a number field K, the constant

$$C_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|D_K|}$$

satisfies the condition in previous lemma.

Example 5.1.6. Before proving this let's see how useful it is. In the quadratic case $K = \mathbb{Q}\left(\sqrt{d}\right)$, if $d < 0$ then $r = 0, s = 1$ and

$$C_K = \frac{2!}{2^2}\frac{4}{\pi}\sqrt{|D_K|} = \frac{2}{\pi}\sqrt{|D_K|} = \begin{cases} \dfrac{2}{\pi}\sqrt{-4d} = \dfrac{4}{\pi}\sqrt{-d} & \text{if } d \not\equiv 1 \bmod 4 \\ \dfrac{2}{\pi}\sqrt{-d} & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

and if $d > 0$ then $r = 2, s = 0$ and

$$C_K = \frac{2!}{2^2}\sqrt{|D_K|} = \frac{1}{2}\sqrt{|D_K|} = \begin{cases} \dfrac{1}{2}\sqrt{4d} = \sqrt{d} & \text{if } d \not\equiv 1 \bmod 4 \\ \dfrac{1}{2}\sqrt{d} & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

For instance, take $K = \mathbb{Q}\left(\sqrt{-5}\right)$, $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-5}\right]$, then $C_K = \frac{4}{\pi}\sqrt{5} < 3$, so $\mathrm{Cl}(\mathcal{O}_K) = \{[I] : N_K(I) \leq 2\}$ by 5.1.3. Since we've seen $(2) = \left(2, 1+\sqrt{-5}\right)^2 = \mathfrak{p}_2^2$, by 3.4.2 $\mathfrak{p}_2$ is the only ideal of norm 2, so $\mathrm{Cl}(\mathcal{O}_K) = \{[\mathcal{O}_K], [\mathfrak{p}_2]\} = \mathbb{Z}/2\mathbb{Z}$.

Theorem 5.1.7. $\mathcal{O}_{-19}$, $\mathcal{O}_{-43}$, $\mathcal{O}_{-67}$, $\mathcal{O}_{-163}$ are PIDs.

Proof. By 3.3.5 it suffices to show $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$ in each case. Note that $-19, -43, -67, -163 \equiv 1 \bmod 4$, so the constants C_K are approximately 2.8, 4.2, 5.2 and 8.1 respectively. Let's look at $\mathcal{O}_{-163}$ in particular and the rest follows from a similar process.

We need to check there is no non-principal ideal of norm ≤ 8, which by the proof of 5.1.2 is generated by prime ideals lying above $2, 3, 5, 7$.

- 2: by 3.4.16 and the fact that $-163 \equiv 5 \bmod 8$, (2) is prime and hence the only ideal lying above 2 is principal.
- 3: by 3.4.15 and the fact that $3 \nmid 163$ with $\nexists a : a^2 \equiv 2 \bmod 3$, (3) is prime.
- 5: similarly, $5 \nmid 163$ and $\nexists a : a^2 \equiv 2 \bmod 5$.
- 7: similarly, $7 \nmid 163$ and $\nexists a : a^2 \equiv 5 \bmod 7$.

□

5.2 Proof of Minkowski's bound using lattices

Definition 5.2.1. A *lattice* is a subgroup $\Lambda \subset \mathbb{R}^n$ with basis $v_1, \ldots, v_n$ as a $\mathbb{Z}$-module which is also a basis of $\mathbb{R}^n$ as an R-vector space.

Example 5.2.2.

- $\mathbb{Z}^n \subset \mathbb{R}^n$ is a lattice (take the standard basis).
- $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \subset \mathbb{C} \xrightarrow{\sim} \mathbb{R}^2 : z \mapsto (\Re(z), \Im(z))$ is a lattice if $d < 0$ by taking $\{1, \sqrt{d}\}$ if $d \equiv 1 \bmod 4$ and $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ if $d \not\equiv 1 \bmod 4$.

Definition 5.2.3. The *fundamental parallelotope* of a lattice $\Lambda \subset \mathbb{R}^n$ with respect to basis $v_1, \ldots, v_n$ is the set

$$P(v_1, \ldots, v_n) = \left\{ \sum_{i=1}^{n} c_i v_i : 0 \le c_i \le 1 \right\}.$$

Remark 5.2.4.

- It's clear that $P(v_1, \ldots, v_n)$ is a fundamental domain for the lattice, i.e.

$$\mathbb{R}^n = \bigsqcup_{v \in \Lambda} (v + P(v_1, \ldots, v_n)).$$

- Recall that from linear algebra $\operatorname{vol}(P(v_1, \ldots, v_n)) = |\det A|$ where $A = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix}$

Lemma 5.2.5. If $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ are two $\mathbb{Z}$-basis for a lattice $\Lambda \subset \mathbb{R}^n$, then $\operatorname{vol}(P(v_1, \ldots, v_n)) = \operatorname{vol}(P(w_1, \ldots, w_n))$.

Proof. Recall again from linear algebra that determinant of a matrix is invariant under change of basis. □

Definition 5.2.6. Define the *covolume* of a lattice $\Lambda \subset \mathbb{R}^n$ to be $\operatorname{covol}(\Lambda) = \operatorname{vol}(P(v_1, \ldots, v_n))$ where v_i's can be any basis for Λ by previous lemma. Then $\operatorname{covol}(\Lambda) = \operatorname{vol}(\mathbb{R}^n / \Lambda)$.

Week 9, lecture 2, 4th March

Lemma 5.2.7. Let $\Lambda \in \mathbb{R}^n$ be a lattice and $S \subset \mathbb{R}^n$ a measurable set. If $\operatorname{vol}(S) > \operatorname{covol}(\Lambda)$, then $\exists x, y \in S : 0 \neq x - y \in \Lambda$.

Proof. Fix a basis $v_1, \ldots, v_n$ for Λ and let $P = P(v_1, \ldots, v_n)$. Write

$$\mathbb{R}^n = \bigsqcup_{v \in \Lambda} (v + P) \quad \text{and hence} \quad S = \bigsqcup_{v \in \Lambda} (v + P) \cap S,$$

so

$$\operatorname{vol}(S) = \sum_{v \in \Lambda} \operatorname{vol}((v + P) \cap S) = \sum_{v \in \Lambda} \operatorname{vol}(P \cap (S - v)).$$

If the sets $P \cap (S - v)$ are pairwise disjoint over $v \in \Lambda$ then by the equation above, $\operatorname{vol}(S) \le \operatorname{vol}(P) = \operatorname{covol}(\Lambda)$, contradicting assumption. This means $(S - v) \cap (S - w) \neq \varnothing$ for some $v \neq w \in \Lambda$. Take $a \in (S - v) \cap (S - w)$, then $a + v, a + w \in S$, so $(a + v) - (a - w) = v - w \in \Lambda$. □

Theorem 5.2.8 (Minkowski)**.** Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $S \subset \mathbb{R}^n$ be measurable, convex, symmetric (i.e. $x \in S \implies -x \in S$) subset. If $\operatorname{vol}(S) > 2^n \operatorname{covol}(\Lambda)$, then $\exists 0 \neq x \in S \cap \Lambda$.

Proof. Apply the previous lemma to $\frac{1}{2}S = \left\{\frac{s}{2} : s \in S\right\}$. Since S is symmetric, $\operatorname{vol}\left(\frac{1}{2}S\right) = \frac{1}{2^n}\operatorname{vol}(S) > \operatorname{covol}(\Lambda)$, so $\exists x, y \in \frac{1}{2}S : 0 \neq x - y \in \Lambda$. Hence $2x, 2y \in S$ and $\frac{1}{2}(2x) + \frac{1}{2}(-2y) = x - y \in S$ by symmetry and convexity, so $x - y \in S \cap \Lambda$. □

Lemma 5.2.9. Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $\Lambda' \subset \Lambda$ a subgroup of finite index. Then Λ' is also a lattice and $\operatorname{covol}(\Lambda') = [\Lambda : \Lambda'] \operatorname{covol}(\Lambda)$.

Proof. Omitted; similar to 2.4.7. □

Remark 5.2.10. If we can embed $\mathcal{O}_K$ into $\mathbb{R}^n$ as a lattice Λ via $\tau : \mathcal{O}_K \xrightarrow{\sim} \Lambda$ where $n = [K : \mathbb{Q}]$ (we choose n since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n; this was 2.3.19), then for an ideal $I \subset \mathcal{O}_K$, $N_K(I) = |\mathcal{O}_K/I| = |\Lambda/\tau(I)|$, so by 5.2.9 $\tau(I)$ is a lattice and $\operatorname{covol}(\tau(I)) = N_K(I) \operatorname{covol}(\mathcal{O}_K)$.

