Course notes for PMATH 641

Christopher Hawthorne

Lectures by David McKinnon

Contents

1 Dedekind domains **2**

2 Geometry of numbers **10**

3 Factorization of primes in extensions **17**

4 Interlude—Finite fields **23**

5 Slightly less finite fields **23**

Preliminaries

My thanks to Bahaa Khaddaj for the use of his notes for the lectures I missed.

All rings are commutative and have unity.

Definition 0.1. A *number field* is a finite extension of $\mathbb{Q}$. An *algebraic number* is an element of a number field.

Definition 0.2. An *algebraic integer* is an $\alpha \in \mathbb{C}$ such that $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

Definition 0.3. Suppose K is a number field. We define the *ring of integers of* K, denoted $\mathcal{O}_K$, to be the set of algebraic integers lying in K.

In fact, $\mathcal{O}_K$ is a ring. That $0 \in \mathcal{O}_K$ is obvious; closure under addition, multiplication, and additive inverses will follow from the following theorem.

Theorem 0.4. *Suppose $\alpha \in \mathbb{C}$. Then α is an algebraic integer if and only if $p(\alpha) = 0$ for some monic $p \in \mathbb{Z}[x]$.*

Proof.

($\implies$) Suppose α is an algebraic integer. Then $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module, say by $f_1(\alpha), \ldots, f_n(\alpha)$. Let $k = \max\{\deg(f_i) : i \in \{1, \ldots, n\}\} + 1$. Then

$$\alpha^k = a_1 f_1(\alpha) + \cdots + a_n f_n(\alpha)$$

So if

$$p(x) = x^k + a_1 f_1(x) + \cdots + a_n f_n(x)$$

then $p \in \mathbb{Z}[x]$ is non-zero and monic, and $p(\alpha) = 0$.

($\impliedby$) Suppose

$$\alpha^k + a_{k-1}\alpha^{k-1} + \cdots + a_0 = 0$$

where $a_0, \ldots, a_{k-1} \in \mathbb{Z}$. Then $\{\alpha^{k-1}, \ldots, \alpha\}$ generates $\mathbb{Z}[\alpha]$ as a $\mathbb{Z}$-module, and $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module.

□ Theorem 0.4

Remark 0.5. $\alpha \in \mathbb{Q}^{\text{alg}}$ is an algebraic integer if and only if its monic minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Hence if $\alpha, \beta \in \mathcal{O}_K$, then $\mathbb{Z}[\alpha, \beta]$ is finitely generated. But $\mathbb{Z}[\alpha + \beta]$, $\mathbb{Z}[\alpha\beta]$, and $\mathbb{Z}[-\alpha]$ are submodules of $\mathbb{Z}[\alpha, \beta]$, and $\mathbb{Z}$ is Noetherian; so $\mathbb{Z}[\alpha + \beta]$, $\mathbb{Z}[\alpha\beta]$, and $\mathbb{Z}[-\alpha]$ are finitely generated, and $\alpha + \beta, \alpha\beta, -\alpha \in \mathcal{O}_K$. So $\mathcal{O}_K$ is a ring.

1 Dedekind domains

Definition 1.1. A *number ring* is the ring of integers of a number field.

It turns out that for number rings, being a UFD is equivalent to being a PID. Not all rings satisfy this property:

Example 1.2. $\mathbb{Z}[\sqrt{10}]$ is not a UFD: $10 = \sqrt{10}\sqrt{10} = 2 \cdot 5$, and all of $\sqrt{10}$, 2, and 5 are irreducible.

We define a kind of ring that better corresponds to number rings:

Definition 1.3. Suppose D is a domain, $T \subseteq D$ is a subring, and $\alpha \in D$ is an element. Then α is *integral over* T if and only if $p(\alpha) = 0$ for some monic $p \in T[x]$.

Fact 1.4. *If T is Noetherian, then α is integral over T if and only if $T[\alpha]$ is a finitely-generated T-module.*

Definition 1.5. The *integral closure of T in D* is $\{\, \alpha \in D : \alpha \text{ is integral over } T \,\}$.

Fact 1.6. *The integral closure of T in D is a ring.*

So the ring of integers $\mathcal{O}_K$ in a number field K is the integral closure of $\mathbb{Z}$ in K.

Definition 1.7. We say D is *integral over* T if every element of D is integral over T.

Fact 1.8. *Suppose $A \subseteq B \subseteq C$ are domains. If B is integral over A and C is integral over B, then C is integral over A.*

Hence the integral closure of $\mathcal{O}_K$ in K is $\mathcal{O}_K$, since every element of the integral closure of $\mathcal{O}_K$ in K is integral over $\mathcal{O}$, and is therefore already in $\mathcal{O}_K$.

Definition 1.9. A *Dedekind domain* is a domain D that is not a field satisfying the following:

1. D is Noetherian.
2. Every non-zero prime ideal of D is maximal.
3. D is integrally closed in its field of fractions.

Proposition 1.10. *Suppose K is a number field of degree d over $\mathbb{Q}$; let $\mathcal{O}_K$ be the ring of integers in K. Suppose $I \subseteq \mathcal{O}_K$ is a non-zero ideal. Then $I \cong \mathbb{Z}^d$ as additive grapes.*

Proof. We first check the case $I = \mathcal{O}_K$.

Claim 1.11. *For any $\alpha \in K$ there is some $n \in \mathbb{Z}$ such that $n\alpha \in \mathcal{O}_K$.*

Proof. Let $p \in \mathbb{Q}[x]$ be the monic minimal polynomial for α over $\mathbb{Q}$. Then for any $n \in \mathbb{N}$, we have $n^a p(\frac{x}{n})$ is the monic minimal polynomial for $n\alpha$ over $\mathbb{Q}$ (where $a = \deg(p)$). If we choose n to cancel the denominators of the coefficients of $p(x)$, we get that $n^a p(\frac{x}{n}) \in \mathbb{Z}$. □ Claim 1.11

Now, let $\alpha_1, \ldots, \alpha_d$ be a basis for K as a vector space over $\mathbb{Q}$. By the claim, we may assume that $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. So $\mathcal{O}_K$ contains an additive subgrape additively isomorphic to $\mathbb{Z}^d$; i.e. $\mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_d$.

We now find non-zero $A \in \mathbb{Z}$ such that $A\mathcal{O}_K \subseteq \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_d$. Choose any $b \in \mathcal{O}_K$. Since $\alpha_1, \ldots, \alpha_n$ are a basis for K over $\mathbb{Q}$, we may write

$$b = a_1\alpha_1 + \cdots + a_d\alpha_d$$

for some (unique) $a_1, \ldots, a_d \in \mathbb{Q}$. For simplicity, we assume that K is a Galois extension of $\mathbb{Q}$. Then for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we get a new equation

$$\sigma_i(b) = a_1\sigma_i(\alpha_1) + \cdots + a_d\sigma_i(\alpha_d)$$

This yields a $d \times d$ system of linear equations in $a_1, \ldots, a_d$:

$$\begin{pmatrix} \sigma_1(b) \\ \vdots \\ \sigma_d(b) \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}$$

But M is invertible: since the $a_1, \ldots, a_d$ are unique, there is a unique solution. So, by Cramer's rule, we get that

$$\begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} = M^{-1} \begin{pmatrix} \sigma_1(b) \\ \vdots \\ \sigma_d(b) \end{pmatrix} = \frac{1}{\det(M)} M' \begin{pmatrix} \sigma_1(b) \\ \vdots \\ \sigma_d(b) \end{pmatrix} \in \frac{1}{\det(M)} \mathcal{O}_K^d$$

But $\det(M) \in \mathcal{O}_K$; so there is an integer $A \in \mathbb{Z}$ such that $\frac{A}{\det(M)} \in \mathcal{O}_K$. So each Aa_i is in $\mathcal{O}_K$. But $Aa_i \in \mathbb{Q}$; so each $a_i \in \mathbb{Z}$, and $Ab \in \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_d$. Since A doesn't depend on b, we get that

$$A\mathcal{O}_K \subseteq \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_d$$

So $\mathcal{O}_K$ is additively isomorphic to a subgrape of $\mathbb{Z}^d$ that contains a copy of $\mathbb{Z}^d$; so $\mathcal{O}_K \cong \mathbb{Z}^d$ as an additive grape.

Now, let $I \subseteq \mathcal{O}_K$ be any non-zero ideal; let $\alpha \in I$ be non-zero. Then $\gamma\mathcal{O}_K \subseteq I$, and $\gamma\mathcal{O}_K \cong \mathcal{O}_K \cong \mathbb{Z}^d$ as additive grapes; better yet, we have $I \subseteq \mathcal{O}_K \cong \mathbb{Z}^d$ as an additive grape. So $I \cong \mathbb{Z}^d$ as an additive grape. □ Proposition 1.10

This then implies that every non-zero prime of $\mathcal{O}_K$ is maximal: for any prime ideal P of $\mathcal{O}_K$, we note that the quotient $\mathcal{O}_K/P$ is an integral domain and it must have finite rank, and is thus a field. So $\mathcal{O}_K$ is a Dedekind domain for every number field K.

In general, every PID that is not a field is a Dedekind domain. We also have that every number ring is a Dedekind domain. In general, we can ask how close a number ring is to being a PID.

Definition 1.12. Suppose D is a domain with fraction field K. A *fractional ideal* of D is a D-submodule I of K such that $\alpha I \subseteq D$ for some $\alpha \in K \setminus \{0\}$.

Remark 1.13. Fractional ideals of D are $\frac{1}{\alpha}I$ for $\alpha \in D \setminus \{0\}$ and some *integral ideal* $I \subseteq D$ (i.e. an ideal in the usual ring-theoretic sense).

Definition 1.14. A fractional ideal I is *invertible* if there is some fractional ideal J such that $IJ = D = (1)$. The *ideal grape of* D is the grape of invertible fractional ideals under $\cdot$.

Definition 1.15. Suppose I is a non-zero fractional ideal of D. We define $I^{-1} = \{\alpha \in K : \alpha I \subseteq D\}$.

Theorem 1.16. *I^{-1} is a fractional ideal, and $II^{-1} = D$ if and only if I is invertible; furthermore, in this case we have that I^{-1} is the unique fractional ideal J with $IJ = D$.*

Proof. We first check that I^{-1} is a fractional ideal. It is immediate that $0 \in I^{-1}$. To check closure under addition, suppose $\alpha, \beta \in I^{-1}$; then $(\alpha + \beta)I = \alpha I + \beta I \subseteq D$, and $\alpha + \beta \in I^{-1}$. To see closure under multiplication by arbitrary elements of D, suppose $\alpha \in I^{-1}$ and $\delta \in D$; then $\delta\alpha I \subseteq \delta D \subseteq D$, and $\delta\alpha \in I^{-1}$. So I^{-1} is a fractional ideal.

We now check the equivalence above.

($\implies$) Immediate.

($\impliedby$) Suppose I is invertible; then there is some fractional ideal J of D with $IJ = D$. Hence $J \subseteq I^{-1}$; then $IJ \subseteq II^{-1} \subseteq D = IJ$, and $II^{-1} = D$.

For the "furthermore", we note that

$$J = J(II^{-1}) = (JI)I^{-1} = DI^{-1} = I^{-1}$$

□ Theorem 1.16

Example 1.17. $I = (2, 1+\sqrt{5}) \subseteq \mathbb{Z}[\sqrt{5}]$ is not invertible. To compute I^{-1}, we note that $a + b\sqrt{5} \in I^{-1}$ is equivalent to requiring that $(1+\sqrt{5})(a+b\sqrt{5}) \in \mathbb{Z}[\sqrt{5}]$ and $2(a+b\sqrt{5}) \in \mathbb{Z}[\sqrt{5}]$. So

$$\begin{aligned} I^{-1} &= \left\{ \frac{n}{2} + \frac{m}{2}\sqrt{5} : m \equiv n \pmod 2 \right\} \\ &= \left\{ \frac{n}{2} + \frac{n+2k}{2}\sqrt{5} : n, k \in \mathbb{Z} \right\} \\ &= \left\{ n\frac{1+\sqrt{5}}{2} + k\sqrt{5} : n, k \in \mathbb{Z} \right\} \\ &= \left(\frac{1+\sqrt{5}}{2}, \sqrt{5} \right) \end{aligned}$$

But

$$(2D + (1+\sqrt{5})D)\left(\left(\frac{1+\sqrt{5}}{2}\right)D + \sqrt{5}D\right) = (1+\sqrt{5})D + 2\sqrt{5}D + (3+\sqrt{5})D + (5+\sqrt{5})D \subseteq 2\mathbb{Z} + \sqrt{5}\mathbb{Z} \subsetneq D$$

Definition 1.18. Suppose D is a domain. The *class grape of* D is the following quotient:

$$\mathrm{Cl}(D) = \{ \text{invertible fractional ideals} \} / \{ \text{principal fractional ideals} \}$$

If every fractional ideal of D is invertible, then $\mathrm{Cl}(D)$ measures how close D is to being a PID; in particular, D is a PID if and only if $\mathrm{Cl}(D) = \{1\}$ (under the above assumption).

