Contents

Part I

Linear Algebra

Part II

Field Theory

Chapter 1

Algebraic Field Extensions

Definition 1 (Splitting Field)**.** A splitting field of a polynomial f over a field K is a field extension L of K over which f factors into linear factors that is

$$f(X) = c \prod_{i=1}^{\deg f} (X - a_i)$$

where $c \in K$ and for each $1 \leq i \leq \deg f$ we have $X - a_i \in L[X]$ with a_i not necessarily distinct and such that the roots a_i generate L over K.

Remark. The extension L is an extension of minimal degree over K in which f splits. Such extension always exist and is unique up to isomorphism. The amount of freedom in that isomorphism is known as the Galois group of f (if we assume it is separable).

Definition 2 (Normal Extension)**.** A algebraic extension L over a field K is normal if one of the following equivalent conditions are met.

1. I don't quite see this.
2. L is a splitting field of a family of polynomials of $K[X]$.
3. Every irreducible polynomials of $K[X]$ that has a root in L factors into linear factors over L.

Chapter 2

Galois Theory

Example 2.1. Let

Proof. The field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is Galois of degree 4. This means that the Galois group is of order 4. The minimal polynomial of $\sqrt{2}$ is $X^2 - 2$, so the conjugate of $\sqrt{2}$ is $-\sqrt{2}$. Similary, the conjugate of $\sqrt{3}$ is $-\sqrt{3}$. □

Part III

Algebraic Number Theory

Theorem 3. Let A be an integral domain, and let L be a field containing A. The elements of L integral over A form a ring.

Remark. The immediate consequence of this theorem is that the ring of integers is indeed a ring.

Definition 4. Symmetric polynomials and elementary symmetric polynomials.

Theorem 5. Let A be a ring. Every symmetric polynomial $P(X_1, \ldots, X_r)$ in $A[X_1, \ldots, X_n]$ can be represented with a linear combination of elementary symmetric polynomials with coeffcients in A.

Proof is constructive and inductive by reducing the polynomial over the lexicographically highest monomial. Not a hard proof, but the indecies are anoying.

The above proof implies:

Let $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$, and let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(X)$ in some ring containing A, so that $f(X) = \prod(X - \alpha_i)$ in the larger ring. Then

$$a_1 = -S_1(\alpha_1, \ldots, \alpha_n), \qquad a_2 = S_2(\alpha_1, \ldots, \alpha_n), \qquad a_n = \pm S_n(\alpha_1, \ldots, \alpha_n).$$

(I'm not quite sure why this is the case. Maybe use the multi-binomial theorem.)

Thus the elementary symmetric polynomials in the roots of f lie in A. And so the theorem implies that every symmetric polynomial in the roots of $f(X)$ lies in A.

Proposition 6. Let A be a integral domain and Ω be an algebraically closed field containing A. If $\alpha_1, \ldots, \alpha_n$ are the roots in Ω of a monic polynomial in $A[X]$, then every polynomial $g(\alpha_1, \ldots, \alpha_n)$ in $A[\alpha_1, \ldots, \alpha_n]$ is a root of a monic polynomial in $A[X]$.

Proof. Clearly,

$$h(X) := \prod_{\sigma \in \mathrm{Sym}_n} (X - g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}))$$

is a monic polynomial whose coeffcients are symmetric polynomials in the α_i, and therefore lie in A. But $g(\alpha_1, \ldots, \alpha_n)$ is one of the roots. □

With this we can prove that the above theorem. I don't quite understand few steps ...

Dedekind's Proof

Proposition 7. Let L be a field containing A. An element α of L is integral over A if and only if there exists a nonzero finitely generated A-submodule of L such that $\alpha M \subset M$ (in fact, we can take $M = A[\alpha]$, the A-subalgebra generated by α).

Proof.

- Let $\alpha \in L$ be integral over A. The A-submodule $A[\alpha]$ in L is generated by $1, \alpha, \ldots, \alpha^{n-1}$, thus finitely generated and clearly nonzero. $\alpha A[\alpha] \subset A[\alpha]$ also holds.
- Let M be a nonzero, finitely generated A-submodule in L such that $\alpha M \subset M$. Since M is finitely generated, there is a set of generators $v_1, \ldots, v_n \in M$. From $\alpha M \subset M$ we have that

$$\alpha v_i = \sum_{j=1}^{n} a_{i,j} v_j$$

for some $a_{i,j} \in A$. We rewrite this system of equations

$$(\alpha - a_{i,i})v_i \sum_{j=1, j\neq i}^{n} a_{i,j}v_j = 0$$

We have the matrix

$$\begin{pmatrix} (\alpha - a_{1,1}) & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & (\alpha - a_{2,2}) & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{n,1} & a_{n,2} & \cdots & (\alpha - a_{n,n}) \end{pmatrix}$$

Applying Cramer's Rule we get $v_i = \frac{\det(C_i)}{\det C}$, but C_i is always 0, and at least one v_i is nonzero, so we have that $\det(C) = 0$.