Theorem 5.2.11 (Minkowski bound for imaginary quadratic case)**.** Fix squarefree $d < 0$ and let $K = \mathbb{Q}\left(\sqrt{d}\right)$. For any nonzero ideal $I \subset \mathcal{O}_K$, $\exists 0 \neq \alpha \in I$ such that

$$|N_K(\alpha)| \leq \left(\frac{2}{\pi}\sqrt{|D_K|}\right) N_K(I),$$

thus making the Minkowski bound $C_K = \frac{2}{\pi}\sqrt{|D_K|}$, agreeing with 5.1.5 and our calculation in 5.1.6.

Proof. Embed $\mathcal{O}_K \hookrightarrow \mathbb{R}^2$ as lattice Λ as mentioned in 5.2.2. Then if $d \not\equiv 1 \bmod 4$ then $\operatorname{covol}(\Lambda) = |1(\sqrt{-d})| = \sqrt{-d} = \frac{\sqrt{-4d}}{2} = \frac{\sqrt{|D_K|}}{2}$; and if $d \equiv 1 \bmod 4$ then $\operatorname{covol}(\Lambda) = \left|-\frac{\sqrt{-d}}{2}\right| = \frac{\sqrt{-d}}{2} = \frac{\sqrt{|D_K|}}{2}$, so either case we have the same result with respect to the discriminant.
Take $S_R = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 \leq R\}$, a circle (hence convex and symmetric) with $\operatorname{vol}(S_R) = \pi R$. Take an ideal $I \subset \mathcal{O}_D$, and hence a lattice with $\operatorname{covol}(I) = N_K(I)\frac{\sqrt{|D_K|}}{2}$ by 5.2.9. If $\pi R > 2^2 N_K(I)\frac{\sqrt{|D_K|}}{2} = 2\sqrt{|D_K|}N_K(I)$, i.e. $R > \frac{2}{\pi}\sqrt{|D_K|}N_K(I)$, then by 5.2.8 $\exists 0 \neq \alpha \in I \cap S_R$, where $\alpha \in S_R \iff N_K(\alpha) = \Re(\alpha)^2 + \Im(\alpha)^2 \leq R$. □

Remark 5.2.12. With the real case ($d > 0$), we use another embedding $\iota : \mathcal{O}_K \to \mathbb{R}^2 : \alpha \mapsto (\tau_1(\alpha), \tau_2(\alpha))$ where τ_i's are the two real embeddings of $\mathbb{Q}\left(\sqrt{d}\right) \hookrightarrow \mathbb{C}$. Then

1. $\iota(\mathcal{O}_K) \subset \mathbb{R}^2$ is a lattice with covol $= \sqrt{|D_K|}$ (follows from 2.4.9 and 2.4.5),
2. $\forall I \subset \mathcal{O}_K,\ \iota(I) \subset \mathbb{R}^2$ is a lattice with $\operatorname{covol}(\iota(I)) = N_K(I)\sqrt{|D_K|}$ (follows from 5.2.9).

Week 9, lecture 3, 5th March

If we were to play the same game with imaginary case, the natural choice for S_R would be $\{(x,y) \in \mathbb{R}^2 : |xy| \leq R\}$ since $N_K(\alpha) = \tau_1(\alpha)\tau_2(\alpha)$ for $\alpha \in \mathcal{O}_K$ (2.3.28), but this is not convex. Instead we take a subset of it which still works for the norm argument: $S_R = \{(x,y) \subset \mathbb{R}^2 : |x| + |y| \leq 2\sqrt{R}\}$, a square with side length $2\sqrt{2R}$ (hence convex and symmetric) with $\operatorname{vol}(S_R) = 8R$. Indeed $(x,y) \in S_R \implies |xy| < R$ since $|xy| \leq \left(\frac{|x|+|y|}{2}\right)^2 \leq R$.

If $8R > 2^2 N_K(I) N_K(I)\sqrt{|D_K|}$, i.e. $R > \frac{1}{2}N_K(I)\sqrt{|D_K|}$, then by 5.2.8 $\exists 0 \neq \alpha \in I \cap S_R$ where $\alpha \in S_R \implies N_K(\alpha) \leq R$. Hence similarly, the Minkowski bound in this case is $C_K = \frac{1}{2}\sqrt{|D_K|}$, again agreeing with 5.1.6.

Remark 5.2.13 (Minkowski in general)**.** Let K be a number field with $[K : \mathbb{Q}] = n = r + 2s$ and write

$$\Sigma_K = \{\tau_1, \ldots, \tau_r, \sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s}\}.$$

Embed the number field as a lattice using

$$\iota : K \hookrightarrow \mathbb{R}^n : \alpha \mapsto (\tau_1(\alpha), \ldots \tau_r(\alpha), \Re(\sigma_1(\alpha)), \Im(\sigma_1(\alpha)), \ldots, \Re(\sigma_s(\alpha)), \Im(\sigma_s(\alpha))).$$

We claim $\iota(\mathcal{O}_K)$ is indeed a lattice with $\operatorname{covol}(\iota(\mathcal{O}_K)) = \frac{\sqrt{|D_K|}}{2^s}$. Indeed, fix an integral basis $\alpha_1, \ldots, \alpha_n$ of $\mathcal{O}_K$. It suffices to calculate

$$\det \begin{pmatrix} \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \tau_r(\alpha_1) & \cdots & \tau_r(\alpha_n) \\ \Re(\sigma_1(\alpha_1)) & \cdots & \Re(\sigma_1(\alpha_n)) \\ \vdots & \ddots & \vdots \\ \Re(\sigma_s(\alpha_1)) & \cdots & \Re(\sigma_s(\alpha_n)) \end{pmatrix},$$

since if it's nonzero then by definition $\iota(\mathcal{O}_K)$ is a lattice, and its absolute value is the covolume. But by the identities $\Re(z) = \frac{z+\overline{z}}{2}$, $\Im(z) = \frac{z-\overline{z}}{2i}$, we have that the above matrix is equal to

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & \frac{1}{2} & \frac{1}{2} & & & \\ & & & \frac{1}{2i} & -\frac{1}{2i} & & & \\ & & & & & \ddots & & \\ & & & & & & \frac{1}{2} & \frac{1}{2} \\ & & & & & & \frac{1}{2i} & -\frac{1}{2i} \end{pmatrix} \begin{pmatrix} \tau_1(\alpha_1) & \cdots & \tau_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \tau_r(\alpha_1) & \cdots & \tau_r(\alpha_n) \\ \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \overline{\sigma_1}(\alpha_1) & \cdots & \overline{\sigma_1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \cdots & \sigma_s(\alpha_n) \\ \overline{\sigma_s}(\alpha_1) & \cdots & \overline{\sigma_s}(\alpha_n) \end{pmatrix}$$

with determinant

$$\left(\frac{1}{-4i} - \frac{1}{4i}\right)^s \sqrt{D_K} = \left(\frac{i}{2}\right)^2 \sqrt{D_K}$$

by 2.4.9, and hence $\operatorname{covol}(\iota(\mathcal{O}_K)) = \left|\left(\frac{i}{2}\right)^2 \sqrt{D_K}\right| = \frac{\sqrt{|D_K|}}{2^s}$ as desired.

Similarly we would want to work with

$$M_R = \left\{(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) \in \mathbb{R}^n : \prod_{i=1}^{r} |x_i| \prod_{i=1}^{s} \left(y_i^2 + z_i^2\right) \leq R\right\}$$

but it's not generally convex, so we use

$$S_R = \left\{(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) \in \mathbb{R}^n : \sum_{i=1}^{r} |x_i| + \sum_{i=1}^{s} 2\sqrt{y_i^2 + z_i^2} \leq nR^{\frac{1}{n}}\right\}$$

It's left as an multivariable calculus exercise to show $S_R \subset M_R$ and $\operatorname{vol}(S_R) = \frac{n^n}{n!} 2^r \left(\frac{\pi}{2}\right)^s R$. Now if

$$\frac{n^n}{n!} 2^r \left(\frac{\pi}{2}\right)^s R > 2^n \frac{\sqrt{|D_K|}}{2^s} N_K(I) \iff \frac{n^n}{n!} \pi^s R > 2^{2s} \sqrt{|D_K|} N_K(I) \iff R > \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|D_K|} N_K(I)$$

then by 5.2.8 $\exists 0 \neq \alpha \in I \cap S_R$ where $\alpha \in S_R \implies N_K(\alpha) \leq R$.

5.3 Computation of class groups

Example 5.3.1. Let's use this to compute $\mathrm{Cl}(\mathcal{O}_{-14})$. Since $-14 \not\equiv 1 \bmod 4$, $\mathcal{O}_{-14} = \mathbb{Z}\left[\sqrt{-14}\right]$. The Minkowski bound is $\frac{2}{\pi}\sqrt{4 \times 14} = \frac{4}{\pi}\sqrt{14} \approx 4.76$. Hence $\mathrm{Cl}(\mathcal{O}_{-14)}$ is generated by $[\mathfrak{p}]$ where $\mathfrak{p}$ is prime with $N_K(\mathfrak{p}) < 5$. Now $(2) = \left(2, \sqrt{-14}\right)^2 = \mathfrak{p}_2^2$ and $(3) = \left(3, 1+\sqrt{-14}\right)\left(3, 1-\sqrt{-14}\right) = \mathfrak{p}_3\overline{\mathfrak{p}_3}$. By the norm argument one can check $\mathfrak{p}_2, \mathfrak{p}_3, \overline{\mathfrak{p}_3}$ are all non-principal. This means $[\mathfrak{p}_2], [\mathfrak{p}_3], [\overline{\mathfrak{p}_3}] \neq 1 \in \mathrm{Cl}(\mathcal{O}_{-14})$. But are they three distinct classes?