We will show that every non-zero fractional ideal of a Dedekind domain is invertible.

Definition 1.19. Suppose D is a domain with fraction field K; suppose $P \subseteq D$ is a prime ideal. We define the *local ring of* D *at* P to be

$$D_P = \left\{ \alpha \in K : \alpha = \frac{a}{b}, b \notin P \right\}$$

One checks that this is a ring whose unique maximal ideal is

$$PD_P = \left\{ \frac{a}{b} : a \in P, b \notin P \right\}$$

Example 1.20. Consider $D = \mathbb{Z}$, $P = (2)$. Then

$$D_P = \mathbb{Z}_{(2)} = \left\{ \alpha \in \mathbb{Q} : \alpha = \frac{a}{b}, b \notin (2) \right\} = \left\{ \alpha \in \mathbb{Q} : \alpha = \frac{a}{b}, b \text{ odd} \right\}$$

Now, given $\frac{a}{b} \in \mathbb{Q}$, we can write

$$\frac{a}{b} = 2^n \frac{a'}{b'}$$

where $2 \nmid a'b'$; this n is called the *(additive)* 2*-adic valuation of* $\frac{a}{b}$, denoted $v_2(\frac{a}{b})$. Then $\mathbb{Z}_{(2)} = \{ \alpha \in \mathbb{Q} : v_2(\alpha) \geq 0 \}$.

A result from algebra:

Theorem 1.21. *If D is a Dedekind domain, then D_P is a PID.*

Definition 1.22. A *local ring* is a ring that has a unique maximal ideal.

Definition 1.23. A *discrete valuation ring* (or *DVR*) is a local ring that is also a PID (and is not a field).

Now, if D_P is a DVR with maximal ideal PD_P, then $PD_P = uD_P$; we call u a *uniformizing parameter* or *uniformizer* for D_P.

Let K be the fraction field of D_P (which is also the fraction field of D). If $\alpha \in K \setminus \{0\}$, we define $v_P(\alpha) = \max\{ n \in \mathbb{Z} : \alpha \in (PD_P)^n \}$ where $(PD_P)^0 = D_P$ and $(PD_P)^{-1} = u^{-1}D_P$.

Example 1.24. Using $D = \mathbb{Z}$ and $P = (2)$ as above, we note that $v_2(47) = 0$ since 2 is a uniformizing parameter and $47 \in \mathbb{Z}_{(2)}$ but $47 \notin 2\mathbb{Z}_{(2)}$.

In general we have that $v_P(\alpha)$ is the largest n such that $\alpha = u^n r$ where $r \in D_P$; i.e. $r = \frac{a}{b}$ with $b \notin P$. To achieve the maximum, we demand that $a, b \notin P$; i.e. $v_P(\alpha)$ is the unique n such that there is some unit v of D_P with $\alpha = u^n v$.

Remark 1.25. PD_P is always principal by the above; if $P = (r_1, \dots, r_n)$ and none of $r_1, \dots, r_n$ generated PD_P as an ideal of D_P, then they would all have valuation greater than 2. Hence if u is a uniformizing parameter, then $u^2 \mid r_i$ for all $i \in \{1, \dots, n\}$; so $u^2 \mid r$ for all $r \in r_1 D_P + \cdots + r_n D_P = PD_P$, and in particular we get that $u^2 \mid u$. So u is a unit, a contradiction. So $PD_P = r_i D_P$ for some $i \in \{1, \dots, n\}$.

Theorem 1.26. *Every non-zero fractional ideal in a Dedekind domain is invertible.*

Proof. Suppose D is a Dedekind domain; suppose I is a fractional ideal of D. Then there is some $\alpha \in K$ (where K is the fraction field of D) such that $\alpha I \subseteq D$ is an integral ideal of D. Better yet, αI is invertible if and only if I is invertible; we may thus assume that $I \subseteq D$. Now, $II^{-1} \subseteq D$ by definition of I^{-1}.

If $II^{-1} \neq D$, then there is some non-zero prime ideal P of D with $II^{-1} \subseteq P \subseteq D$; consider the ideal $I_P = ID_P$ of D_P. Also consider the ideal $(I^{-1})_P = I^{-1}D_P$ of D_P. Finally, consider $(I_P)^{-1}$, the inverse of the fractional ideal of I_P of D_P.

Now, D_P is a DVR, and in particular is a PID; so I_P, $(I_P)^{-1}$, and $(I^{-1})_P$ are all principal, and thus invertible. So $I_P(I_P)^{-1} = D_P$.

Claim 1.27. $(I_P)^{-1} = (I^{-1})_P$.

Proof. We first note that

$$(I^{-1})_P = \left\{ \frac{\alpha}{b} : b \notin P, \alpha I \subseteq D \right\} \subseteq \left\{ \frac{\alpha}{b} : \frac{\alpha}{b} I_P \subseteq D_P \right\} = (I_P)^{-1}$$

For the converse, write $I = a_1 D + \cdots + a_n D$. Then $x \in (I_P)^{-1}$ implies that $xa_i \in D_P$ for all i; in particular, there is some $c_i \in D \setminus P$ such that $c_i x a_i \in D$. Now, if $c = c_1 \cdots c_n$, then $(cx)a_i \in D$ for all i. So $cx \in I^{-1}$, and $c \notin P$; so $x \in (I^{-1})_P$. □ Claim 1.27

So $(II^{-1})_P = I_P(I^{-1})_P = I_P(I_P)^{-1} = D_P$. But $II^{-1} \subseteq P \subseteq D$, so $(II^{-1})_P \subseteq P_P \subsetneq D_P$, a contradiction. □ Theorem 1.26

Theorem 1.28. *Every non-zero fractional ideal of a Dedekind domain D can be written uniquely (up to permutation) as a product of prime ideals and their inverses.*

Proof. Let I be a non-zero fractional ideal of D; then $I = \frac{1}{a}J$ for some integral ideal J of D and some $a \in D$. If $J + (a)$ can be factorized, then I can as well; we may thus assume that $I \subseteq D$.

Now, if $I = D$, then I is the empty product of prime ideals, and we're done. If I is prime, we're also done. Otherwise, there is some maximal ideal P with $I \subseteq P \subseteq D$. Then $I = P(IP^{-1})$, and P and IP^{-1} are both integral ideals of D. Iterating, we get

$$I \subseteq IP_1^{-1} \subseteq IP_1^{-1}P_2^{-1} \subseteq \cdots \subseteq D$$

Since D is Noetherian, we get that this process must terminate. Hence $IP_1^{-1} \cdots P_n^{-1} = D$, and $I = P_1 \cdots P_n$.

Uniqueness follows straightforwardly from the invertibility of all of the P_i. □ Theorem 1.28

So every ideal in a Dedekind domain factors uniquely into prime ideals. If we want to understand all ideals, it then suffices to understand prime ideals.

Example 1.29. What do the prime ideals of $\mathbb{Z}[i]$ look like? Well, if $\rho \subseteq \mathbb{Z}[i]$ is prime, then $\mathbb{Z}[i]/\rho$ is a finite field (by Proposition 1.10). So $\mathbb{Z}[i]/\rho \supseteq \mathbb{F}_p$ for some prime p; in other words, $p \in \rho$. i.e. Every prime ρ of $\mathbb{Z}[i]$ contains some prime p of $\mathbb{Z}$; hence $\rho \supseteq (p)$. Hence if we factor (p) inside $\mathbb{Z}[i]$, we will find ρ as a factor.

The upshot is that if we want to find all of the primes of $\mathbb{Z}[i]$, all we have to do is start with the primes $p \in \mathbb{Z}$ and factor (p) in $\mathbb{Z}[i]$; every ρ will show up as a factor for some p.

Case 1. By homework, if $p \equiv 3 \pmod 4$ then (p) is prime in $\mathbb{Z}[i]$.

Case 2. If $p = 2$, we note that $2 = (1+i)(1-i) = (1-i)^2 i$.

Case 3. Suppose $p \equiv 1 \pmod 4$. Note that

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[x]/(p, x^2+1) \cong \mathbb{F}_p/(x^2+1)$$

Fact 1.30. *$x^2 + 1 = (x-a)(x-b)$ in $\mathbb{F}_p[x]$ for some $a, b \in \mathbb{F}_p$.*

Claim 1.31. *$a \neq b$.*

Proof. We simply note that $\gcd(x^2+1, \frac{\mathrm{d}}{\mathrm{d}x}(x^2+1)) = 1$, and hence x^2+1 has no multiple roots. Alternatively, note that $p \neq 2$, so $b = -a \neq a$. □ Claim 1.31

Then $(x-a)$ and $(x-b)$ are comaximal, and

$$\begin{aligned}\mathbb{F}_p/(x^2+1) &\cong \mathbb{F}_p[x]/(x-a)\mathbb{F}_p[x]/(x-b) \\ &\cong \mathbb{Z}[x]/(x^2+1, x-a, p) \times \mathbb{Z}[x]/(x^2+1, x-b, p) \\ &\cong \mathbb{Z}[x]/(x-a, p) \times \mathbb{Z}[x]/(x-b, p)\end{aligned}$$

One then checks (by hand) that $(p) = (p, i-a)(p, i-b)$. (Or one follows the maps through and verifies that the above guarantees equality.)

Hence all the primes in $\mathbb{Z}[i]$ are

- (p) for $p \equiv 3 \pmod 4$
- $(1+i) = (1-i)$
- $(p, i-a)$ where $p \equiv 1 \pmod 4$ and $a^2 \equiv -1 \pmod p$

The above algorithm also works for any quadratic number field; we'll end up with

- Some (p) already prime.
- Some that are of the form $(p) = \rho^2$.
- The rest of the form $(p) = (p, x-a)(p, x-b)$.

We will later show that the class grape is finite.

Question 1.32. How do we tell if we've written down all generators of the class grape?

Some definitions:

Definition 1.33. Suppose K is a number field; suppose $\alpha \in K$ and $[K : \mathbb{Q}] = n$. We then have n embeddings $f_1, \ldots, f_n \colon K \hookrightarrow \mathbb{C}$. We define the *trace of* α to be

$$\mathrm{tr}_K(\alpha) = \sum_{i=1}^{n} f_i(\alpha)$$

We define the *norm of* α to be

$$N_K(\alpha) = \prod_{i=1}^{n} f_i(\alpha)$$

Remark 1.34. Note that $\mathrm{tr}_K(\alpha), N_K(\alpha) \in \mathbb{Q}$, as they are both Galois-invariant. Further note that if $\alpha \in \mathcal{O}_K$, then $\mathrm{tr}(\alpha), N(\alpha) \in \mathbb{Z}$; this is because the characteristic polynomial of α is

$$x^n - \mathrm{tr}(\alpha)x^{n-1} + \cdots \pm N(\alpha)$$

and the characteristic polynomial is a power of the minimal polynomial, which has integer coefficients if $\alpha \in \mathcal{O}_K$.

The converse is false: there are $\alpha \in K \setminus \mathcal{O}_K$ with $\mathrm{tr}(\alpha), N(\alpha) \in \mathbb{Z}$.

Example 1.35. Let $K = \mathbb{Q}(\alpha)$ where α satisfies $x^3 + x^2 + \frac{14}{67}x + 4$. Then $\alpha \in K \setminus \mathcal{O}_K$, but

$$\begin{aligned} \mathrm{tr}(\alpha) &= -1 \\ N(\alpha) &= -4 \end{aligned}$$

Remark 1.36. $\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$ and $N(\alpha\beta) = N(\alpha)N(\beta)$.