But calculating the determinant of C gives us

$$\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$$

as desired.

□

Now take α and β integral over A and denote $\alpha M \subset M$ and $\beta N \subset N$.

1. MN is an A-submodule of L.

Dedekind's proof is much easier to understand, lol.

Integral Elements

Proposition 8. Let K be the field of fractions of A, and let L be a field containing K. If $\alpha \in L$ is algebraic over K, then there exists a nonzero $d \in A$ such that $d\alpha$ is integral over A.

Corollary 1. Let A be an integral domain with field of fractions K, and let B be the integral closure of A in a field L containing K. If L is algebraic over K, then it is the field of fractions B.

Example 8.1. Let d be a square-free integer. Consider $A = \mathbb{Z}[\sqrt{d}]$. Show that every element of R can be written as a product of irreducible elements.

Proof. Define $N : R \longrightarrow \mathbb{N}$ as $N(a+b\sqrt{d}) = |a^2 - db^2|$ where $a, b \in \mathbb{Z}$. Let $a_1 + b_1\sqrt{d}$ and $a_2 + b_2\sqrt{d}$ be two elements in $\mathbb{Z}[\sqrt{d}]$ with $a_1, b_1, a_2, b_2 \in \mathbb{Z}$, then

$$\begin{aligned} N((a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})) &= N((a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}) \\ &= |(a_1a_2 + b_1b_2d)^2 - d(a_1b_2 + a_2b_1)^2| \\ &= |a_1^2a_2^2 + 2a_1a_2b_1b_2d + b_1^2b_2^2d^2 - a_1^2b_2^2d - 2a_1a_2b_1b_2d - a_2^2b_1^2d| \\ &= |a_1^2a_2^2 - a_1^2b_2^2d - a_2^2b_1^2d + b_1^2b_2^2d^2| \end{aligned}$$

on the other hand

$$\begin{aligned} N(a_1 + b_1\sqrt{d})N(a_2 + b_2\sqrt{d}) &= |a_1^2 - db_1^2||a_2^2 - db_2^2| \\ &= |a_1^2a_2^2 - a_1^2b_2^2d - a_2^2b_1^2d + b_1^2b^2d^2| \end{aligned}$$

so we have $N((a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})) = N(a_1 + b_1\sqrt{d})N(a_2 + b_2\sqrt{d})$. Moreover, let $u \in \mathbb{Z}[\sqrt{d}]$ be a unit, then there is an element $v \in \mathbb{Z}[\sqrt{d}]$ such that $uv = 1$. Applying the function defined above, we get

$$1 = N(1) = N(uv) = N(u)N(v)$$

so $N(u) = 1$. Now suppose $N(a + b\sqrt{d}) = 1$ with $a, b \in \mathbb{Z}$. Consider

$$(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 = \pm 1$$

and therefore $a + b\sqrt{d}$ is a unit.

We have shown that N is a norm map. R is also an integral domain because if $x \in R$ is a zero-divisor, then we have $0 = N(x) = |a^2 - db^2|$, but this is impossible since d is square-free. Applying the example before, we get the desired result. □

Example 8.2. 2.1.3. did it before

Example 8.3. Let R be a domain in which every element can be written as a product of irreducibles. Show that the following are equivalent.

1. this factorization is unique
2. if π is irreducible and π divides ab, then $\pi|a$ or $\pi|b$

Proof. Let the factorization be unique, $\pi \in R$ be irreducible and divide ab. Then $ab = \pi x$ for some $x \in R$. On the other hand, ab has a unique factorization that is the product of the factorization of a and b but must contain π.

For the other side let $p_1^{r_1} \cdot \ldots \cdot p_n^{r_n}$ and $q_1^{s_1} \cdot \ldots \cdot q_m^{r_m}$ be two factorizations of an element in R. Then p_1 divides $q_1^{s_1} \cdot \ldots \cdot q_m^{r_m}$ so p_1 divides some q_i. But q_i is irreducible, so we have $p_1 = q_i$. Induction yields the desired result. □

Example 8.4. Show that if π is an irreducible element of a principal ideal domain, then (π) is a maximal ideal.