Suppose $[\mathfrak{p}_2] = [\mathfrak{p}_3]$, then $[\mathfrak{p}_3]^{-1}[\mathfrak{p}_3] = 1$, but $[\mathfrak{p}_2]^2 = 1$, i.e. $[\mathfrak{p}]$ is its own inverse, so $[\mathfrak{p}_2][\mathfrak{p}_3] = 1$, i.e. $\mathfrak{p}_2\mathfrak{p}_3$ is principal. But $N_K(\mathfrak{p}_2\mathfrak{p}_3) = 6$ and again by the norm argument this is not possible. Similarly $[\mathfrak{p}_2] \neq [\overline{\mathfrak{p}_3}]$.

Now suppose $[\mathfrak{p}_3] = [\overline{\mathfrak{p}_3}]$, then $[\mathfrak{p}_3]^2 = 1$; write $\mathfrak{p}^3 = (\alpha)$, then $N_K(\alpha) = 9$, so $\alpha = \pm 3$ and we have $\mathfrak{p}_3^2 = (3) = \mathfrak{p}_3\overline{\mathfrak{p}_3}$, so by 3.2.12 $\mathfrak{p}_3 = \overline{\mathfrak{p}_3}$, a contradiction.

Hence we have one element of order 2 and two elements of order 4 in $\mathrm{Cl}(\mathcal{O}_{-14})$; this can only be $\mathbb{Z}/4\mathbb{Z}$.

Example 5.3.2. Let $K = \mathbb{Q}\left(\sqrt{33}\right)$ and write $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{33}}{2}\right]$. The Minkowski bound is $\frac{\sqrt{|D_K|}}{2} = \frac{33}{2} < 3$, so it suffices to see how (2) splits. By 3.4.16, $(2) = \left(2, \frac{1+\sqrt{33}}{2}\right)\left(2, \frac{1-\sqrt{33}}{2}\right) = \mathfrak{p}_2\overline{\mathfrak{p}_2}$. But $\mathfrak{p}_2$ is principal: note that

$$N_K\left(a + b\left(\frac{1+\sqrt{33}}{2}\right)\right) = N_K\left(\frac{2a+b}{2} + \frac{b}{2}\sqrt{33}\right) = \frac{4a^2 + 4ab + b^2}{4} - 33\frac{b^2}{4} = a^2 + ab - 8b^2,$$

and $a^2 + ab - 8b^2 = \pm 2$ does have solution $a = 2, b = 1$, with $2 + \frac{1+\sqrt{33}}{2} \in \mathfrak{p}_2$, so $\mathfrak{p}_2 = \left(2 + \frac{1+\sqrt{33}}{2}\right)$. It follows that $[\overline{\mathfrak{p}_2}] \cdot 1 = 1$, i.e. $\overline{\mathfrak{p}_2}$ is principal as well, hence $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$ and in particular $\mathcal{O}_K$ is a PID by 3.3.5.

Week 10, lecture 1, 10th March: problem class (sheet 4)

Exercise 5.3.3. 5. At the end of this problem we will have proved that if $\mathcal{O}_d = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a PID for $d < 0$ then either $d = -1, -2, -7$, or $d \equiv 5 \bmod 8$ and $-d$ is prime.

(a) Suppose $\mathcal{O}_d$ is a PID. Show that $\mathcal{O}_d$ has elements of norm 2 iff $d = -1, -2, -7$, and deduce that if $\mathcal{O}_d$ has no norm 2 elements, 2 must be inert in $\mathcal{O}_d$ (and so $d \equiv 5 \bmod 8$ by 3.4.16).

(b) It now remains to show that in the case that $\mathcal{O}_d$ has no norm 2 elements, $-d$ is prime. We first show this: if $d \equiv 1 \bmod 4$ and a prime p is the norm of some element, then $p \geq \frac{1-d}{4}$. Deduce that any prime $p < \frac{1-d}{4}$ is inert in $\mathcal{O}_d$.

(c) Deduce that if $d \equiv 5 \bmod 8$ then $-d$ is prime.

(d) Prove that $n^2 - n + 41$ is prime for $1 \leq n \leq 40$ by using $\mathcal{O}_{-163}$ is a PID.

Solution.

(a) If $d \not\equiv 1 \bmod 4$ then $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$ and $N\left(a + \sqrt{d}b\right) = a^2 - db^2$, hence either $b = 0$ and $N\left(a + \sqrt{d}b\right)$ is a square, or $b \neq 0$ and $N\left(a + \sqrt{d}b\right) \geq -d$. If $d \equiv 1 \bmod$ then $\mathcal{O}_d = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ and $N\left(a + b\frac{1+\sqrt{d}}{2}\right) = a^2 + ab + \left(\frac{1-d}{4}\right)b^2$, hence again either $b = 0$ and $N\left(a + b\frac{1+\sqrt{d}}{2}\right)$ is a square, or $b \neq 0$ and $N\left(a + b\frac{1+\sqrt{d}}{2}\right) \geq \frac{1-d}{4}$.

Hence we cannot exclude elements of norm 2 if $d \geq -2$ and $d \not\equiv 1 \bmod 4$ or $d \geq -7$ and $d \equiv 1 \bmod 4$, i.e. $d = -1, -2$ or $-3, -7$. Now indeed $1 + i \in \mathcal{O}_{-1}$, $\sqrt{-2} \in \mathcal{O}_{-2}$ and $1 - \sqrt{-7} \in \mathcal{O}_{-7}$ has norm 2, but we claim $a^2 + ab + b^2 = 2$ has no integer solutions so $\mathcal{O}_{-3}$ has no norm 2 elements after all, i.e. $\mathcal{O}_d$ has no norm 2 elements unless $d = -1, -2, -7$ as desired.

To prove that last claim, suppose per contra $a, b \in \mathbb{Z}$ satisfies $a^2 + ab + b^2 = (a + b)^2 - ab = 2$, then $(a + b)^2$ and ab are either both even or both odd. If ab is even then WLOG a is even, but then $a^2 + b^2$ being forces b to be even, so $\frac{a}{2}, \frac{b}{2}$ is another solution. Infinite descent gives a contradiction, so suppose ab is odd. Then both a and b are odd, so a^2 and b^2 are odd, but then $a^2 + b^2$ is even, another contradiction.

Now assume $d \neq -1, -2, -7$ and suppose per contra 2 is not inert in $\mathcal{O}_d$. If $2\mathcal{O}_d = \mathfrak{p}_2^2$ (ramifies) or $2\mathcal{O}_d = \mathfrak{p}_2\overline{\mathfrak{p}_2}$ (splits), then $N(\mathfrak{p}_2) = 2$ so since $\mathcal{O}_d$ has no norm 2 elements, $\mathfrak{p}_2$ is not principal, contradicting that $\mathcal{O}_D$ is a PID. Hence 2 is inert.

(b) We already know if $d \equiv 1 \bmod 4$ then $N(\alpha)$ is either a square or $\geq \frac{1-d}{4}$ for any $\alpha \in \mathcal{O}_d$, and clearly a prime is never a square, so the first part is proved. p cannot ramify or split by the same argument for 2 in the last paragraph of (a).

(c) Suppose per contra $-d$ is not prime. We claim it has a prime factor $p \leq \frac{-d}{5}$. Indeed, since $d \equiv 5 \bmod 8$, $-d \equiv 3 \bmod 8$, but $3, 11, 19$ are all prime, so $-d \geq 27$, in particular $-d > 25$. If every prime factor p satisfies $p > \frac{-d}{5}$, then in particular for distinct prime factors p, q of $-d$, we have $pq > \frac{(-d)(-d)}{25} > -d$, an absurdity. Hence we have some $p \mid d$ (hence p ramifies in $\mathcal{O}_d$ by 3.4.15 and 3.4.16) with $p \leq \frac{-d}{5} < \frac{1-d}{4}$ which is inert by (b), a contradiction.

(d) Note that $-163 \equiv 1 \bmod 4$ and

$$N\left(n + \frac{-1 + \sqrt{-163}}{2}\right) = n^2 - n + 41.$$

Write the prime factorisation

$$\left(n + \frac{-1 + \sqrt{-163}}{2}\right) = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

If there is some i with $\mathfrak{p}_i = (p)$ then $p \mid n + \frac{-1+\sqrt{-163}}{2}$ which is clearly not possible, so each $\mathfrak{p}_i$'s lies above some prime that either splits or ramifies. By (b), these primes ≥ 41, so $N(\mathfrak{p}_i) \geq 41$ $\forall i$. But since $1 \leq n \leq 40$, $41 \leq n^2 - n + 41 < 41^2$, so $\left(n + \frac{-1+\sqrt{-163}}{2}\right)$ is prime and since $n + \frac{-1+\sqrt{-163}}{2} \notin \mathbb{Z}$, we have $n^2 - n + 41$ is prime.