Definition 1.37. We say $\alpha_1, \ldots, \alpha_n \in K$ is an *integral basis* if $n = [K : \mathbb{Q}]$ and

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$$

i.e. if $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, they form a $\mathbb{Q}$-basis for K, and $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$. (I think this is just a $\mathbb{Z}$-module basis.)

Remark 1.38. Integral bases always exist, since by Proposition 1.10 we know $\mathcal{O}_K \cong \mathbb{Z}^n$.

Question 1.39. How do we find an integral basis in practice?

Definition 1.40. Let $n = [K : \mathbb{Q}]$. If $\alpha_1, \ldots, \alpha_n \in K$, we define the *discriminant of* $\alpha_1, \ldots, \alpha_n$ to be

$$\det(f_j(\alpha_i))^2 = \left(\det \begin{pmatrix} f_1(\alpha_1) & \cdots & f_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ f_n(\alpha_1) & \cdots & f_n(\alpha_n) \end{pmatrix} \right)^2$$

Example 1.41. A special case: we would like to find $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. This is equivalent to $1, \alpha, \ldots, \alpha^{n-1}$ being an integral basis. Computing the discriminant, we find

$$\begin{aligned} \mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) &= \left(\det \begin{pmatrix} 1 & f_1(\alpha) & f_1(\alpha)^2 & \cdots & f_1(\alpha)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & f_n(\alpha) & f_n(\alpha)^2 & \cdots & f_n(\alpha)^{n-1} \end{pmatrix} \right)^2 \\ &= \prod_{i<j} (f_i(\alpha) - f_j(\alpha))^2 \\ &= \mathrm{disc}\left(\prod_{i=1}^{n} (x - f_i(\alpha)) \right) \\ &= \text{the characteristic polynomial of } \alpha \end{aligned}$$

Remark 1.42. If $\alpha_1, \ldots, \alpha_n \in K$ is *not* a vector space basis for K over $\mathbb{Q}$ then $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0$. This is because in this case we have $c_1, \ldots, c_n \in \mathbb{Q}$ not all 0 such that

$$\sum_{i=1}^{n} c_i \alpha_i = 0$$

So

$$0 = f_j\left(\sum_{i=1}^{n} c_i \alpha_i \right) = \sum_{i=1}^{n} c_i f_j(\alpha_i)$$

for all j. Hence the columns of $(f_j(\alpha_i))_{ij}$ are linearly dependent; hence the determinant is 0, and hence the discriminant is 0.

If, on the other hand, $\alpha_1, \dots, \alpha_n$ *is* a basis, then the discriminant is non-zero. This is because if $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = 0$, then the columns of $(f_j(\alpha_i))_{ij}$ are linearly dependent. So there are $c_1, \dots, c_n \in \mathbb{Q}$ such that for all j we have

$$f_j\left(\sum_{i=1}^{n} c_i \alpha_i\right) = \sum_{i=1}^{n} c_i f_j(\alpha_i) = 0$$

But the f_j are embeddings; so

$$\sum_{i=1}^{n} c_i \alpha_i = 0$$

and the α_i are linearly dependent.

Remark 1.43. If $\{\alpha_1, \dots, \alpha_n\}$ and $\{\beta_1, \dots, \beta_n\}$ are both bases, how do $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$ and $\operatorname{disc}(\beta_1, \dots, \beta_n)$ relate? Well, there is a unique $\mathbb{Q}$-linear $T\colon K \to K$ such that $\alpha_i \mapsto \beta_i$. In this case, we get $T \cdot (f_j(\alpha_i))_{ij} = (f_j(\beta_i))_{ij}$; hence $\operatorname{disc}(\beta_1, \dots, \beta_n) = \det(T)^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n)$.

If in fact $\{\alpha_1, \dots, \alpha_n\}$ is an *integral* basis and $\beta_1, \dots, \beta_n \in \mathcal{O}_K$, then $T \in M_{n\times n}(\mathbb{Z})$; hence

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

where $(\det(T))^2$ is a square integer. Hence if $\{\alpha_1, \dots, \alpha_n\}$ and $\{\beta_1, \dots, \beta_n\}$ are both integral bases, then T is invertible. But $T \in M_n(\mathbb{Z})$; so $\det(T) = \pm 1$, and $\det(T)^2 = 1$. So in this case we get $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \operatorname{disc}(\beta_1, \dots, \beta_n)$.

This allows the following definition:

Definition 1.44. Suppose K is a number field. We define the *discriminant of* K to be $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$ for *any* integral basis $\alpha_1, \dots, \alpha_n$. We just showed that this is well-defined and independent of the choice of integral basis.

Remark 1.45. If $\beta_1, \dots, \beta_n \in \mathcal{O}_K$ and $\operatorname{disc}(\beta_1, \dots, \beta_n) \neq 0$ is not divisible by the square of an integer, then $\{\beta_1, \dots, \beta_n\}$ is an integral basis.

Unfortunately, the converse fails.

Definition 1.46. Say K is a number field with $\mathcal{O}_K$ its ring of integers; say $I \subseteq \mathcal{O}_K$ is a non-zero ideal. We define the *norm* of I to be $N(I) = |\mathcal{O}_K / I|$.

(Recall that the norm of an element is given by

$$N(\alpha) = \prod_{f\colon K \hookrightarrow \mathbb{C}} f_i(\alpha)$$

We will see later how these relate.)

Theorem 1.47. $N(I)^2 = \frac{\operatorname{disc}(I)}{\operatorname{disc}(K)}$.

(I think we define $\operatorname{disc}(I)$ to be the discriminant of an integral basis for I; i.e. $\alpha_1, \dots, \alpha_d \in I$ such that $I = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_d$, where $d = [K : \mathbb{Q}]$. Recall by Proposition 1.10 that $I \cong \mathbb{Z}^d$ as additive grapes.)

Proof. Let $\{a_1, \dots, a_d\}$ and $\{b_1, \dots, b_d\}$ be integral bases for $\mathcal{O}_K$ and I, respectively; let $T\colon \mathcal{O}_K \to I$ be the unique $\mathbb{Q}$-linear transformation with $T(a_i) = b_i$ for all i.

Recall from linear algebra that

$$\pm(\text{volume of the polytope spanned by } \{a_1, \dots, a_d\}) \det(T) = (\text{volume of the polytope spanned by } \{b_1, \dots, b_d\})$$

But then

$$|\det(T)| = \frac{\text{volume of the polytope spanned by } \{a_1, \dots, a_d\}}{\text{volume of the polytope spanned by } \{b_1, \dots, b_d\}} = [\mathcal{O}_K : I] = |\mathcal{O}_K / I| = N(I)$$

(The third equality follows by noting that $(\mathcal{O}_K / I) \cong (K/I)/(K/\mathcal{O}_K)$, with K/I the fundamental polytope of I and $K/\mathcal{O}_K$ the fundamental polytope of $\mathcal{O}_K$. Here the *fundamental domain* of a grape action is a set that every orbit intersects exactly once.)

But $\frac{\operatorname{disc}(I)}{\operatorname{disc}(K)} = (\det(T))^2 = N(I)^2$ by Remark 1.43. □ Theorem 1.47

We can thus extend the definition of norm to fractional ideals as follows:

Definition 1.48. Suppose I is a fractional ideal of $\mathcal{O}_K$. We define

$$N(I) = \sqrt{\frac{\operatorname{disc}(I)}{\operatorname{disc}(K)}}$$

Definition 1.49. A sequence $A \xrightarrow{f} B \xrightarrow{g} C$ is *exact* at B if $\operatorname{im}(f) = \ker(g)$.

TODO 1. *Swapped definition of norm of ideals?*

Theorem 1.50. *Given non-zero fractional ideals I and J of $\mathcal{O}_K$, we have $N(I)N(J) = N(IJ)$.*

Proof. If $I = \alpha I'$, then playing with integral bases we get

$$N(I) = \sqrt{\frac{\operatorname{disc}(K)}{\operatorname{disc}(I)}} = \sqrt{\frac{\operatorname{disc}(K)}{\operatorname{disc}(\alpha I')}} = \frac{1}{|N(\alpha)|}\sqrt{\frac{\operatorname{disc}(K)}{\operatorname{disc}(I')}}$$

So if we choose $\alpha \in \mathcal{O}_K$ such that $\alpha I, \alpha J \subseteq \mathcal{O}_K$, then

$$N(\alpha)^2 N(I)N(J) = N(\alpha I)N(\alpha J)$$

and

$$N(\alpha)^2 N(IJ) = N(\alpha I \alpha J)$$

Hence if we can prove the theorem for αI and αJ, it will follow for I and J; i.e. we may assume $I, J \subseteq \mathcal{O}_K$.

Now, since $\mathcal{O}_K$ is a Dedekind domain, we can factor I and J into primes

$$I = P_1^{a_1} \cdots P_r^{a_r}$$
$$J = P_1^{b_1} \cdots P_r^{b_r}$$

Then $N(I) = N(P_1^{a_1} \cdots P_r^{a_r} = N(P_1^{a_1}) \cdots N(P_r^{a_r})$ by Chinese remainder theorem. (Pairwise comaximality follows by noting that any prime in the factorization of $P_i^{a_i} + P_j^{a_j}$ must contain both $P_i^{a_i}$ and $P_j^{a_j}$, and hence must be both P_i and P_j, a contradiction if $I \neq J$; so the prime factorization is empty, and $P_i^{a_i} + P_j^{a_j} = \mathcal{O}_K$. Alternatively, a general theorem states that powers of distinct maximal ideals are comaximal.) So

$$N(I) = N(P_1^{a_1}) \cdots N(P_r^{a_r})$$
$$N(J) = N(P_1^{b_1}) \cdots N(P_r^{b_r})$$
$$N(J) = N(P_1^{a_1+b_1}) \cdots N(P_r^{a_r+b_r})$$

It then suffices to show that $N(P_i^{a_i}) = N(P_i)^{a_i}$. We proceed by induction on a_i; the claim is clear if $a_i = 1$.

For the induction step, we note that

$$0 \to \underbrace{P_i^{a_i}/P_i^{a_i+1}}_{N(P_i) \text{ elements}} \to \mathcal{O}_K/P_i^{a_i+1} \to \underbrace{\mathcal{O}_K/P_i^{a_i}}_{N(P_i)^{a_i} \text{ elements}} \to 0$$

is exact. The latter claim about sizes is just the induction hypothesis; for the former, we use the following:

Claim 1.51. *$P^a/P^{a+1} \cong P^a D_P/P^{a+1}D_P$ where $D = \mathcal{O}_K$, $P = P_i$, and $a = a_i$.*

Proof. We define $\Phi\colon P^a/P^{a+1} \to P^a D_P/P^{a+1}D_P$ by $a + P^{a+1} \mapsto \alpha + P^{a+1}D_P$. This is clearly an injective homomorphism. For surjectivity, we note that P^a/P^{a+1} is a vector space over $\mathcal{O}_K/P$ via

$$(\alpha + P)(\beta + P^{a+1}) = \alpha\beta + P^{a+1}$$

It has dimension 1, as it is spanned by u^a (where $PD_P = (u)$); surjectivity then follows because because P^a/P^{a+1} is a 1-dimensional vector space over D_P/PD_P and $P^a \neq P^{a+1}$. □ Claim 1.51

In particular, for $a = 0$, we get that $\mathcal{O}_K/P \cong D_P/PD_P$, which has $N(P)$ elements. But $P_i^{a_i}/P_i^{a_i+1}$ is a 1-dimensional vector space over $\mathcal{O}_K/P_i$, as noted above; so by the short exact sequence, we get that $\mathcal{O}_K/P_i^{a_i+1}$ has $N(P_i)N(P_i)^{a_i} = N(P_i)^{a_i+1}$ elements. □ Theorem 1.50

Theorem 1.52. *If $\alpha \neq 0$ then $N((\alpha)) = |N(\alpha)|$.*

Proof. If $K = \mathbb{Q}(\alpha)$, then the characteristic polynomial of $T\colon K \to K$ given by $x \mapsto \alpha x$ is the monic minimal polynomial for α over $\mathbb{Q}$. Its constant term is both $N(\alpha)$ and $\det(T) = \pm N((\alpha))$. □ Theorem 1.52

2 Geometry of numbers

Definition 2.1. Suppose K is a number field. Let $f_1, \dots, f_{r_1}$ be the distinct embeddings of $K \hookrightarrow \mathbb{R}$; let $f_{r_1+1}, g_{r_1+1}, \dots, f_{r_1+r_2}, g_{r_1+r_2}$ be the complex conjugate pairs of embeddings $K \hookrightarrow \mathbb{C}$ (i.e. with $f_i = \overline{g_i}$). Then $[K : \mathbb{Q}] = r_1 + 2r_2 = d$. Define

$$\Theta_K \colon K \to \left(\prod_{i=1}^{r_1} \mathbb{R}\right) \times \left(\prod_{i=1}^{r_2} \mathbb{C}\right)$$

by

$$\alpha \mapsto (f_1(\alpha), \dots, f_{r_1}(\alpha), f_{r_1+1}(\alpha), \dots, f_{r_1+r_2}(\alpha))$$

This Θ_K is the *Minkowski map*. Its codomain is *Minkowski space*, usually considered as a vector space over $\mathbb{R}$.