Proof. Assume (π) is not maximal, then there is an ideal (a) with $a \neq 1$ such that $(\pi) \subsetneq (a)$. But this implies $\pi = ra$ for some $r \in R$ that is not a unit. This is a contradiction. □

Example 8.5. If F is a field, prove that $F[x]$ is Euclidean.

Proof. Define $\phi : F[x] \longrightarrow \mathbb{N}$ as $\phi(f) = \deg(f)$. Fix two polynomials $f, g \in F[x]$. If $\deg(f) >= \mathrm{g}$, then we can do polynomial division to get $f = gp + r$ where $\deg(g) > \mathrm{r}$. □

Example 8.6. Show that $\mathbb{Z}[i]$ is Euclidean.

Proof. Fix two elements $x, y \in \mathbb{Z}[i]$ and write $x = a_x + ib_x$ and $y = a_y + ib_y$. It is

$$\frac{x}{y} = \underbrace{\frac{a_x a_y + b_x b_y}{a_y^2 + b_y^2}}_{=:\alpha} + i \underbrace{\frac{a_y b_x - a_x b_y}{a_y^2 + b_y^2}}_{=:\beta}$$

Set p_x to be the closest integer to α and p_y to be the closest integer to β and $p = p_x + ip_y$. Moreover, set $r = ((\alpha - p_x) + i(\beta - p_y))y$.

It is

$$\begin{aligned} r &= y(\alpha + i\beta) - y(p_x + ip_y) \\ &= y\frac{x}{y} - py \\ &= x - py \end{aligned}$$

so we got the desired representation.

Furthermore, we have

$$\begin{aligned} N(r) &= N(y)((\alpha - p_x)^2 + (\beta - p_y)^2) \\ &\leq N(y)\frac{1}{2} \end{aligned}$$

□

Example 8.7. Prove that if p is a positive prime, then there is an element $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 \equiv -1 \mod p$ if and only if either $p = 2$ or $p \equiv 1 \mod 4$.

Proof. 1. Let $p = 2$, then we can simply choose $x = 1$. Now let $p \equiv 1 \mod 4$. With Wilson's Theorem we have

$$-1 \equiv (p-1)! \equiv 1 \cdot \ldots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot p \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \cdot (-1)^{\frac{p-1}{2}} \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2$$

where $\mod p$. So choose the last expression as x and we are done.

2. If $p = 2$, then we are done. Now let $x^2 \equiv -1 \mod p$. If $p \equiv 3 \mod (4)$, we have

$$x^{p-1} = x^{4n+2} = x^{4n}x^2 \equiv -1(x^4)^n \equiv -1 \mod p$$

as $x^4 \equiv 1 \mod p$. But this contradicts Fermat's Little Theorem.

□

Example 8.8. Find all integer solutions to $y^2 + 1 = x^3$ with $x, y \neq 0$.

Proof. If x is even, then $4|x^3$, so $x^3 - 1 \equiv 3 \mod 4$ which cannot be a square since all squares are congruent to either 0 or 1 $\mod 4$. So x is odd and y is even. Write $y^2 + 1 = (y + i)(y - i)$. If a prime divides $(y + i)(y - i)$, then the prime divides also their difference $2i$. So $p = 2$ up to units. But then p divides y as y was even, but this is impossible since p also divides $y + i$. □

Example 8.9. What are the primes of $\mathbb{Z}[i]$?

Proof. We have two types of primes in $\mathbb{Z}[i]$.

1. p and ip where $p \equiv 3 \mod 4$.
2. $a + ib$ with $a^2 + b^2 \equiv 1 \mod 4$ and prime.

This is because of the norm function $N(a + ib) = a^2 + b^2$. □

Example 8.10. A positive integer a is the sum of two squares if and only if $a = b^2c$ where c is not divisible by any positive prime $p \equiv 3 \mod 4$.

Proof. I don't know. □

Example 8.11. $\mathbb{Z}[\rho]$ is a ring where

$$\rho = \frac{-1 + \sqrt{-3}}{2}.$$

Proof. 1. $(\mathbb{Z}[\rho], +)$ is an abelian group.

(a) If $a_1 + b_1\rho$ and $a_2 + b_2\rho$ are elements of $\mathbb{Z}[\rho]$, then $a_1 + b_1\rho + a_2 + b_2\rho = a_1 + a_2 + (b_1 + b_2)\rho$, so the addition is well-defined.

(b) Associativity and commutativity is inhereted from the addition of integers.

(c) The additive identity is 0.

(d) If $a + b\rho$ is in $\mathbb{Z}[\rho]$, then its inverse is $-a - b\rho$.

2. $(\mathbb{Z}[\rho], \cdot)$ is a monoid.