4. Compute class group of $\mathcal{O}_{-23}$.

Solution. Since $-23 \equiv 1 \bmod 4$, by our calculation in 5.1.6 the Minkowski bound is $\frac{2}{\pi}\sqrt{23} < 4$, so we need to investigate the primes 2 and 3. By 3.4.16, since $-23 \equiv 1 \bmod 8$, we have $(2) = \left(2, \frac{1+\sqrt{-23}}{2}\right)\left(2, \frac{1-\sqrt{-23}}{2}\right) = \mathfrak{p}_2\overline{\mathfrak{p}_2}$, so $N(\mathfrak{p}_2) = N(\overline{\mathfrak{p}_2}) = 2$, and by 3.4.15, since $-23 \equiv 1 \equiv 1^2 \bmod 3$, we have $(3) = \left(3, 1 + \sqrt{-23}\right)\left(3, 1 - \sqrt{-23}\right) = \mathfrak{p}_3\overline{\mathfrak{p}_3}$ with $N(\mathfrak{p}_3) = N(\overline{\mathfrak{p}_3}) = 3$ similarly. We therefore have $\mathrm{Cl}(K) = \{1, [\mathfrak{p}_2], [\overline{\mathfrak{p}_2}], [\mathfrak{p}_3], [\overline{\mathfrak{p}_3}]\}$.

Now $a^2+ab+\frac{1+23}{4}b^2 = a^2+ab+6b^2 = 2,3$ doesn't have integer solutions, so $[\mathfrak{p}_2], [\overline{\mathfrak{p}_2}], [\mathfrak{p}_3], [\overline{\mathfrak{p}_3}] \neq 1$. But $N\left(\frac{1+\sqrt{-23}}{2}\right) = 6$ and

$$\frac{1+\sqrt{-23}}{2} \in \mathfrak{p}_2\mathfrak{p}_3 = \left(6, 2+2\sqrt{-23}, \frac{3+3\sqrt{-23}}{2}, -11+\sqrt{-23}\right)$$

(since $\frac{1+\sqrt{-23}}{2} = \frac{4+4\sqrt{-23}}{2} - \frac{3+3\sqrt{-23}}{2}$) where $N(\mathfrak{p}_2\mathfrak{p}_3) = N(\mathfrak{p}_2)N(\mathfrak{p}_3) = 6$, so we must have $\mathfrak{p}_2\mathfrak{p}_3 = \left(\frac{1+\sqrt{-23}}{2}\right)$, in particular principal, so $[\mathfrak{p}_2] = [\mathfrak{p}_3]^{-1} = [\overline{\mathfrak{p}_2}]^{-1}$, in particular $[\overline{\mathfrak{p}_2}] = [\mathfrak{p}_3]$. Also, $N(\mathfrak{p}_2^2) = N(\overline{\mathfrak{p}_2}^2) = 4$ but the only solutions to $a^2+ab+6b^2 = 4$ is $a = \pm 2, b = 0$, and $\mathfrak{p}_2^2, \overline{\mathfrak{p}_2}^2 \neq (2)$ since otherwise $\mathfrak{p}_2 = \overline{\mathfrak{p}_2}$ which is false, so $[\mathfrak{p}_2]^2, [\overline{\mathfrak{p}_2}]^2 \neq 1$ (which implies $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]$), and similarly $[\overline{\mathfrak{p}_3}]^2 \neq 1$. Hence in the group we have at least 3 $(1, [\mathfrak{p}_2], [\mathfrak{p}_3])$ and at most 4 (we don't know if $[\overline{\mathfrak{p}_3}]$ is any of the 3 before) distinct elements with no elements of order 2; the group must be $\mathbb{Z}/3\mathbb{Z}$.

Week 10, lecture 2, 11th March

5.4 Class groups as machinery to solve Diophantine equations

Theorem 5.4.1 (Fermat)**.** Let p be a prime. Then

1. $p = x^2+y^2$ for $x, y \in \mathbb{Z} \iff p = 2$ or $p \equiv 1 \bmod 4$,
2. $p = x^2+2y^2$ for $x, y \in \mathbb{Z} \iff p = 2$ or $p \equiv 1, 3 \bmod 8$.

Proof. We've seen numerous times how to prove the first statement using Minkowski (in elementary number theory and in exercise for elliptic curves). But there's a quicker way. Note that $p = x^2+y^2 = N(x+iy) = (x+iy)(x-iy)$ in the larger ring $\mathbb{Z}[i]$. Since $N(p) = p^2$ and $\mathbb{Z}[i]$ is a PID, this means p cannot be inert, and by 3.4.16 and 3.4.15, this means either $p = 2$ or $\exists a \in \mathbb{Z} : a^2 \equiv -1 \bmod p$, i.e. $\left(\frac{-1}{p}\right) = 1$, which by 4.1.5 is equivalent to $(-1)^{\frac{p-1}{2}} = 1$, i.e. $\frac{p-1}{2}$ is even, i.e. $p \equiv 1 \bmod 4$.
The same argument with $\mathbb{Z}\left(\sqrt{-2}\right)$ implies the second statement. □

Let's now see how the class group helps us in the case that our ring is not a PID. We've seen in 5.1.6 that $\mathrm{Cl}(\mathcal{O}_{-5}) = \mathbb{Z}/2\mathbb{Z}$.

Theorem 5.4.2. Let p be a prime.

1. If $p \equiv 1, 9 \bmod 20$, then $p\mathcal{O}_{-5} = \mathfrak{p}\overline{\mathfrak{p}}$ splits where $\mathfrak{p}, \overline{\mathfrak{p}}$ are principal. In particular, $p = x^2+5y^2$ for some $x, y \in \mathbb{Z}$ by the same argument.
2. If $p \equiv 3, 7 \bmod 20$, then $p\mathcal{O}_{-5} = \mathfrak{p}\overline{\mathfrak{p}}$ where $[\mathfrak{p}] = [\overline{\mathfrak{p}}] = [\mathfrak{p}_2]$ where $\mathfrak{p}_2 = \left(2, 1+\sqrt{-5}\right)$ is non-principal. In particular, $2p = x^2+5y^2$.
3. 2 and 5 ramify.
4. In any other case p is inert.

Proof. By 3.4.15, p splits $\iff \left(\frac{-5}{p}\right) = 1$. By 4.1.6, $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right) = 1$ either if $p \equiv 1 \bmod 4$ and $p \equiv \pm 1 \bmod 5$ (hence $p \equiv 1, 9 \bmod 20$) or if $p \equiv 3 \bmod 4$ and $p \equiv \pm 2 \bmod 5$ (hence $p \equiv 3, 7 \bmod 20$). Hence together with statement 3 (follows immediately from 3.4.19), this already gives 4.
Now the case $p\mathcal{O}_{-5} = \mathfrak{p}\overline{\mathfrak{p}}$ remains. There are two possibilities:

1. $[\mathfrak{p}] = 1$, then $[\overline{\mathfrak{p}}] = 1 \cdot 1^{-1} = 1$ as well, so $\exists x, y \in \mathbb{Z} : N\left(x+\sqrt{-5}y\right) = x^2+5y^2 = N(\mathfrak{p}) = p$. This cannot happen if p is not a square modulo 5, so $p \equiv 1, 9 \bmod 20$. This proves statement 1.
2. $[\mathfrak{p}] = [\mathfrak{p}_2]$, then $[\overline{\mathfrak{p}}] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$. But this also means $[\mathfrak{p}][\mathfrak{p}_2] = [\mathfrak{p}_2]^2 = 1$, i.e. $\mathfrak{p}\mathfrak{p}_2$ is principal, so $\exists x, y \in \mathbb{Z} : x^2+5y^2 = N(\mathfrak{p}\mathfrak{p}_2) = N(\mathfrak{p}_2)N(\mathfrak{p}) = 2p$, which cannot happen if $2p$ is not a square modulo 5, i.e. if p is a square modulo 5, so $p \equiv 3, 7 \bmod 20$. This proves statement 2.

□

5.4.1 Mordell equations

Mordell equations are of the form $y^2 = x^3 + d$. The general strategy is to rewrite it as $x^3 = y^2 - d = \left(y + \sqrt{d}\right)\left(y - \sqrt{d}\right)$ in $\mathbb{Z}\left[\sqrt{d}\right]$.

Example 5.4.3. $y^2 = x^3 - 1$. As above, rewrite it as $(y - i)(y + i) = x^3$. We solve it in the following steps.