The choice of which embedding is f_i and which is g_i is not important.

Fact 2.2. *The image of $\mathcal{O}_K$ under Θ_K is a lattice.*

Example 2.3. Let $K = \mathbb{Q}(i)$. We pick $f_1(a + bi) = a + bi$) and $g_1(a + bi) = a - bi$. So $r_1 = 0$ and $r_2 = 1$. Then $\mathcal{O}_K = \mathbb{Z}[i]$, and its image under Θ_K is $\mathbb{Z}[i]$.

Example 2.4. Let $K = \mathbb{Q}(\sqrt{2})$. Here as well we have $r_1 = 2$; we pick $f_1(a+b\sqrt{2}) = a+b\sqrt{2}$ and $f_2(a+b\sqrt{2}) = a-b\sqrt{2}$. We note that $\mathbb{Q}$ gets mapped to the diagonal, with $\mathbb{Z}$ mapped to the integer points on the diagonal. We also note that $\sqrt{2}\mathbb{Q}$ gets mapped to the antidiagonal. We finally note that the "unit ball" (in which $|N(\alpha)| \le 1$) is a hyperbola, since it is defined by $1 = |N(\alpha)| = |f_1(\alpha)f_2(\alpha)|$, and hence is given by $y = \frac{1}{x}$. In particular, it isn't compact.

Remark 2.5. If the unit ball *is* compact, then there are finitely many units in $\mathcal{O}_K$, since units have norm 1.

Remark 2.6. Θ_K is a $\mathbb{Q}$-linear map, since if $\alpha \in \mathbb{Q}$ and $x \in K$ then $f_i(\alpha x) = f_i(\alpha)f_i(x) = \alpha f_i(x)$.

We think of Minkowski space as "unfolding" the $\mathbb{Q}$-vector space so it no longer lies on the real line.

Aside 2.7 (How to compute $\mathcal{O}_K$ from K). Find some algebraic integers $\alpha_1, \dots, \alpha_n \in K$, and consider $R = \mathbb{Z}[\alpha_1, \dots, \alpha_n]$; compute the discriminant Δ of R. By Remark 1.43 we have $\operatorname{disc}(\mathcal{O}_K)(\det(T))^2 = \operatorname{disc}(R)$. But all of these are integers; so if Δ is square-free, then $[\Theta_K : R] = 1$, so $R = \mathcal{O}_K$.

N.B. It might be the case that $\operatorname{disc}(\mathcal{O}_K)$ has a square factor.

Example 2.8. Find $\mathcal{O}_K$ (with proof) if $K = \mathbb{Q}(\alpha)$ where α is a root of $x^3 + 3x + 7 = 0$.

We first make a guess; we let $D = \mathbb{Z}[\alpha]$, and we guess that $D = \mathcal{O}_K$. We know that $\frac{\operatorname{disc}(D)}{\operatorname{disc}(\mathcal{O}_K)} = [\mathcal{O}_K : D]^2$ (where the index is taken as additive grapes).

Let's compute $\operatorname{disc}(D)$. If $\operatorname{disc}(D)$ is square-free, then since $[\mathcal{O}_K : D]^2 \mid \operatorname{disc}(D)$, we get that $[\mathcal{O}_K : D] = 1$ and $D = \mathcal{O}_K$.

Fact 2.9. $|\operatorname{disc}(\mathbb{Z}[\alpha])| = |\operatorname{disc}(m(x))|$ *where $m(x)$ is a monic minimal polynomial for α over $\mathbb{Q}$.*

The *discriminant of a monic polynomial* is

$$\prod_{i<j} (r_i - r_j)^2$$

where the r_i are the roots of the polynomial. It also coincides with the *resultant* of the polynomial and its derivative, given by

$$\operatorname{Res}(f, f') = \det \begin{pmatrix} 1 & a_{n-1} & \cdots & a_0 & & & \\ & 1 & a_{n-1} & \cdots & a_0 & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & 1 & a_{n-1} & \cdots & a_0 \\ n & (n-1)a_{n-1} & \cdots & a_1 & & & \\ & n & (n-1)a_{n-1} & \cdots & a_1 & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & n & (n-1)a_{n-1} & \cdots & a_1 \end{pmatrix}$$

where $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. For example,

$$\operatorname{disc}(x^2 - 2) = \det \begin{pmatrix} 1 & 0 & -2 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} = -8$$

In our case, we end up with

$$|\operatorname{disc}(\mathbb{Z}[\alpha])| = |\operatorname{disc}(x^3 + 3x + 7)| = \left| \det \begin{pmatrix} 1 & 0 & 3 & 7 & 0 \\ 0 & 1 & 0 & 3 & 7 \\ 3 & 0 & 3 & 0 & 0 \\ 0 & 3 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 & 0 \end{pmatrix} \right| = 1431 = 3^3 \cdot 53$$

Thus $[\mathcal{O}_K : D]$ is 3 or 1. Now, if every local ring D_Q (for Q a prime ideal of D) is a DVR, then D is a Dedekind domain (since D is already Noetherian and one-dimensional (i.e. every non-zero prime ideal is maximal)). Conversely, if any D_Q is not a DVR, then D is not a Dedekind domain.

How does this help? Well, Dedekind domains are integrally closed in their field of fractions, and K is the fraction field of D; hence if D is a Dedekind domain then $\mathcal{O}_K \subseteq D$, and $\mathcal{O}_K = D$.

Now, let $Q \subseteq D$ be a prime ideal. How do we check if D_Q is a DVR? Well, D_Q is a DVR if and only if QD_Q is a principal ideal. But every non-zero prime ideal Q of D contains a unique positive prime integer q.

Case 1. If $q \neq 3$ then for any prime ideal P of $\mathcal{O}_K$ with $Q \subseteq P$ we have $D_Q = (\mathcal{O}_K)_P$, which is a local ring.

Proof. If $D = \mathcal{O}_K$, we're done. Otherwise, we have $[\mathcal{O}_K : D] = 3$, so for all $a \in \mathcal{O}_K$ we have $3a \in D$; hence $3a \in D_Q$, and $a \in D_Q$. So $\mathcal{O}_K \subseteq D_Q$, and $(\mathcal{O}_K)_P \subseteq D_Q$. Hence $(\mathcal{O})_P = D_Q$. □

Case 2. We must now check all the prime ideals Q of D containing 3. By the correspondence theorem, these are in bijection with prime ideals of

$$D/(3) \cong \mathbb{Z}[x]/(x^3 + 3x + 7, 3) \cong (\mathbb{Z}/3\mathbb{Z})[x]/(x^3 + 3x + 7) \cong (\mathbb{Z}/3\mathbb{Z})[x]/(x + 1)^3$$

Fact 2.10 (IMPORTANT). *In general the prime ideals of $F[x]/(g)$ correspond to the irreducible factors of g.*

In our case, we get that the only prime ideal of $D/(3)$ is $(\alpha+1)$, which corresponds to the ideal $(\alpha+1, 3)$ of D. So $Q = (\alpha + 1, 3)$ is the only prime ideal of $D = \mathbb{Z}[\alpha]$ containing 3.

We now check if QD_Q is principal. (This is equivalent to checking that Q is a DVR.) Well, $QD_Q = (3, \alpha + 1)D_Q$ is a principal ideal if and only if $QD_Q = (3)D_Q$ or $QD_Q = (\alpha + 1)D_Q$, which occurs if and only if $\frac{3}{\alpha+1} \in D_Q$ or $\frac{\alpha+1}{3} \in D_Q$. We easily get that $\frac{3}{\alpha+1} \notin D_Q$; on the other hand, we have

$$(\alpha + 1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = -3\alpha - 7 + 3\alpha^2 + 3\alpha + 1 = 3\alpha^2 - 6 = 3(\alpha^2 - 2)$$

Hence

$$\frac{3}{\alpha + 1} = \frac{(\alpha + 1)^2}{\alpha^2 - 2} \in D_Q$$

But $\alpha^2 - 2 \notin Q$ (since $(\alpha+1)(\alpha-1) = \alpha^2 - 1 \in Q$, and hence otherwise we would have $1 \in Q$). Hence $\frac{3}{\alpha+1} \in D_Q$. So QD_Q is principal.

So D is a Dedekind domain, and $D = \mathcal{O}_K$.

Theorem 2.11 (Convex body)**.** *Suppose L is a lattice in $\mathbb{R}^n$; i.e. L is a subgrape of $\mathbb{R}^n$ isomorphic to $\mathbb{Z}^n$ with the property that a basis for L (over $\mathbb{Z}$) is also a basis for $\mathbb{R}^n$ as a vector space. Let F be the fundamental domain of L; i.e. a subset of $\mathbb{R}^n$ such each coset of L intersects in exactly one point. (We will need F to have a sensible volume, so we will require that it be measurable, and in practice we will imagine it to be the parallelepiped given by the basis for L.) Let S be a symmetric convex subset of $\mathbb{R}^n$. ("Symmetric" here means that if $x \in S$ then $-x \in S$.) If $\operatorname{vol}(S) > 2^n \operatorname{vol}(F)$ then $S \cap L$ contains a non-zero vector.*

Proof. We may assume S is bounded. For any $\overrightarrow{v} \in L$ we define

$$T_{\overrightarrow{v}} = \frac{1}{2}S + \overrightarrow{v} = \{\, \frac{1}{2}\overrightarrow{x} + \overrightarrow{v} : \overrightarrow{x} \in S \,\}$$

Then

$$\mathrm{vol}(T_{\overrightarrow{v}}) = \frac{\mathrm{vol}(S)}{2^n} > \mathrm{vol}(F)$$

Hence for some $\overrightarrow{v} \neq \overrightarrow{w} \in L$, we must have $T_{\overrightarrow{v}} \cap T_{\overrightarrow{w}} \neq \emptyset$. Then for some $\overrightarrow{x}, \overrightarrow{y} \in S$, we have

$$\frac{1}{2}\overrightarrow{x} + \overrightarrow{v} = \frac{1}{2}\overrightarrow{y} + \overrightarrow{w}$$

and thus

$$\overrightarrow{v} - \overrightarrow{w} = \frac{1}{2}(\overrightarrow{y} - \overrightarrow{x}) \in S$$

So $\overrightarrow{v} - \overrightarrow{w} \in (L \cap S) \setminus \{\, 0 \,\}$. □ Theorem 2.11

Example 2.12. Consider $K = \mathbb{Q}[\sqrt{15}]$, in which $\mathcal{O}_K = \mathbb{Z}[\sqrt{15}]$. Draw the lattices $\mathcal{O}_K$, $(2, 3 - \sqrt{15})$, and $(3, \sqrt{15})$ in Minkowski space. Compute the fundamental domain volumes, discriminants, and smallest nonzero vectors.

Theorem 2.13. *Suppose K is a number field of degree $n = r_1 + 2r_2$ (where r_1 is the number of real embeddings of K and r_2 is the number of complex conjugate pairs of complex embeddings). Let $A \subseteq \mathcal{O}_K$ be an additive subgrape of finite index m. Then there is some $\alpha \in A$ with*

$$|N(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!m}{n^n} \sqrt{\mathrm{disc}(\mathcal{O}_K)}$$

(Note here that $\sqrt{\mathrm{disc}(\mathcal{O}_K)}$ is the volume of the fundamental domain of $\mathcal{O}_K$, and $m\sqrt{\mathrm{disc}(\mathcal{O}_K)}$ is the volume of the fundamental domain of A.)

Proof. For $B \in \mathbb{R}$ define

$$S_B = \left\{ (\alpha_1, \ldots, \alpha_{r_1}, \beta_1, \ldots, \beta_{r_2}) : \sum_{j=1}^{r_1} |\alpha_j| + 2\sum_{j=1}^{r_2} |\beta_j| \leq B \right\} \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

For example, if $r_1 = 0$ and $r_2 = 1$ then we end up with the disc $2|z| \leq B$; if $r_1 = 2$ and $r_2 = 0$ then we end up with the diamond $|x| + |y| \leq B$. It turns out S_B are "roughly" products of the things in the above two examples. In particular, S_B is bounded, symmetric, and convex, with volume

$$2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{B^n}{n!}$$

Pick $B > \left(\left(\frac{4}{\pi}\right)^{r_2} n!m\sqrt{\mathrm{disc}(\mathcal{O}_K)}\right)^{\frac{1}{n}}$. Then

$$\mathrm{vol}(S_B) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{B^n}{n!} > 2^n\left(2^{-r_2} m\sqrt{\mathrm{disc}(\mathcal{O}_K)}\right)$$

But the volume of a fundamental polytope of A is $2^{-r_2}(m\sqrt{\mathrm{disc}(\mathcal{O}_K)})$; hence by Theorem 2.11 there is nonzero $\alpha \in \Theta^{-1}(\Theta(A) \cap S_B)$.

Now, let $f_1, \ldots, f_{r_1+r_2}$ be the embeddings of K into $\mathbb{R}$ and $\mathcal{C}$ (up to complex conjugation). Then

$$\sum_{j=1}^{r_1} |f_j(\alpha)| + 2\sum_{j=1}^{r_2} |f_{r_1+j}(\alpha)| \leq \left(\left(\frac{4}{\pi}\right)^{r_2} n!m\sqrt{\mathrm{disc}(\mathcal{O}_K)}\right)^{\frac{1}{n}} + \varepsilon$$

$$\implies \left(\sum_{j=1}^{r_1} |f_j(\alpha)| + 2\sum_{j=1}^{r_2} |f_{r_1+j}(\alpha)|\right)^n \leq \left(\frac{4}{\pi}\right)^{r_2} n!m\sqrt{\mathrm{disc}(\mathcal{O}_K)} + \varepsilon'$$

$$\implies \left(\frac{1}{n}\sum_{j=1}^{r_1} |f_j(\alpha)| + \frac{2}{n}\sum_{j=1}^{r_2} |f_{r_1+j}(\alpha)|\right) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} m\sqrt{\mathrm{disc}(\mathcal{O}_K)} + \varepsilon''$$

(Here $\varepsilon = B - \left(\left(\frac{4}{\pi}\right)^{r_2} n! m \sqrt{\operatorname{disc}(\mathcal{O}_K)}\right)^{\frac{1}{n}}$, and ε' and ε'' can be computed from ε; in particular, they approach 0 as ε approaches 0.)

Hence, by the arithmetic-geometric mean inequality, we get that

$$|N(\alpha)| = \prod_{j=1}^{r_1} |f_j(\alpha)| \prod_{j=1}^{r_2} |f_{r_1+j}(\alpha)|^2 \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} m \sqrt{\operatorname{disc}(\mathcal{O}_K} + \varepsilon''$$

We somehow concluded that an α can be chosen to work for all sufficiently small ε. Hence this is our desired α. □ Theorem 2.13

In particular, if $A = I$ is an ideal, then $m = N(I)$; so we have $\alpha \in I$ with

$$|N(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{\operatorname{disc}(\mathcal{O}_K)} N(I)$$

Exercise 2.14. Verify the above theorem for $K = \mathbb{Q}(\sqrt{15})$ with ideals $\mathbb{Z}[\sqrt{15}]$, $(2, 3 - \sqrt{15})$, and $(3, \sqrt{15})$.

When working in a fixed K with r_1 real embeddings and r_2 pairs of complex embeddings, we typically denote

$$M = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{\operatorname{disc}(\mathcal{O}_K)}$$

Theorem 2.15. *Suppose K is a number field. Then $\mathrm{Cl}(\mathcal{O}_K)$ is finite.*

Proof. Well, for any $B \in \mathbb{R}$ we have that there are only finitely many fractional ideals I with $N(I) \leq B$; it then suffices to show that there is some B such that every ideal class contains a representative of norm $\leq B$.

Let $B = M = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{\operatorname{disc}(\mathcal{O}_K)}$. We will show that for any fractional ideal I there is some $\alpha \in K^*$ with $N(\alpha I) \leq M$.

Suppose I is a non-zero fractional ideal; then there is an integral ideal $J \subseteq \mathcal{O}_K$ in the ideal class of I^{-1}. Then by Theorem 2.13 there is some $\alpha \in J \setminus \{0\}$ with $|N(\alpha)| \leq M \cdot N(J)$. But $I \equiv \alpha J^{-1}$ in $\mathrm{Cl}(\mathcal{O}_K)$, and

$$N(\alpha J^{-1}) = \frac{|N(\alpha)|}{|N(J)|} \leq M$$

as desired. □ Theorem 2.15

Example 2.16. Compute the ideal class grape of $\mathcal{O}_K$ in $K = \mathbb{Q}(\alpha)$ where $\alpha^3 + 3\alpha + 7 = 0$. (See Example 2.8.) Our steps:

1. We compute $\mathcal{O}_K$. In our case, Example 2.8 yields that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
2. We compute
$$M = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{\operatorname{disc}(\mathcal{O}_K)} \approx 10.7 < 11$$
3. Pick representatives of each of the residue classes of $\mathbb{Z}/\lceil M \rceil \mathbb{Z}$, apply f, and factor the results; ideally pick representatives n that make $f(n)$ small.

-5	-133	$= -7 \cdot 19$
-4	-69	$= -3 \cdot 23$
-3	-29	
-2	-7	
-1	3	
0	7	
1	11	
2	21	$= 3 \cdot 7$
3	43	
4	83	
5	147	$= 3 \cdot 7^2$

Why is this useful? Well, for any n we have $|N(\alpha - n)|$ is the absolute value of the constant coefficient of the minimal polynomial for $\alpha - n$. But the minimal polynomial for $\alpha - n$ is $f(x+n)$, which has constant term $f(n)$; hence $|N(\alpha - n)| = |f(n)|$.

4. List all the ideals of $\mathcal{O}_K$ of norm $< M$.

   - (2) is prime since $\mathbb{Z}[\alpha]/(2) \cong (\mathbb{Z}/2\mathbb{Z})[x]/(x^3 + x + 1)$ is a field.
   - $(3) = (3, \alpha + 1)^3$, as computed in Example 2.8; we let $P_3 = (3, \alpha + 1)$.
   - (5) is prime.
   - $(7) = (7, \alpha)(7, \alpha + 2)(7, \alpha + 5) = P_7 Q_7 R_7$.

   But any prime P of norm < 11 would have to satisfy $|\mathcal{O}_K/P| = p^e$ for some $p \in \{2, 3, 5, 7\}$, and hence would have to contain one such p. So these are all the primes of norm < 11.

5. The above primes thus generate $\mathrm{Cl}(K)$; in fact we can omit the principal ideals, so we get $\mathrm{Cl}(K) = \langle P_3, P_7, Q_7, R_7 \rangle$.

   We immediately get that $P_3^3 \equiv 1$ and $P_7 Q_7 R_7 \equiv 1$. Using the table, we see that $|N(\alpha)| = |f(0)| = 7$, and hence that $|\mathcal{O}_K/(\alpha)| = N((\alpha)) = |N(\alpha)| = 7$; in particular we get that $7 \equiv 0$ in $\mathcal{O}_K/(\alpha)$, and that $7 \in (\alpha)$, and thus that $P_7 = (7, \alpha) = (\alpha)$. So P_7 is principal, and $P_7 \equiv 1$.

   We likewise get that $P_3 R_7 \equiv 1$ (since $|N(\alpha - 2)| = 21$ implies that $P_3 R_7 = (\alpha - 2)$) and that $P_3 Q_7^2 \equiv 1$ (since $|N(\alpha - 5)| = 3 \cdot 7^2$ implies $(\alpha - 5) = P_3 Q_7^2$ since $5 \in Q_7$ and $5 \notin R_7$).

   Continuing, we find $P_3 \equiv 1$ and $Q_7 \equiv 1$. So $\mathrm{Cl}(K)$ is trivial.

Exercise 2.17. Compute $\mathrm{Cl}(\mathbb{Q}(\sqrt{46}))$. (It will be the trivial grape.)

We showed last time how to compute the ideal class grape, modulo being able to figure out if a given ideal is principal. We do an example of the last question.

Example 2.18. Say $K = \mathbb{Q}(\sqrt{10})$; then $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$. Consider $P = (2, \sqrt{10})$. Is P principal?

Well, if P is principal, then $P = (\alpha)$ for some α, and $|N(\alpha)| = N(P) = 2$. But $\alpha = a + b\sqrt{10}$ for some $a, b \in \mathbb{Z}$. So

$$a^2 - 10b^2 = \pm 2$$

Reducing this equation modulo 5, we find that $a^2 \equiv \pm 2 \pmod 5$, which has no solutions for a. So P is not principal.

This strategy works for all quadratic number fields.

Example 2.19. Let $K = \mathbb{Q}(\alpha)$ where $\alpha^3 - 2\alpha + 5 = 0$.

1. It turns out then that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. (One checks that the discriminant is -643, which is prime, and in particular is square-free.)

2. The Minkowski constant is then

$$M = \left(\frac{4}{\pi}\right)^{r_2} \left(\frac{n!}{n^n}\right) \sqrt{|\mathrm{disc}(K)|} = \frac{4}{\pi}\frac{6}{27}\sqrt{643} \leq 8$$

   (Observe that making the Minkowski constant a bit bigger won't be problematic; it may just make a bit more work.)

3.

-3	-16	$= -2^4$	$= -N(\alpha + 3)$
-2	1		$= -N(\alpha + 2)$
-1	6	$= 2 \cdot 3$	$= -N(\alpha + 1)$
0	5		$= -N(\alpha)$
1	4	$= 2^2$	$= -N(\alpha - 1)$
2	9	$= 3^2$	$= -N(\alpha - 2)$
3	26	$= 2 \cdot 13$	$= -N(\alpha - 3)$

4.

$$(2) = \underbrace{P_2}_{\text{norm 2}} \cdot \underbrace{Q_2}_{\text{norm 4}}$$
$$(3) = \underbrace{P_3}_{\text{norm 3}} \cdot \underbrace{Q_3}_{\text{norm 9}}$$
$$(5) = \underbrace{P_5}_{\text{norm 5}} \cdot \underbrace{Q_5}_{\text{norm 25}}$$
$$(7)$$

5.

$$P_2Q_2 \equiv 1$$
$$P_3Q_3 \equiv 1$$
$$P_5Q_5 \equiv 1$$
$$P_2P_3 \equiv 1$$
$$P_5 \equiv 1$$
$$P_3^2 \equiv 1$$

Manipulating, we find that $P_2 \equiv P_3$ and $P_2 \equiv Q_2$. So $\mathrm{Cl}(K) = \langle P_2 \rangle$ with $P_2^2 \equiv 1$. Is P_2 principal? Well, $P_2 = (2, \alpha + 1)$. Our plan is to find a small box B such that if there is an element of norm 2 then there is an element of norm 2 in B; we will then look in B. Now,

$$\Theta_K(a) = (f_1(a), f_2(a)) \in \mathbb{R} \times \mathbb{C}$$

Checking by hand, we find that

$$1 < |f_2(\alpha + 2)| < \frac{10}{3}$$

If $|N(u)| = 2$, then by multiplying and dividing by appropriate powers of $\alpha + 2$ (which has norm 1), we can ensure that

$$1 \leq |f_2(u)| \leq \frac{10}{3}$$

Since $|N(u)| = 2$, we get that $|f_1(u)||f_2(u)| = 2$; hence

$$\frac{3}{5} \leq |f_1(u)| \leq 2$$

So our box is

$$|f_1(u)| \leq 2$$
$$|f_2(u)| \leq \frac{10}{3}$$

This box contains $1 - \alpha$, α, 1, $2 - \alpha$, and other elements that obviously don't have norm ± 2. (e.g. $2 - 2\alpha$ has a factor of 2, and hence its norm has a factor of 4, and is not 2.)

What does the grape $\mathcal{O}_K^*$ look like? Well, it contains elements of finite order, namely the roots of unity in K.