1. Show that the ideals $(y - i), (y + i) \subset \mathcal{O}_{-1}$ are coprime.

   If $\mathfrak{p} \mid (y - i), (y + i)$ then $\mathfrak{p} \mid (2i)$, so either $2 \in \mathfrak{p}$ or $i \in \mathfrak{p}$. But $i \in \mathcal{O}_{-1}^\times$ and $\mathfrak{p}$ is proper, so $2 \in \mathfrak{p}$, i.e. $\mathfrak{p}$ lies above 2. Now $2 = (1+i)(1-i)$, so $\mathfrak{p}$ is either $(1+i)$ or $(1-i)$. In either case, $N(\mathfrak{p}) = 2 \mid N((y-i)(y+i)) = x^3$, so $8 \mid x^3$ and $y^2 \equiv -1 \bmod 8$, which is impossible.
2. By unique ideal factorisation of $(x)^3 = (y - i)(y + i)$ and step 1, $(y - i) = \mathfrak{q}^3$ and $(y + i) = \overline{\mathfrak{q}}^3$ for some ideals $\mathfrak{q}, \overline{\mathfrak{q}}$.
3. Since $\mathrm{Cl}(\mathcal{O}_{-1})$ is trivial, $\mathfrak{q} = (a + ib)$ for some $a, b \in \mathbb{Z}$, in particular $y - i = u(a + ib)^3$ where $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Similar for $y + i$. Up to signs and relabelling a and b we can write $y - i = (a + ib)^3$.
4. We now simply expand: $(a+ib)^3 = a^3 - 3ab^2 + i\left(b\left(3a^2 - b^2\right)\right)$, and we have $y = a^3 - 3ab^2$, $1 = b\left(3a^2 - b^2\right)$. Hence $b = 3a^2 - b^2 = \pm 1$. If $b = 1$ then $3a^2 = 0$ so $a = 0$. If $b = -1$ then $3a^2 = 2$ which is impossible.
5. Hence we have $y = 0$ in any case ($b = 1, a = 0,\ b = -1, a = 0,\ b = 0, a = 1,\ b = 0, a = -1$), so the only solution is $x = 1, y = 0$.

Example 5.4.4. $y^2 = x^3 - 5$. Again rewrite it as $\left(y - \sqrt{-5}\right)\left(y + \sqrt{-5}\right) = x^3$.

1. Show that the ideals $\left(y - \sqrt{-5}\right), \left(y + \sqrt{-5}\right) \subset \mathcal{O}_{-5}$ are coprime.

   Similarly, if $\left(y - \sqrt{-5}\right), \left(y + \sqrt{-5}\right) \subset \mathfrak{p}$ where $\mathfrak{p}$ is prime then $2\sqrt{-5} \in \mathfrak{p}$, so $N(\mathfrak{p}) \mid N\left(2\sqrt{-5}\right) = 20$, so $\mathfrak{p}$ lies above 2 or 5. On the other hand, $x^3 = \left(y - \sqrt{-5}\right)\left(y + \sqrt{-5}\right) \in \mathfrak{p}$, so $x \in \mathfrak{p}$. If $\mathfrak{p}$ lies above 2 then $x \in (2)$, so again $8 \mid x^3$ hence $y^2 \equiv 3 \bmod 8$ which is impossible. If $\mathfrak{p}$ lies above 5 then $5 \mid x \implies 5 \mid x^3 - 5 \implies 5 \mid y$, but then $25 \mid x^3 - y^2 = 5$ which is also impossible.
2. By unique ideal factorisation of $(x)^3 = \left(y - \sqrt{-5}\right)\left(y + \sqrt{-5}\right)$ and step 1, $\left(y + \sqrt{-5}\right) = \mathfrak{q}^3$ and $\left(y - \sqrt{-5}\right) = \overline{\mathfrak{q}}^3$ for some ideals $\mathfrak{q}, \overline{\mathfrak{q}}$.

Week 10, lecture 3, 12th March

3. We can't immediately conclude $\mathfrak{q}$ is principal since $\mathrm{Cl}(\mathcal{O}_{-5}) = \mathbb{Z}/2\mathbb{Z}$, but since $\mathfrak{q}^3$ is principal, its order divides 3, hence in $\mathbb{Z}/2\mathbb{Z}$ it must be the identity, i.e. $\mathfrak{q}$ (and similarly $\overline{\mathfrak{q}}$) is principal. Now $\left(y + \sqrt{-5}\right) = \left(a + b\sqrt{-5}\right)^3$ for some $a, b \in \mathbb{Z}$, so $y + \sqrt{-5} = u\left(a + b\sqrt{-5}\right)^3$ where $u \in \mathbb{Z}\left[\sqrt{-5}\right]^\times = \{\pm 1\}$, so up to signs $y + \sqrt{-5} = \left(a + b\sqrt{-5}\right)^3$.
4. Again we expand: $\left(a + \sqrt{-5}\right)^3 = a(a^2 - 15b^2) + \sqrt{-5}b(3a^2 - 5b^2)$, hence $b = 3a^2 - 5b^2 = \pm 1$. If $b = 1$ then $3a^2 = 6$ which is impossible, if $b = -1$ then $3a^2 = 4$ which is again impossible.
5. Hence $y^2 = x^3 - 5$ has no integer solutions.

In more generality. Consider $d < 0$ squarefree and $d \not\equiv 1 \bmod 4$. Then $\mathcal{O}_d = \mathbb{Z}\left[\sqrt{d}\right]$. We solve $y^2 = x^3 + d$ following the same steps and see what can go wrong.

1. Suppose $\left(y + \sqrt{d}\right), \left(y - \sqrt{d}\right) \subset \mathfrak{p}$ for some prime ideal $\mathfrak{p}$. Then $2\sqrt{-d} \in \mathfrak{p}$. This tells us $\mathfrak{p}$ lies above either 2 or some p that divides d.

   If $\mathfrak{p}$ lies above 2, note that $x^3 = \left(y + \sqrt{d}\right)\left(y - \sqrt{d}\right) \in \mathfrak{p} \cap \mathbb{Z} = (2)$, so $8 \mid x^3$, so $y^2 \equiv d \bmod 8$, but only quadratic residues of 8 are $0, 1, 4$, and d is squarefree and $d \not\equiv 1 \bmod 4$, so this case is excluded.

   Otherwise, similarly $p \mid x^3$, but also $p \mid d$, so $p \mid y$ and hence $p^2 \mid x^3 - y^2 = -d$, but d is squarefree, again impossible.

   We conclude that $\left(y + \sqrt{d}\right), \left(y - \sqrt{d}\right)$ are coprime.
2. This allows to write $\left(y + \sqrt{d}\right) = \mathfrak{q}^3$ for some ideal $\mathfrak{q} \subset \mathcal{O}_d$, similar for $\left(y - \sqrt{d}\right)$.
3. If $3 \nmid |\mathrm{Cl}(\mathcal{O}_d)|$ then $\mathrm{Cl}(\mathcal{O}_d)$ cannot have order 3 elements, so $\mathfrak{q}$ is principal.

4. If $\mathfrak{q}$ is principal then $y+\sqrt{d} = u\left(a+b\sqrt{d}\right)^3$ for $u \in \mathbb{Z}\left[\sqrt{d}\right] = \begin{cases} \{\pm1\} \text{ if } d<-1 \\ \{\pm1, \pm i\} \text{ if } d=-1 \end{cases}$, and again up to signs (and relabelling if $d=-1$) we can simply write $y+\sqrt{d} = \left(a+b\sqrt{d}\right)^3$.

5. $\left(a+b\sqrt{d}\right)^3 = a(a^2+3db^2)+\sqrt{d}b(3a^2+db^2)$, so in general ($d \neq -1$) one has $b = 3a^2+db^2 = \pm1$. If this does have a solution $a=\pm a_0$, then $y = \pm a_0(a_0^2+3d)$, and $x^3 = \left(y+\sqrt{d}\right)\left(y-\sqrt{d}\right) = \left(a_0+\sqrt{d}\right)^3\left(a_0-\sqrt{d}\right)^3 = \left(a_0^2-d\right)^3$, so $x = a_0^2-d$, hence in this case we have solutions $\left(a_0^2-d, \pm a_0\left(a_0^2+3d\right)\right)$.

Theorem 5.4.5. Suppose $d<0$ is squarefree and $d \not\equiv 1 \bmod 4$. If $\exists a \in \mathbb{Z} : 3a^2+d = \pm1$, then

$$(x,y) = \left(a^2-d, \pm a\left(a^2+3d\right)\right)$$

is a solution of the Diophantine equation $y^2 = x^3+d$. Moreover, if $3 \nmid |\mathrm{Cl}(\mathcal{O}_d)|$, then these are the only solutions.

Example 5.4.6.

- $d=-13$: in this case $3a^2=12$ has solutions $a=\pm2$, so $(x,y) = (4+13, \pm2(4-3\times13)) = (17,\pm70)$ are solutions to $y^2 = x^3-13$. Moreover, $\frac{2}{\pi}\sqrt{4\cdot13} < 5$, with the primes 2 ramifying (3.4.16) and 3 inert (3.4.15 and 2 is not a square modulo 3), so $\mathrm{Cl}(\mathcal{O}_{-13}) = \mathbb{Z}/2\mathbb{Z}$ and so the above solutions are all.