Definition 2.20. Let

$$V_K = \left(\prod_{i=1}^{r_1} \mathbb{R} \right) \times \left(\prod_{i=1}^{r_2} \mathbb{C} \right)$$

be Minkowski space. We define a map

$$\log \colon V_K' \to \prod_{i=1}^{r_1 + r_2}$$

(where $V_K' = V_K \setminus \{ (x_1, \dots, x_{r_1}, z_{r_1+1}, \dots, z_{r_1+r_2}) : x_1 \cdots x_{r_1} z_{r_1+1} \cdots z_{r_1+r_2} = 0 \}$) by

$$\log(x_1, \dots, x_{r_1}, z_{r_1+1}, \dots, z_{r_1+r_2}) = (\log(|x_1|), \dots, \log(|x_{r_1}|), 2\log(|z_{r_1+1}|), \dots, 2\log(|z_{r_1+r_2}|))$$

(The base doesn't particular matter; we can choose e.)

The point of log is to turn the multiplicative set $\mathcal{O}_K^*$ into the additive subset $\log(\Theta_K(\mathcal{O}_K^*))$.

Remark 2.21. One notes that log and Θ_K are homomorphisms; what is $\ker(\log \circ \Theta_K)$? It's the grape of roots of unity. Indeed, if w is a root of unity, then $|f_i(w)| = 1$ for all i, and $\log(\Theta_K(w)) = 0$. Conversely, if $\log(\Theta_K(w)) = 0$, then $|f_i(w)| = 1$ for all i; hence every power of w is contained in the finite set $\Theta_K(\mathcal{O}_K) \cap B$ (where $B = \{ v : |v_i| \leq 1 \}$). Hence $w^a = w^b$ for some $a \neq b$, and w is a root of unity.

Hence

$$0 \to W \xrightarrow{i} \mathcal{O}_K^* \xrightarrow{\log \circ \Theta_K} \Gamma \to 0$$

is a short exact sequence, where W is the grape of roots of unity in K and $\Gamma = \log(\Theta_K(\mathcal{O}_K^*))$; i.e. $\log \circ \Theta_K$ induces an isomorphism $\mathcal{O}_K^*/W \cong \Gamma$.

Sadly, Γ is not a full lattice in $\mathbb{R}^{r_1+r_2}$: if $\alpha \in \mathcal{O}_K^*$, then $|N(\alpha)| = 1$; hence

$$\prod_{i=1}^{r_1} |f_i(\alpha)| \cdot \prod_{i=1}^{r_2} |f_{r_1+i}(\alpha)|^2 = 1$$

and thus

$$\sum_{i=1}^{r_1} \log(|f_i(\alpha)|) + 2 \sum_{i=1}^{r_2} \log(|f_{r_1+i}(\alpha)|) = 0$$

So $\log(\Theta_K(\alpha)) \in H$ where $H \subseteq \mathbb{R}^{r_1+r_2}$ is the hyperplane given by

$$\sum_{i=1}^{r_1+r_2} x_i = 0$$

(where the x_i are the coordinates in $\mathbb{R}^{r_1+r_2}$).

Theorem 2.22 (Dirichlet Unit Theorem)**.** *Let K be a number field of degree d with r_1 real embeddings and r_2 pairs of complex embeddings. Then $\mathcal{O}_K^* \cong W \times \mathbb{Z}^{r_1+r_2-1}$ where W is the grape of roots of unity in K.*

Exercise 2.23. Compute $\mathcal{O}_K^*$, where $K = \mathbb{Q}(\sqrt{2})$.

It turns out $\mathcal{O}_K^*$ is generated by -1 and $1+\sqrt{2}$. By the Dirichlet unit theorem, we get that the torsion-free part of $\mathcal{O}_K^*$ is cyclic; hence, since $1+\sqrt{2}$ has infinite order, it must be a power of the generator. But if $1+\sqrt{2}$ is a power of some $\alpha \in \mathcal{O}_K^*$, then in particular every coordinate of $1+\sqrt{2}$ in Minkowski space is a power of the corresponding coordinate of α; i.e. $f_i(\alpha)^n = f_i(1+\sqrt{2})$ for all i. But then $|f_i(\alpha)| \leq |f_i(1+\sqrt{2})|$ for all i, which yields a box in Minkowski space; checking every element of the box, we find that none of them has $1+\sqrt{2}$ as a power. (In principal this would involve checking every power of everything in the box; however, for any α in the box we note that once n becomes large enough that α^n lands outside the box, we can stop checking.)

Proof of Theorem 2.22. We have maps

$$K^* \xrightarrow{\theta_K} \prod_{i=1}^{r_1} \mathbb{R} \times \prod_{i=1}^{r_2} \mathbb{C} \xrightarrow{\log} \mathbb{R}^{r_1+r_2}$$

Let $\Gamma = \log|\theta_K(\mathcal{O}_K^*)|$. We will prove that Γ is a full lattice in the (r_1+r_2-1)-dimensional space $H = \{ (x_1, \dots, x_{r_1+r_2}) : x_1 + \cdots + x_{r_1+r_2} = 0 \}$.

1. Modulo units, there are only finitely many elements of $\mathcal{O}_K$ of norm N, for any fixed N. Indeed, if $N(\alpha) = N$, then $N((\alpha)) = |N|$, and $N \in (\alpha)$; so there are only finitely many choices for (α), and hence only finitely many choices for α up to units.

2. Note that Γ is a discrete subset of $\mathbb{R}^{r_1+r_2}$ because $\theta_K(\mathcal{O}_K)$ is discrete in Minkowski space.

3. Let A be the fundamental domain of $\mathcal{O}_K$ in Minkowski space. Pick $C > 2^d \operatorname{vol}(A)$. Choose $a_1, \ldots, a_N \in \mathcal{O}_K$ such that every $\alpha \in \mathcal{O}_K$ with $1 \leq |N(\alpha)| \leq C$ satisfies $\alpha = ua_i$ for some $u \in \mathcal{O}_K^*$ and some $i \in \{1, \ldots, N\}$.

4. Write $\theta_K = (f_1, \ldots, f_{r_1}, f_{r_1+1}, \ldots, f_{r_1+r_2})$. Choose $c_1, \ldots, c_{r_1+r_2} \in \mathbb{R}_{>0}$ with $c_1 \cdots c_{r_1+r_2} = C$.

5. Define
$$X = \{ (x_1, \ldots, x_{r_1}, z_{r_1+1}, \ldots, z_{r_1+r_2}) : |x_i| < c_i, |z_i| < c_i \} \subseteq \prod_{i=1}^{r_1} \mathbb{R} \times \prod_{i=1}^{r_2} \mathbb{C}$$
Set
$$T = \bigcup_{i=1}^{N} [\theta_K(a_i)]^{-1} \cdot X$$
(where the reciprocal is taken component-wise).

6. Note that T is bounded. We will show that H is covered by the translates of $\log|T|$ by Γ.
If $\overrightarrow{v} \in H$ then the inverse image of $\log|X| - \overrightarrow{v}$ contains a non-zero vector $\theta_K(\alpha)$ for some $\alpha \in \mathcal{O}_K$ by the convex body theorem. Hence if $\overrightarrow{v} = \log(y)$ then $\theta_K(\alpha) = xy^{-1}$ for some $x \in X$. Then $N(\alpha) < C$ by definition of X and H, so $u\alpha = a_i$ for some i. So $y = x\theta_K(\alpha)^{-1} = x\theta_K(a_i^{-1}u)$; so
$$\underbrace{\overrightarrow{v}}_{\in H} = \underbrace{\log|x\theta_K(a_i^{-1})|}_{\in \log|T|} + \underbrace{\log|\theta_K(u)|}_{\in \Gamma}$$
So H is covered by Γ-translates of $\log|T|$. But $\log|T|$ has finite volume; so there is a fundamental domain of Γ of finite volume, and Γ is a full lattice.

□ Theorem 2.22

Exercise 2.24. Compute $\mathbb{Z}[\sqrt{3}]^*$.

Fact 2.25. *Any finite subgrape of F^* is cyclic if F is a field.*

3 Factorization of primes in extensions

Given an extension L/K of number fields and a non-zero prime ideal P of $\mathcal{O}_K$, how does $P\mathcal{O}_L$ factor into prime ideals of $\mathcal{O}_L$?

Fact 3.1. *If P is a prime ideal of $\mathcal{O}_L$, then $Q = P \cap \mathcal{O}_K$ is prime.*

In this case we say that P *lies over* Q. Now, $Q\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$, though not necessarily prime; we also have that $Q\mathcal{O}_L \subseteq P$. So
$$Q\mathcal{O}_L = P^a \prod_{i=1}^{r} P_i^{a_i}$$
where $P_i \neq P$ for any i.

Definition 3.2. We set
$$e(P/Q) = a$$
$$f(P/Q) = [\mathcal{O}_L/P : \mathcal{O}_K/Q]$$
The former is called the *ramification index of P over Q*, and the latter is called the *inertia degree of P over Q* (or sometimes the *residue degree of P over Q*).

Example 3.3. Let $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$. Let $Q = (2)$ and $P = (1+i)$. From previous work we know that $Q\mathcal{O}_L = P^2$; hence $e(P/Q) = 2$. We also have $f(P/Q) = 1$ because $|\mathcal{O}_L/P| = |\mathcal{O}_K/Q| = 2$.

Remark 3.4. In general we can compute inertia degrees just from the norms of P and Q, since the quotients are always finite.

Example 3.5. Let $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$. Let $Q = (3)$ and $P = (3)$. Then $e(P/Q) = 1$ and $f(P/Q) = [\mathbb{Z}[i]/(3) : \mathbb{Z}/(3)] = 2$.

Example 3.6. Let $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$. Let $Q = (5)$ and $P = (2+i)$ or $(2-i)$. (It doesn't matter which because they are conjugate over K, and hence the ramification indices and inertia degrees are the same.) Then $e(P/Q) = 1$ since $Q\mathcal{O}_L = (2+i)(2-i)$, and $f(P/Q) = [\mathbb{Z}[i]/(2+i) : \mathbb{Z}/5] = 1$ (since $N(2+i) = 5$).

Remark 3.7. Suppose $K \subseteq L \subseteq M$ are number fields; suppose $P \subseteq \mathcal{O}_M$ is prime, and let $Q = P \cap \mathcal{O}_L$ and $R = P \cap \mathcal{O}_K = Q \cap \mathcal{O}_K$. Then

$$e(P/R) = e(P/Q)e(Q/R)$$
$$f(P/R) = f(P/Q)f(Q/R)$$

(This last is because $[\mathcal{O}_M/P : \mathcal{O}_K/R] = [\mathcal{O}_M/P : \mathcal{O}_L/Q][\mathcal{O}_L/Q : \mathcal{O}_K/R]$.)

Theorem 3.8. *Suppose L/K be number fields; suppose $Q \subseteq \mathcal{O}_K$ is a non-zero prime ideal. Factor $Q\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$. Then*

$$\sum_{i=1}^{r} e(P_i/Q)f(P_i/Q) = [L : K]$$

Proof. We check the case $K = \mathbb{Q}$. Note that

$$N(Q\mathcal{O}_L) = \prod_{i=1}^{r} N(P_i)^{e_i}$$

Since $K = \mathbb{Q}$, we have that

$$N(Q\mathcal{O}_L) = |\mathcal{O}_L/Q\mathcal{O}_L|$$

and we may write $Q = (q)$. But by the Chinese remainder theorem we have

$$\mathcal{O}_L/Q\mathcal{O}_L \cong \mathcal{O}_L/P_1^{e_1} \times \cdots \times \mathcal{O}_L/P_r^{e_r}$$

where $e_i = e(P_i/Q)$. Hence

$$\begin{aligned} q^{[L:K]} &= |\mathcal{O}_K/Q|^{[L:K]} \\ &= |\mathcal{O}_L/Q\mathcal{O}_L| \\ &= |\mathcal{O}_L/P_1^{e_1}| \cdots |\mathcal{O}_L/P_r^{e_r}| \\ &= N(P_1)^{e_1} \cdots N(P_r^{e_r}) \\ &= (q^{f(P_1/Q)})^{e(P_1/Q)} \cdots (q^{f(P_r/Q)})^{e(P_r/Q)} \end{aligned}$$

as desired. □ Theorem 3.8

Definition 3.9. Suppose L/K be an extension of number fields; suppose $a \in L$. Consider $T : L \to L$ given by $T_a(x) = ax$; then T_a is a K-linear transformation. We then define

$$\mathrm{tr}_{L/K}(a) = \mathrm{tr}(T_a)$$
$$N_{L/K}(a) = \det(T_a)$$

Remark 3.10.

$$\mathrm{tr}_{L/K}(a) = \sum_{i=1}^{r} f_i(a)$$
$$N_{L/K}(a) = \prod_{i=1}^{r} f_i(a)$$

where $f_1, \ldots, f_r : L \to \overline{K}$ are the embeddings of L into $\overline{K}$. That is, fix an embedding $\varphi : K \hookrightarrow \mathbb{C}$ and let $f_1, \ldots, f_r$ be the embeddings $L \hookrightarrow \mathbb{C}$ such that $f_i \restriction K = \varphi$. Equivalently, regard $\overline{K}$ and L as K-algebras, and let $f_1, \ldots, f_r$ be the K-embeddings (that is, embeddings of K-algebras) $L \hookrightarrow \overline{K}$.

Exercise 3.11. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbb{Q}(\sqrt{2})$. One checks that $\mathcal{O}_L = \mathbb{Z}\left[\sqrt{2}, \frac{\sqrt{2}+\sqrt{6}}{2}\right]$ and that $\operatorname{disc}(\mathcal{O}_L) = 2^8 \cdot 3^2$. Factor (2), (3), and (5) in $\mathcal{O}_L$ and compute all of the ramification indices and inertia degrees that come up.

Example 3.12. Let $K = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Let $a = \sqrt{2} + \sqrt{5}$. Then

$$\begin{aligned} \operatorname{tr}_{L/K}(a) &= (\sqrt{2} + \sqrt{5}) + (\sqrt{2} - \sqrt{5}) \\ &= 2\sqrt{2} \\ N_{L/K}(a) &= (\sqrt{2} + \sqrt{5})(\sqrt{2} - \sqrt{5}) \\ &= -3 \end{aligned}$$

(using Remark 3.10). Alternatively, we can use the definitions: we use the basis $\{1, \sqrt{5}\}$ for L over K. Then

$$\begin{aligned} T_a(1) &= \sqrt{2} + \sqrt{5} \\ &\leftrightarrow (\sqrt{2}, 1) \\ T_a(\sqrt{5}) &= \sqrt{2} \cdot \sqrt{5} + 5 \\ &\leftrightarrow (5, \sqrt{2}) \end{aligned}$$

Hence

$$[T_a] = \begin{pmatrix} \sqrt{2} & 5 \\ 1 & \sqrt{2} \end{pmatrix}$$

and

$$\begin{aligned} \operatorname{tr}_{L/K}(a) &= 2\sqrt{2} \\ N_{L/K}(a) &= -3 \end{aligned}$$

Remark 3.13. Suppose $K \subseteq L \subseteq M$ is a tower of fields. Then

$$\begin{aligned} N_{L/R}(N_{M/L}(a)) &= N_{M/K}(a) \\ \operatorname{tr}_{L/K}(\operatorname{tr}_{M/L}(a)) &= \operatorname{tr}_{M/K}(a) \end{aligned}$$

We also have $N_{L/K}(a), \operatorname{tr}_{L/K}(a) \in K$, and if $a \in \mathcal{O}_L$ then $N_{L/K}(a), \operatorname{tr}_{L/K}(a) \in \mathcal{O}_K$.

Remark 3.14. The converse to the last statement is false; there are a with $N_{L/K}(a), \operatorname{tr}_{L/K}(a) \in \mathcal{O}_K$ but $a \notin \mathcal{O}_L$. (Note that $N_{L/K}(a)$ and $\operatorname{tr}_{L/K}(a)$ are, up to sign, coefficients in (the monic minimal polynomial of a over K raised to the power $[L : K(a)]$).)

We also want to define $N_{L/K}(I)$ for an ideal $I \subseteq \mathcal{O}_L$. Factor

$$I = P_1^{a_1} \cdots P_r^{a_r}$$

for prime ideals $P_i \subseteq \mathcal{O}_L$. Now, if $K = \mathbb{Q}$, then

$$N_{L/K}(I) = (p_1)^{a_1 f(P_i/p_i)} \cdots (p_r)^{a_r f(P_r/p_r)}$$

(where $P_i \cap \mathbb{Z} = (p_i)$).

Definition 3.15. We set

$$N_{L/K}(I) = Q_1^{a_1 f(P_1/Q_1)} \cdots Q_r^{a_r f(P_r/Q_r)}$$

where $Q_i = P_i \cap \mathcal{O}_K$.

Exercise 3.16. (Continuation of Exercise 3.11.) Let $K = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $\mathcal{O}_L = \mathbb{Z}\left[\sqrt{2}, \frac{\sqrt{6}+\sqrt{2}}{2}\right]$ with $\operatorname{disc}(\mathcal{O}_L) = 2^8 \cdot 3^2$. Factor (2), (3), and (5), in $\mathcal{O}_L$, and compute all relevant e and f values that arise. Further compute $N_{L/K}\left(\frac{\sqrt{6}+\sqrt{2}}{2}\right)$ and $\operatorname{tr}_{L/K}\left(\frac{\sqrt{6}+\sqrt{2}}{2}\right)$.

Suppose now that L/K is a Galois extension. Say $P \subseteq \mathcal{O}_K$ is prime; factor $P\mathcal{O}_K = Q_1^{e_1} \cdots Q_g^{e_g}$.

Claim 3.17. *$e_1 = \cdots = e_g$ and $f_1 = \cdots = f_g$.*

Example 3.18. This is not necessarily true if L/K is not Galois. Consider $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$, and $P = (5)$. Then $\mathcal{O}_L$ contains $\mathbb{Z}[\sqrt[3]{2}]$ as a subring of finite index, and $5 \nmid \operatorname{disc}(\mathbb{Z}[\sqrt[3]{2}])$. So $(\mathbb{Z}[\sqrt[3]{5}])_{Q \cap \mathbb{Z}[\sqrt[3]{2}]} = (\mathcal{O}_L)_Q$ and $\mathbb{Z}[\sqrt[3]{2}]/(Q \cap \mathbb{Z}[\sqrt[3]{2}]) \cong \mathcal{O}_L/Q$ for any Q containing 5. Hence we can do our computations in $\mathbb{Z}[\sqrt[3]{5}]$ instead of $\mathcal{O}_K$. Now

$$\begin{aligned}\mathbb{Z}[\sqrt[3]{2}]/(5) &\cong \mathbb{Z}[x]/(x^3 - 2, 5) \\ &\cong (\mathbb{Z}/5\mathbb{Z})[x]/(x^3 - 2) \\ &\cong (\mathbb{Z}/5\mathbb{Z})[x]/(x+2)(x^2 - 2x - 1)\end{aligned}$$

Hence

$$(5) = \underbrace{(\sqrt[3]{2} + 2, 5)}_{f=1}\underbrace{(\sqrt[3]{4} - 2\sqrt[3]{2} - 1, 5)}_{f=2}$$

Proof of Claim 3.17. This follows from the fact that if $Q_i \cap \mathcal{O}_K = Q_j \cap \mathcal{O}_K$ for prime ideals $Q_i, Q_j \subseteq \mathcal{O}_L$, then there is some element $\sigma \in \operatorname{Gal}(L/K)$ satisfying $\sigma(Q_i) = Q_j$; it remains to check this fact.

Fix i; choose $\alpha \in Q_i$ such that $\alpha \equiv 1 \pmod{Q_j}$ for all $j \neq i$. (Possible by the Chinese remainder theorem.) Then $N_{L/K}(\alpha) \in P \subseteq \mathcal{O}_K$. But

$$N_{L/K}(\alpha) = \prod_{\sigma \in \operatorname{Gal}(L/K)} \sigma(\alpha) \in Q_j$$

for all j, because $P \subseteq Q_j$ for all j. Hence for each j there is some σ_j in the Galois grape with $\sigma_j(\alpha) \in Q_j$. But $\sigma_j(\alpha) \equiv 1 \pmod{Q_K}$ for all other k; so $\sigma_j(\alpha) \notin Q_k$ for $k \neq j$. So $\sigma_j(Q_i) = Q_j$. □ Claim 3.17

Given $\sigma \in \operatorname{Gal}(L/K)$, can we "reduce σ modulo P" for some prime ideal $P \subseteq \mathcal{O}_L$?

We cannot!

Example 3.19. Consider $L = \mathbb{Q}(\sqrt{2}$, $K = \mathbb{Q}$, and $P = (7, \sqrt{2} - 3)$. Then

$$\begin{aligned}\mathcal{O}_L/P &\cong \mathbb{Z}[\sqrt{2}]/(7, \sqrt{2} - 3) \\ &\cong \mathbb{Z}[x]/(x^2 - 2, x - 3, 7) \\ &\cong (\mathbb{Z}/7\mathbb{Z})[x]/(x^2 - 2, x - 3) \\ &= (\mathbb{Z}/7\mathbb{Z})[x]/(x - 3) \\ &\cong \mathbb{Z}/7\mathbb{Z}\end{aligned}$$

But if σ is the non-trivial automorphism of L over K, we would be trying to fill in the following diagram:

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \downarrow{\scriptstyle q} & \searrow^{q \circ \sigma} & \downarrow{\scriptstyle q} \\ \mathcal{O}_L/P & \overset{\overline{\sigma}}{\dashrightarrow} & \mathcal{O}_L/P \end{array}$$

The universal property of quotients tells us that $\overline{\sigma} \in \operatorname{Gal}((\mathcal{O}_L/P)/(\mathcal{O}_K/P \cap K))$ exists exactly when $P \subseteq \ker(q \circ \sigma) = \sigma^{-1}(P)$; i.e. when $P = \sigma(P)$.

Definition 3.20. For fixed P, we have that $D_P = \{\, \sigma \in \operatorname{Gal}(L/K) : \sigma(P) = P \,\}$ is a subgrape of $\operatorname{Gal}(L/K)$, called the *decomposition grape of P*. We then get a homomorphism $\varphi_P \colon D_P \to \operatorname{Gal}((\mathcal{O}_L/P)/(\mathcal{O}_K/P \cap K))$, called the *decomposition homomorphism*. This homomorphism need not be injective; we thus define the *inertia grape of P* to be

$$I_P = \ker(\varphi_P) = \{\, \sigma \in D_P : \sigma = 1 \text{ in } \operatorname{Gal}((\mathcal{O}_L/P)/(\mathcal{O}_K/P \cap K)) \,\}$$

Exercise 3.21. As in Exercise 3.16, we let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so $\mathcal{O}_L = \mathbb{Z}\left[\sqrt{2}, \frac{\sqrt{6}+\sqrt{2}}{2}\right]$, and we let $K = \mathbb{Q}$ so that $\mathcal{O}_K = \mathbb{Z}$. We saw that

$$P_2 = \left(\frac{\sqrt{6}+\sqrt{2}}{2} + 1, \sqrt{2}\right)$$
$$P_3 = \left(\frac{\sqrt{6}+\sqrt{2}}{2} + \sqrt{2}, 3\right)$$
$$P_5 = \left(\frac{\sqrt{6}+\sqrt{2}}{2} - 3\sqrt{2} + 3, 5\right)$$

were prime. Find D_P and I_P for all of these ideals.

Definition 3.22. Suppose L/K is an extension of number fields; suppose $I \subseteq \mathcal{O}_L$ is an ideal. The *codifferent of* I is

$$I^* = \{\, x \in L : \mathrm{tr}_{L/K}(xI) \subseteq \mathcal{O}_K \,\}$$

This turns out to be a fractional ideal of $\mathcal{O}_L$. The *codifferent of* L/K is the codifferent of $\mathcal{O}_L$ over K. The *different of* I is $(I^*)^{-1}$; the *different of* L/K is $\mathcal{D}_{L/K} = (\mathcal{O}_L^*)^{-1}$.