- $d=-26$: $3a^2=27$ has solutions $a=\pm3$, so $(x,y) = (9+26, \pm3(9-3\times26)) = (35,\pm207)$ are solutions to $y^2=x^3-26$. But by staring, $(3,\pm1)$ is another solution, so $3 \mid \mathrm{Cl}(\mathcal{O}_{-26})$ (i.e. we can also reverse the process to obtain information of the class group).

Theorem 5.4.7. For $d \neq 0$, the Diophantine equation $y^2=x^3+d$ has finitely many integer solutions.

5.4.2 Units in real quadratic fields

In previous section we only considered $\mathbb{Z}\left[\sqrt{d}\right]$ with $d<0$, where there are a very limited set of units and hence makes step 4 in the general "algorithm" simpler. But it turns out in $\mathbb{Z}\left[\sqrt{d}\right]$ with $d>0$ we have infinite number of units, which can still be systematically described.

Example 5.4.8. Note that $1+\sqrt{2} \in \mathcal{O}_2^\times$, since $N\left(1+\sqrt{2}\right) = \left(1+\sqrt{2}\right)\left(1-\sqrt{2}\right) = -1$. But this means $\left(1+\sqrt{2}\right)^n \in \mathcal{O}_2^\times \ \forall n \in \mathbb{Z}$, and since $1+\sqrt{2}>1$, this means they are all distinct and we have an infinite family of units. We will later see that these together with ±1 generate all units in $\mathcal{O}_2$.

Theorem 5.4.9. Let $d>1$ be squarefree. Then $\exists! \varepsilon \in \mathcal{O}_d^\times$ with $\varepsilon>1$ such that $\mathcal{O}_d^\times = \{\pm\varepsilon^n : n \in \mathbb{Z}\}$. This ε is called the *fundamental unit*. In particular, $\mathcal{O}_d^\times \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}$.

Remark 5.4.10. When $d \not\equiv 1 \bmod$, the units give solutions to the Diophantine equations $x^2-dy^2=\pm1$ (Pell). Indeed, $x+\sqrt{d}y \in \mathcal{O}_d$ is a unit $\iff N\left(x+\sqrt{d}y\right) = \pm1$.

Example 5.4.11. $1+\sqrt{2}$ is the fundamental unit of $\mathcal{O}_2^\times$, $2+\sqrt{3}$ for $\mathcal{O}_3^\times$, $\frac{1+\sqrt{5}}{2}$ for $\mathcal{O}_5^\times$, $170+39\sqrt{19}$ for $\mathcal{O}_{19}^\times$, and $2143295+221064\sqrt{94}$ for $\mathcal{O}_{94}^\times$.

Week 11, lecture 1, 17th March

Lemma 5.4.12. Let $d>1$ be squarefree, $K = \mathbb{Q}\left(\sqrt{d}\right)$ and $\mathcal{O}_d$ the ring of integer of K. Then there exists $u \in \mathcal{O}_d^\times$ with $u \neq \pm1$.

Proof. We claim that $\exists c>0$ such that there are infinitely many $\alpha \in \mathcal{O}_d$ with $|N_K(\alpha)| < c$. Let's first see how this claim suffices to imply the lemma. Recall 5.1.2 which says that there are finitely many ideals with norm $<c$. By pigeonhole, $\exists \alpha \neq \beta \neq \gamma : (\alpha) = (\beta) = (\gamma)$ with at least one of β and γ distinct from $-\alpha$. WLOG suppose it's β. Hence $\beta = u\alpha$ where $u \notin \{\pm1\}$.

Now let's prove our claim. Recall the realisation of real quadratic fields as lattices (5.2.12). Take

$$S_r = \left\{(x,y) \in \mathbb{R}^2 : |x|<r, |y|<\frac{c}{r}\right\} = \left\{(x,y) \in \mathbb{R}^2 : N(x,y) = |x\cdot y| < c\right\}$$

as the convex, symmetric subset of $\mathbb{R}^2$ to be applied to 5.2.8. Let $c > \sqrt{|D_K|} = \mathrm{covol}(\iota(\mathcal{O}_K))$. Then

$$\mathrm{vol}(S_r) = (2r)\left(\frac{2c}{r}\right) = 4c > 2^2\,\mathrm{covol}(\iota(\mathcal{O}_K)),$$

so $\forall r>0$, $\exists 0 \neq \alpha \in \mathcal{O}_d : \iota(\alpha) \in S_r$, i.e. $|\alpha|<r$ and $|\tau_2(\alpha)| < \frac{c}{r}$, so $|N_K(\alpha)| = |\tau_1(\alpha)\tau_2(\alpha)| < c$. Take $0 \neq \alpha_1 \in \mathcal{O}_d \cap S_1$, $0 \neq \alpha_2 \in \mathcal{O}_d \cap S_{|a_1|}$ and iterate infinitely to get a sequence (α_i). Since by this construction $|\alpha_1| > |\alpha_2| > |\alpha_3| > \cdots$, we have an infinite number of elements with norm $<c$, as desired. □

Lemma 5.4.13. Let $d > 1$ be squarefree, $K = \mathbb{Q}\left(\sqrt{d}\right)$ and $\mathcal{O}_d$ the ring of integer of K. Let $u = a + b\sqrt{d} \in \mathcal{O}_d^\times$. Then $u > 1 \iff a, b > 0$; moreover, if $u' = a' + b'\sqrt{d}$ with $u' > 1$, then $u \geq u' \iff a \geq a'$ and $b \geq b'$. In fact, $u \geq u' \iff b \geq b'$ with the only exception $d = 5$, $u = \frac{1+\sqrt{5}}{2}$, $u' = \frac{3+\sqrt{5}}{2}$.

Proof. 1. $\Longleftarrow$: $a, b > 0$ in particular means $a, b \geq \frac{1}{2}$, but then $u = a + b\sqrt{d} \geq \frac{1+\sqrt{d}}{2} > 1$.

$\Longrightarrow$: $u \in \mathcal{O}_d^\times \implies N_K(u) = \pm 1 = u\overline{u}$, so $u > 1 \implies |\overline{u}| < 1$. This implies $u + \overline{u}, u - \overline{u} > 0$, where $u + \overline{u} = 2a$ and $u - \overline{u} = 2\sqrt{d}b$, so $a, b > 0$.

2. Write

$$u - u' = 2\sqrt{d}(b - b') + \overline{u} - \overline{u'}. \tag{$*$}$$

If $b \neq b'$, then if $d \not\equiv 1 \bmod 4$, we have $|b - b'| \geq 1$ and so $2\sqrt{d}|b - b'| \geq 2$, and if $d \equiv 1 \bmod 4$ then $|b - b'| \geq \frac{1}{2}$ so $2\sqrt{d}|b - b'| \geq \sqrt{d} \geq 2$ as well. Since again $|\overline{u}|, |\overline{u'}| < 1$, we have $|\overline{u} - \overline{u'}| < 2$, so

$$b > b' \implies 2\sqrt{d}(b - b') + \overline{u} - \overline{u'} > 0 \implies u > u'$$

by $(*)$, and similarly $b < b' \implies u < u'$. It remains to see what happens when $b = b'$. Then by $(*)$, $u \geq u' \iff \overline{u} \geq \overline{u'}$. Since $a, a' > 0$, WLOG $a^2 - db^2 = 1$ and $(a')^2 - d(b')^2 = -1$, so $a^2 - (a')^2 = 2$. If $d \not\equiv 1 \bmod 4$, then $a, a' \in \mathbb{Z}$, so since $(n+1)^2 - n^2 = 2n + 1 > 2$, $a^2 - (a')^2 = 2$ can never happen. If $d \equiv 1 \bmod 4$, then $b \in \frac{1}{2} + \mathbb{Z}$ and $a, a' \in \frac{1}{2}\mathbb{Z} \backslash \mathbb{Z}$. Write $a' = \frac{2n+1}{2}$ and $a = \frac{2n+2k+1}{2}$. Then

$$a^2 - (a')^2 = \frac{(2n + 2k + 1)^2 - (2n + 1)^2}{4} = 2$$

has only solution $n = 0, k = 1$, so $a' = \frac{1}{2}$, $a = \frac{3}{2}$, hence $db^2 = \frac{5}{4}$, so it can only be that $b = \frac{1}{2}$ and $d = 5$.

□

Proof of 5.4.9. Let $\varepsilon \in \mathcal{O}_d^\times$ be minimal with $\varepsilon > 1$. Let $u \in \mathcal{O}_d^\times$ with $u \neq \pm 1$. Write $u' = |u|$, in particular $u' > 0$. Then $\varepsilon^k < u'$ for some small enough $k < 0$. Similarly $\varepsilon^k > u'$ for some big enough $k > 0$. This means $\exists k$ maximal with $\varepsilon^k \leq u'$ and $u' < \varepsilon^{k+1}$, i.e. $1 \leq \frac{u'}{\varepsilon^k} < \varepsilon$. By minimality of ε, this implies $\frac{u'}{\varepsilon^k} = 1$, i.e. $u = \pm\varepsilon^k$. □

Example 5.4.14. The proof also gives a constructive way to find the fundamental unit: we find solution to $a^2 - db^2 = \pm 1$ with $a, b > 0$ and b minimal. For instance, for $\mathcal{O}_{11}$, we solve $a^2 - 11b^2 = \pm 1$ starting from $b = 1$. Then $a^2 = 12$ or 10, which yields no solutions; if $b = 2$ then $a^2 = 45$ or 43, again no solutions; if $b = 3$ then $a^2 = 100$ (so $a = 10$) or 98 (no solution), so $\varepsilon = 10 + 3\sqrt{11}$ is the fundamental unit of $\mathcal{O}_{11}$.

Remark 5.4.15. We often need to solve equations of the form $N_K(\alpha) = n$ for $n \in \mathbb{Z}$. But now $N_K\left(\pm\eta^k\alpha\right) = n\ \forall k \geq 1$ where $\eta > 1$ is the smallest unit $N_K(\eta) = 1$. We can pick k in a way that

$$\sqrt{|n|}\eta^{-\frac{1}{2}} \leq \alpha' := \pm\varepsilon^k\alpha \leq \sqrt{|n|}\eta^{\frac{1}{2}},$$

then $|\overline{\alpha'}| = \frac{n}{\alpha'} \leq \sqrt{|n|}\eta^{\frac{1}{2}}$ implies $|\alpha' - \overline{\alpha'}| = |2b\sqrt{d}| \leq 2\sqrt{|n|}\eta^{\frac{1}{2}}$, so $b \leq \sqrt{\frac{\eta|n|}{d}}$. This gives us: any solution to $N_K(\alpha) = n$ for $\alpha \in \mathcal{O}_d$ has the form $\alpha = \pm\eta^k\left(a + b\sqrt{d}\right)$ where $N_K\left(a + \sqrt{d}b\right) = n$ and $|b| \leq \sqrt{\frac{\eta|n|}{d}}$ with $\eta > 1$ and $N_K(\eta) = 1$. Such η does always exist; it's either the fundamental unit ε or ε^2.

Week 11, lecture 2, 18th March

Example 5.4.16. We compute $\mathrm{Cl}(K)$ where $K = \mathbb{Q}\left(\sqrt{79}\right)$ and write $\mathcal{O}_{79} = \mathcal{O}_K$. The Minkowski bound is $C_K = \sqrt{79} < 9$, so we need to investigate primes 2, 3, 5 and 7.

By 3.4.16 and 3.4.15,

- $2\mathcal{O}_K = \left(2, \sqrt{79} + 1\right)^2 =: \mathfrak{p}_2^2$ since $79 \equiv 3 \bmod 4$;
- $3\mathcal{O}_K = \left(3, \sqrt{79} + 1\right)\left(3, \sqrt{79} - 1\right) =: \mathfrak{p}_3\overline{\mathfrak{p}_3}$ since $79 \equiv 1 = 1^2 \bmod 3$;
- $5\mathcal{O}_K = \left(5, \sqrt{79} + 2\right)\left(5, \sqrt{79} - 2\right) =: \mathfrak{p}_5\overline{\mathfrak{p}_5}$ since $79 \equiv 4 = 2^2 \equiv 5$.
- $7\mathcal{O}_K = \left(7, \sqrt{79} + 3\right)\left(7, \sqrt{79} - 3\right) =: \mathfrak{p}_7\overline{\mathfrak{p}_7}$ since $79 \equiv 2 \equiv 3^2 \equiv 7$.

We now have a lot of primes. The vague idea is to find elements with small norm to find relations between them. We start with $b = 1, 2$ and find a that gives small values of $a^2 - 79b^2$, and we have that

$$N\left(8+\sqrt{79}\right) = -15,\ N\left(9+\sqrt{79}\right) = 2,\ N\left(10+\sqrt{79}\right) = 21,\ N\left(17+2\sqrt{79}\right) = -27,$$

and this tells us $\left(8+\sqrt{79}\right)$ is the product of either $\mathfrak{p}_3$ or $\overline{\mathfrak{p}_3}$ and either $\mathfrak{p}_5$ or $\overline{\mathfrak{p}_5}$, but in any of these 4 cases, we have $[\mathfrak{p}_3] = [\mathfrak{p}_5]$ or $[\mathfrak{p}_3] = [\mathfrak{p}_5]^{-1}$, i.e. we can already get rid of $\mathfrak{p}_5$ and $\overline{\mathfrak{p}_5}$. Similarly, with $\left(10+\sqrt{79}\right)$ we can get rid of $\mathfrak{p}_7$ and $\overline{\mathfrak{p}_7}$. Now $9+\sqrt{79} = 4 \times 2 + \sqrt{79} + 1 \in \mathfrak{p}_2$, so since $\left(9+\sqrt{79}\right)$ and $\mathfrak{p}_2$ have the same norm, they must be the same ideal and $[\mathfrak{p}_2] = 1$. We have thus deduced that $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_3]$ alone.

We claim that $\left(17+2\sqrt{79}\right)$ is either $\mathfrak{p}_3^3$ or $\overline{\mathfrak{p}_3}^3$; by its norm it suffices to show $\mathfrak{p}_3\overline{\mathfrak{p}_3} \nmid \left(17+2\sqrt{79}\right)$. Indeed, $17+2\sqrt{79} \in \mathfrak{p}_3\overline{\mathfrak{p}_3} = (3)$ is clearly false. This tells us $[\mathfrak{p}_3]^3 = [\overline{\mathfrak{p}_3}]^3 = 1$.

It remains to see $\mathfrak{p}_3$ is not principal to conclude $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$. We prove $a^2 - 79b^2 = \pm 3$ has no integer solutions:

- $a^2 - 79b^2 \equiv a^2 \equiv 3 \bmod 79$ doesn't have solutions since $\left(\frac{3}{79}\right) = -\left(\frac{79}{3}\right) = -\left(\frac{1}{3}\right) = -1$.
- The fundamental unit of $\mathcal{O}_{79}$ is $\varepsilon = 80 + 9\sqrt{79}$ with $N(\varepsilon) = 1$. By 5.4.15, if $N_K(\alpha) = -3$ has a solution, it also has a solution $a + b\sqrt{79}$ with $|b| < \sqrt{\frac{3\varepsilon}{79}} \approx 2.46$, so it is enough to solve $N\left(a + b\sqrt{79}\right) = -3$ for a when $b = 0, \pm 1, \pm 2$. If $b = 0$ then $a^2 = -3$ has no solution. If $b = \pm 1$ then $a^2 = 76$ also has no solution. If $b = \pm 2$ then $a^2 = 313$ again has no solution.

Theorem 5.4.17 (Dirichlet's unit theorem)**.** Let K be a number field and suppose k has r real embeddings and s conjugate pairs of complex embeddings. Let $\mu(K) = \{x \in K : x^n = 1 \text{ for some } n\}$ be the set of roots of unity. Then $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$. In other words, $\exists \varepsilon_1, \ldots, \varepsilon_{r+s-1} \in \mathcal{O}_K^\times$ such that every $u \in \mathcal{O}_K^\times$ can be written as $\zeta\varepsilon_1^{n_1} \cdots \varepsilon_{r+s-1}^{n_{r+s-1}}$ for some $\zeta \in \mu(K)$ and $n_i \in \mathbb{N}$.

Example 5.4.18. 1. $K = \mathbb{Q},\ r = 1,\ s = 0,\ r + s - 1 = 0$ and indeed $\mathcal{O}_K^\times = \mathbb{Z}^\times = \{\pm 1\} = \mu(\mathbb{Q})$.

2. $K = \mathbb{Q}\left(\sqrt{-d}\right)$ where $d > 0$ is squarefree, then $r = 0,\ s = 1$ so again $r+s-1 = 0$ and $\mathcal{O}_K^\times = \mu\left(\mathbb{Q}\left(\sqrt{-d}\right)\right) = \{\pm 1\}$ unless $K = \mathbb{Q}(i)$ (then $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$) and $K = \mathbb{Q}(\zeta_3)$ (then $\mathcal{O}_K^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$).
3. $K = \mathbb{Q}\left(\sqrt{d}\right)$ where $d > 0$ is squarefree, then $r = 2,\ s = 0$ so $r + s - 1 = 1$ and $\mathcal{O}_d^\times \cong \mu\left(\mathbb{Q}\left(\sqrt{d}\right)\right) \times \mathbb{Z}$ as in 5.4.9.

Example 5.4.19. 1. $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$, then $r = 1,\ s = 1,\ r + s - 1 = 1$, so $\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbb{Z}$. One can check $N(1 + \sqrt[3]{2} + \sqrt[3]{4}) = 1$ and it turns out this is the fundamental unit.