Example 3.23. We compute the codifferent of (1) in $\mathbb{Z}[\sqrt{2}]$ over $\mathbb{Q}$; i.e. the codifferent of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Note that $\mathrm{tr}(a+b\sqrt{2}) = 2a$; we thus require that $2a \in \mathbb{Z}$. Further note that $\mathrm{tr}((a+b\sqrt{2})\sqrt{2}) = \mathrm{tr}(2b+a\sqrt{2}) = 4b$; we thus require that $4b \in \mathbb{Z}$. Hence

$$(1)^* = \left\{ \frac{k}{2} + \frac{\ell\sqrt{2}}{4} : k, \ell \in \mathbb{Z} \right\} = \left(\frac{\sqrt{2}}{4}\right)$$

We thus also get that the different is $\mathcal{D}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} = (I^*)^{-1} = (2\sqrt{2})$.

Fact 3.24. *$II^* = \mathcal{O}_L^*$.*

Proof. It is easily seen that $II^* \subseteq \mathcal{O}_L^*$; hence

$$I^* \subseteq I^{-1}\mathcal{O}_L^* \subseteq I^*$$

and $I^{-1}\mathcal{O}_L^* = I^*$. □ Fact 3.24

Fact 3.25. *If $I \subseteq \mathcal{O}_L$ then $(I^*)^{-1} \subseteq \mathcal{O}_L$.*

Proof. This is just because if $I \subseteq J$ then $J^* \subseteq I^*$. □ Fact 3.25

Example 3.26. Compute the different of $L = \mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$. Well, $\mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. We want $\mathrm{tr}(a+b\sqrt{5}) = 2a \in \mathbb{Z}$ and $\mathrm{tr}\left((a+b\sqrt{5})\left(\frac{1+\sqrt{5}}{2}\right)\right) = a + 5b \in \mathbb{Z}$ for $a, b \in \mathbb{Q}$. We thus get that $a + b\sqrt{5} = \frac{\ell}{2} + \frac{1}{5}\left(m - \frac{\ell}{2}\right)\sqrt{5}$. Hence

$$\mathcal{O}_L^* = \left\{ \ell\left(\frac{5-\sqrt{5}}{10}\right) + m\left(\frac{\sqrt{5}}{5}\right) : \ell, m \in \mathbb{Z} \right\} = \left(\frac{5-\sqrt{5}}{10}, \frac{\sqrt{5}}{5}\right) = \left(\frac{\sqrt{5}}{5}\right)$$

(since $\frac{5-\sqrt{5}}{10} = \frac{\sqrt{5}}{5}\left(\frac{-1+\sqrt{5}}{2}\right)$). Hence $\mathcal{D}_{L/K} = (\sqrt{5})$.

Fact 3.27. *$\mathcal{D}_{M/K} = \mathcal{D}_{M/L}\mathcal{D}_{L/K}$. Also, if L/K is Galois, then for all $\sigma \in \mathrm{Gal}(L/K)$ we have $\sigma(\mathcal{D}_{L/K}) = \mathcal{D}_{L/K}$.*

Definition 3.28. The *discriminant of* L/K is $\Delta_{L/K} = N_{L/K}(\mathcal{D}_{L/K})$.

Theorem 3.29. $(\mathrm{disc}(\mathcal{O}_K)) = \Delta_{K/Q}$.

Proof. We will show that $\operatorname{disc}(\mathcal{O}_K)^2$ generates $\Delta_{K/Q}^2$. For any ideal $I \subseteq \mathcal{O}_K$, we have that $I = a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}$ for some $a_1, \ldots, a_n \in \mathcal{O}_K$. The ideal I^* is $a_1^*\mathbb{Z} + \cdots + a_n\mathbb{Z}^*$ where $a_i^* \in K$ is given by $\operatorname{tr}(a_i a_j^* = \delta_{ij}$. So $\mathcal{O}_K^*$ (the codifferent of $\mathcal{O}_K$) is $a_1\mathbb{Z}^* + \cdots + a_n^*\mathbb{Z}$ where $\mathcal{O}_K = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$. But $\mathcal{O}_K^*$ is a fractional ideal of $\mathcal{O}_K$; so there is some non-zero $m \in \mathbb{Z}$ with $m\mathcal{O}_K^* \subseteq \mathcal{O}_K$. Define $I = m\mathcal{O}_K^*$; then

$$N_{K/\mathbb{Q}}(\mathcal{D}_{K/\mathbb{Q}})^2 = \frac{1}{N_{K/\mathbb{Q}}(\mathcal{O}_K^*)^2} = \frac{m^{2n}}{N_{K/\mathbb{Q}}(I)^2} = \frac{m^{2n}\Delta_K}{\operatorname{disc}(ma_1^*, \ldots, ma_n^*)} = \frac{\Delta_K}{\operatorname{disc}(a_1^*, \ldots, a_n^*)}$$

(since $\mathcal{O}_K^{*-1} = \mathcal{D}_{K/\mathbb{Q}}$). (Here we regard $N_{K/\mathbb{Q}}(\mathcal{D}_{K/\mathbb{Q}})$ as an integer by identifying it with a generator of this ideal.) (Here Δ_K refers to $\operatorname{disc}(K) = \operatorname{disc}(a_1, \ldots, a_n)$.)

Claim 3.30. $\operatorname{disc}(a_1^*, \ldots, a_n^*) = \frac{1}{\operatorname{disc}(a_1, \ldots, a_n)}$.

Proof. We note that

$$\operatorname{disc}(a_1, \ldots, a_n) = \det \begin{pmatrix} f_1(a_1) & \cdots & f_n(a_1) \\ \vdots & \ddots & \vdots \\ f_1(a_n) & \cdots & f_n(a_n) \end{pmatrix}^2$$

$$\operatorname{disc}(a_1^*, \ldots, a_n^*) = \det \begin{pmatrix} f_1(a_1^*) & \cdots & f_1(a_n^*) \\ \vdots & \ddots & \vdots \\ f_n(a_1^*) & \cdots & f_n(a_n^*) \end{pmatrix}^2$$

But the (i, j) entry of the product of these two matrices is

$$f_1(a_i)f_1(a_j^*) + \cdots + f_n(a_i)f_n(a_j^*) = \operatorname{tr}_{K/\mathbb{Q}}(a_i a_j^*) = \delta_{ij}$$

Hence $\operatorname{disc}(a_1^*, \ldots, a_n^*) = \frac{1}{\operatorname{disc}(a_1, \ldots, a_n)}$. □ Claim 3.30

□ Theorem 3.29

Fact 3.31. $\Delta_{M/K} = \Delta_{L/K}^{[M:L]} N_{L/K}(\Delta_{M/L})$.

Some hard facts:

Fact 3.32.

1. *Say $P \subseteq \mathcal{O}_L$ is prime; let $Q = P \cap \mathcal{O}_K$ and $e = e(P/Q)$. Then $P^{e-1} \mid \mathcal{D}_{L/K}$ and if $\gcd(e, N_{L/\mathbb{Q}}(P)) = 1$ then $P^e \nmid \mathcal{D}_{L/K}$.*
2. *Suppose $n \in \mathbb{Z}$; suppose $\mathcal{S}$ is a finite set of prime ideals of $\mathcal{O}_K$. Then the set of extensions L/K with $[L : K] \leq n$ and L ramified only over primes in $\mathcal{S}$ is finite.*
3. *(Due to Hermite.) Suppose $n \in \mathbb{Z}$. Then there are finitely many number fields with discriminant at most n.*

Example 3.33. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ so that $\mathcal{O}_L = \mathbb{Z}\left[\sqrt{2}, \frac{\sqrt{6}+\sqrt{2}}{2}\right]$; let $K = \mathbb{Q}(\sqrt{2})$ so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. Compute $\Delta_{L/K}$.

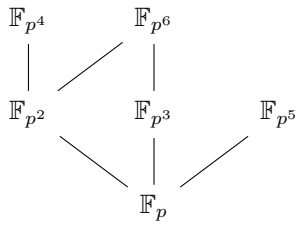
Steps:

1. Compute $\mathcal{O}_L^*$ (codifferent, not grape of units) over K.
2. Invert it to get $\mathcal{D}_{L/K}$.
3. Compute $N_{L/K}(\mathcal{D}_{L/K}) = \Delta_{L/K}$.

4 Interlude—Finite fields

Suppose we have a field extension K of $\mathbb{F}_p$ with p^d elements; so $[K : \mathbb{F}_p] = d$. Then K^* has $p^d - 1$ elements and is a grape; so K is the splitting field of $x^{p^d} - 1$. One checks that it is also a separable extension; hence every extension of finite fields is Galois. But splitting fields are unique up to isomorphism; hence up to isomorphism there is exactly one field with p^d elements.

How do they relate? In partial diagram:



In general, the lattice of finite fields of characteristic p is isomorphic to the lattice of positive integers under the divisibility relation.

What of the Galois theory? What is $\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$? There is a natural automorphism $\mathrm{Frob}_p \colon \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ given by $\mathrm{Frob}_p(\alpha) = \alpha^p$. By Fermat's little theorem we get that Frob_p fixes $\mathbb{F}_p$ pointwise. Is it true that $\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$?

Well, $|\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)| = k$. What is $|\langle \mathrm{Frob}_p \rangle|$? Well, $(\mathrm{Frob}_p)^n(\alpha) = \alpha^{p^n}$; so $(\mathrm{Frob}_p)^n$ is trivial if and only if $\alpha = \alpha^{p^n}$ for all $\alpha \in \mathbb{F}_{p^k}$. But $\mathbb{F}_{p^k}$ is the splitting field of $x^{p^k} - x$; so the order of Frob_p divides k. Can it be smaller? Well, any α fixed by $(\mathrm{Frob}_p)^n$ satisfies $x^{p^n} - x = 0$, and there are no more than p^n such α; hence the order of Frob_p is k.

So $\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$. So $\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$ is cyclic; thus $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ is also cyclic, and is generated by $(\mathrm{Frob}_p)^m$.

Exercise 4.1. Let $a \in \mathbb{F}_{5^3} = \mathbb{F}_5(a)$ be a root of $x^3 + 3x + 7$. Express the other two roots as $x + ya + za^2$ for some $x, y, z \in \mathbb{F}_5$.

5 Slightly less finite fields

Suppose now we have a Galois extension of number fields $L \supseteq K$; suppose we have $P \subseteq \mathcal{O}_L$ lying over $Q \subseteq \mathcal{O}_K$. Recall that

$$D_P = \{\, \sigma \in \mathrm{Gal}(L/K) : \sigma(P) = P \,\}$$
$$I_P = \{\, \sigma \in D_P : \sigma \equiv \mathrm{id} \pmod{P} \,\}$$

Definition 5.1. Suppose L/K be a Galois extension of number fields; suppose $P \subseteq \mathcal{O}_L$ is a prime ideal lying over $Q \subseteq \mathcal{O}_K$. The *decomposition field of P over K*, denoted Z_P is the fixed field of D_P. The *inertia field of P over K*, denoted F_P, is the fixed field of I_P. (This notation is not standard.)

Remark 5.2. If P_1 and P_2 both lie over Q, then D_{P_1} and D_{P_2} are conjugate; so Z_{P_1} and Z_{P_2} are isomorphic.

Theorem 5.3. *Suppose L/K is a Galois extension of number fields; suppose $P \subseteq \mathcal{O}_L$ is prime and $Q = P \cap \mathcal{O}_K$. Let $Z = Z_P$ be the decomposition field of P; let $P = P \cap \mathcal{O}_Z$. Then*

1. *P is the only prime ideal of $\mathcal{O}_L$ that lies over P_Z.*
2. *$[L : Z] = |D_P| = e(P/Q)f(P/Q)$.*
3. *$e(P_Z/Q) = f(P_Z/Q)$.*

Proof.

1. Well, $\mathrm{Gal}(L/Z) = D_P$; so $\mathrm{Gal}(L/Z)$ fixes P. But $\mathrm{Gal}(L/Z)$ acts transitively on the primes lying over P_Z (see the proof of Claim 3.17).

2. Well,
$$[L : K] = e(P/Q)f(P/Q)(\text{index of } D_P \text{ in } \mathrm{Gal}(L/K)) = \frac{e(P/Q)f(P/Q)[L : K]}{|D_P|}$$
Hence $|D_P| = e(P/Q)f(P/Q)$.

3. Well, $[L : Z] = e(P/P_Z)f(P/P_Z)$; so $[L : K] = e(P/P_Z)f(P/P_Z)[Z : K]$. But $[L : K] = e(P/Q)f(P/Q)[Z : K]$; so $e(P/P_Z)f(P/P_Z) = e(P/Q)f(P/Q)$. So $e(P_Z/Q) = f(P_Z/Q) = 1$. □ Theorem 5.3