2. Cyclotomic field $K = \mathbb{Q}(\zeta_5)$, then $r = 0,\ s = 2,\ r + s - 1 = 1$, so again $\mathcal{O}_K^\times \cong \mu(\mathbb{Q}(\zeta_5)) \times \mathbb{Z}$. Note that $\mathbb{Q}\left(\sqrt{5}\right) \subset \mathbb{Q}(\zeta_5)$, so $\mathcal{O}_5^\times = \left\{\pm\left(\frac{1+\sqrt{5}}{2}\right)^n : n \in \mathbb{Z}\right\} \subset \mathcal{O}_K^\times$. It turns out that $\mathcal{O}_K^\times = \left\{\zeta_{10}^k\left(\frac{1+\sqrt{5}}{2}\right)^n : k, n \in \mathbb{Z}\right\}$.

Week 11, lecture 3, 19th March: problem class (sheet 5)

Exercise 5.4.20. 3. Let K be a number field and suppose $\alpha\beta = \gamma^n$ for $\alpha, \beta, \gamma \in \mathcal{O}_K$ and $n > 0$. Suppose $(\alpha, \beta) = \mathcal{O}_K$, i.e. α, β are coprime. Prove that if $(n, |\mathrm{Cl}(\mathcal{O}_K)|) = 1$ then $\alpha = u\delta^n$ for some $u \in \mathcal{O}_K^\times$ and $\delta \in \mathcal{O}_K$.

Solution. Since $(\alpha), (\beta) \subset \mathcal{O}_K$ are coprime ideals, i.e. the factorisations of (α) and (β) don't have any common prime factor, and that $(\alpha)(\beta) = (\gamma)^n$, we have $(\alpha) = I^n$ and $(\beta) = J^n$ for some ideals $I, J \subset \mathcal{O}_K$. But then $[I]^n = 1$, and since $n \nmid |\mathrm{Cl}(\mathcal{O}_K)|$, $[I] = 1$ and $I = (\delta)$ for some $\delta \in \mathcal{O}_K$, so $\alpha = u\delta^n$ as desired.

1. We investigate primes of the form $x^2 + 13y^2$ where $x, y \in \mathbb{Z}$. Show that:

   (a) $\mathrm{Cl}(\mathcal{O}_{-13}) = \{1, [\mathfrak{p}_2]\}$.

   (b) p splits in $\mathcal{O}_{-13}$ iff $p \equiv 1 \bmod 4$ and $\left(\frac{p}{13}\right) = 1$ or $p \equiv 3 \bmod 4$ and $\left(\frac{p}{13}\right) = -1$.

   (c) In the case $p \equiv 1 \bmod 4$, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p}, \overline{\mathfrak{p}}$ are principal, and in the case $p \equiv 3 \bmod 4$, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ where $[\mathfrak{p}] = [\overline{\mathfrak{p}}] = [\mathfrak{p}_2]$.

   (d) $p = x^2 + 13y^2$ iff $p = 13$ or $p \equiv 1 \bmod 4$ and $\left(\frac{p}{13}\right) = 1$.

   Solution.

   (a) We did this in 5.4.6.

(b) Since $-13 \equiv 3 \bmod 4, 8$, by 3.4.16, 3.4.15, a prime p splits iff p is odd, $p \nmid -13$ and $\left(\frac{-13}{p}\right) = 1$. p is odd means either $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$. If former, then

$$\left(\frac{p}{13}\right) = \left(\frac{13}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-13}{p}\right) = 1 \times 1 = 1,$$

and if latter than

$$\left(\frac{p}{13}\right) = \left(\frac{-1}{p}\right)\left(\frac{-13}{p}\right) = -1 \times 1 = -1.$$

(c) We know $\mathfrak{p}$ is principal iff $p = x^2 + 13y^2$ has a solution over $\mathbb{Z}$, which implies $\left(\frac{p}{13}\right) = 1$, and $[\mathfrak{p}] = [\mathfrak{p}_2]$ iff $[\mathfrak{p}_2][\mathfrak{p}] = [\mathfrak{p}_2]^{-1}[\mathfrak{p}_2] = 1$ iff $2p = x^2 + 13y^2$ has a solution over $\mathbb{Z}$, which implies $\left(\frac{2p}{13}\right) = 1 \implies \left(\frac{p}{13}\right) = -1$ $\big($since $\left(\frac{2}{13}\right) = -1\big)$.

(d) Clearly $13 = 0^2 + 13 \cdot 1^2$. The second case follows from (c) since $p = x^2 + 13y^2 \iff \exists$ principal ideal $\mathfrak{p}$ with $N(\mathfrak{p}) = p$.

4. We demonstrate a trick to solve $y^2 = x^3 + d$ where $d > 0$. In particular let $d = 7$. Write the equation as $y^2 + 1 = x^3 + 8 = (x+2)\left(x^2 - 2x + 4\right)$. Show that:

(a) x is odd.

(b) $x^2 - 2x + 4 \equiv 3 \bmod 4$ and $x^2 - 2x + 4 > 0$.

(c) $\exists p \equiv 3 \bmod 4$ prime with $p \mid x^2 - 2x + 4$ (and so $p \mid y^2 + 1$).

(d) The equation $y^2 = x^3 + 7$ has no solutions over $\mathbb{Z}$.

Solution.

(a) If x is even then $8 \mid x^3$, so $y^2 \equiv -1 \bmod 8$ which is impossible since -1 is not a quadratic residue mod 8.

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

(c) Write $x^2 - 2x + 4 = p_1 \cdots p_r$ where p_i's are prime. If all $p \equiv 1 \bmod 4$ then $x^2 - 2x + 4 \equiv 1 \bmod 4$, contradicting (b).

(d) (c) says there is a prime $p \equiv 3 \bmod 4$ such that $y^2 + 1 \equiv x^2 - 2x + 4 \equiv 0 \bmod p$, contradicting that $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \bmod 4$.

2. Let $\mathfrak{p}_2 = \left(2, \sqrt{-14}\right) \subset \mathcal{O}_{-14}$. You can assume it's nonprincipal. Show that:

(a) $\exists$ ideal $\mathfrak{p} \subset \mathcal{O}_{-14}$ with $N(\mathfrak{p}) = p$ and $[\mathfrak{p}] = [\mathfrak{p}_2] \iff p = 2x^2 + 7y^2$ for $x, y \in \mathbb{Z}$.

(b) $x^2 + 14y^2$ and $2x^2 + 7y^2$ take the same set of values mod N $\forall N > 0$.

Solution.

(a) We first show that $p = 2x^2 + 7y^2$ for some $x, y \in \mathbb{Z}$ iff $2p = a^2 + 14b^2$ for some $a, b \in \mathbb{Z}$.

$\Longleftarrow$: Modulo 2 we have $a^2 \equiv 0 \bmod 2$, i.e. a is even, so $2p = a^2 + 14b^2$ can be reduced to $2p = (2a_0)^2 + 14b^2 \iff p = 2a_0^2 + 7b^2$.

$\Longrightarrow$: $p = 2x^2 + 7b^2 \implies 2p = 4x^2 + 14b^2 = (2x)^2 + 14b^2$.

Now note that $2p = a^2 + 14b^2$ for $a, b \in \mathbb{Z}$ iff $\exists$ a principal ideal of norm $2p$ iff (by calculation in 5.3.1, $\mathrm{Cl}(\mathcal{O}_{-14}) \cong \mathbb{Z}/4\mathbb{Z}$) $\exists$ a principal ideal of the form $\mathfrak{p}\mathfrak{p}_2$ where $N(\mathfrak{p}) = p$ iff $\exists \mathfrak{p} \subset \mathcal{O}_{-14}$ such that $N_K(\mathfrak{p}) = p$ and $[p] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$.

(b) Modulo 7 we have $x^2 + 14y^2 = x^2$ and $2x^2 + 7y^2 = 2x^2$, and since $2 \equiv 9 = 3^2 \bmod 7$, we have $2x^2 \equiv (3x)^2 \bmod 7$.

Modulo 8 (by brute-force computation) they both take values $\{0, \pm 1, \pm 2, \pm 4\}$.

Modulo p for $p \neq 2, 7$, we prove that in general $ax^2 + by^2$ where $a, b \in \mathbb{F}_p^\times$ takes all values. Note that ax^2 take $\frac{p+1}{2}$ values, and similarly for $k - by^2$ for $k \in \mathbb{F}_p$. But then $\{ax^2 : x \in \mathbb{F}_p\} \cap \{k - by^2 : k, y \in \mathbb{F}_p\} \neq \varnothing$ since $p + 1 > p$, so any k can be written as $ax^2 + by^2$ for some $x, y \in \mathbb{F}_p$.

5. Prove that $(x, y) = (1, 0)$ is the only solution to $y^2 = x^5 - 1$ over $\mathbb{Z}$.

Solution. Rewrite $(y+i)(y-i) = x^5$ and follow the same strategy of solving Mordell equations (note that $u^5 = u$ $\forall u \in \mathbb{Z}[i]^\times$).