(a) If $a_1 + b_1\rho$ and $a_2 + b_2\rho$ are two elements of $\mathbb{Z}[\rho]$, then we have

$$\begin{aligned}
(a_1 + b_1\rho)(a_2 + b_2\rho) &= a_1a_2 + b_1b_2\rho^2 + (a_1b_2 + a_2b_1)\rho \\
&= a_1a_2 + b_1b_2\overline{\rho} + (a_1b_2 + a_2b_1)\rho \\
&= a_1a_2 + b_1b_2\frac{-1 - \sqrt{3}}{2} + (a_1b_2 + a_2b_1)\frac{-1 + \sqrt{3}}{2} \\
&= a_1a_2 - \frac{b_1b_2}{2} - \frac{a_1b_2 + a_2b_1}{2} - \frac{b_1b_2\sqrt{-3}}{2} + \frac{(a_1b_2 + a_2b_1)\sqrt{-3}}{2} \\
&= a_1a_2 + \frac{-a_1b_2 - a_2b_2 - b_1b_2}{2} + \frac{(a_1b_2 + a_2b_1 - b_1b_2)\sqrt{-3}}{2}
\end{aligned}$$

I made some mistake, but should be right.

(b) The multiplicative identity is 1

3. Distributive law is again inherited.

□

Example 8.12. 1. Show that $\mathbb{Z}[\rho]$ is Euclidean.

Proof. Fix two elements $x_1 + x_2\rho$ and $y_1 + y_2\rho$ of $\mathbb{Z}[\rho]$. We have

$$\begin{aligned}\frac{x_1 + x_2\rho}{y_1 + y_2\rho} &= \frac{x_1 + x_2\rho}{y_1 + y_2\rho}\frac{y_1 - y_2\rho}{y_1 - y_2\rho} \\ &= \frac{x_1y_1 - x_2y_2\overline{\rho} - x_1y_2\rho + x_2y_1\rho}{y_1^2 + y_2^2\overline{\rho}}\end{aligned}$$

I think this should work at the end of the day, but I'm too lazy to write it out. □

2. Show that the only units in $\mathbb{Z}[\rho]$ are ± 1, $\pm\rho$, and $\pm\overline{\rho}$.

Chapter 3

Cheet Sheet

$K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer.

1. $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where

$$\alpha := \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \\ \sqrt{d} & d \equiv 2, 3 \mod 4 \end{cases}$$

Chapter 4

Algebraic Numbers and Integers

Example 8.13. Show that

$$\alpha := \frac{\sqrt{2}}{3}$$

is an algebraic number, but not an algebraic integer.

Proof. First of all, α is the root of

$$X^2 - \frac{2}{9} \in \mathbb{Q}[X],$$

so it is an algebraic number.

Now assume α is an algebraic integer. Then, there is a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. It is

$$f(\alpha) = \left(\frac{\sqrt{2}}{3}\right)^n + a_{n-1}\left(\frac{\sqrt{2}}{3}\right)^{n-1} + \cdots + a_1\frac{\sqrt{2}}{3} + a_0 = 0$$
$$(\sqrt{2})^n + 3a_{n-1}(\sqrt{2})^{n-1} + \cdots + 3^{n-1}a_1\sqrt{2} + 3^n a_0 = 0$$

If n is odd, then $\sqrt{2}$ is not an integer, therefore, we can separate the sum into two smaller ones.

$$\sum_{k \text{ even}} 3^{n-k}a_k(\sqrt{2})^k = 0$$

and

$$\sum_{k \text{ odd}} 3^{n-k}a_k(\sqrt{2})^k = \sqrt{2}\sum_{k \text{ even}} 3^{n-k}a_k(\sqrt{2})^{\frac{k-1}{2}} = 0.$$

Both sums are divisible by 3 as 3 divides 0 and since all summands except for the very last one contains multiples of 3, they are divisible by 3, so the last summand must be divisible by 3 as well. But this cannot be. Hence α is not an algebraic integer. □

Example 8.14. Show that if $r \in \mathbb{Q}$ is an algebraic integer, then $r \in \mathbb{Z}$.

Proof. Write $r = \frac{p}{q}$ such that $q \nmid p$ and we have

$$p^n + qa_{n-1}p^{n-1} + \cdots + q^n a_0 = 0$$

q divides the whole sum, it divides all summands, but it does not divide p^n, therefore $q = 1$. □

Chapter 5

3

Example 8.15. Let K be an algebraic number field. If $\alpha \in K$, then there is a nonzero integer $m \in \mathbb{Z}$ such that $m\alpha \in \mathcal{O}_K$.

Proof. Since α is an algebraic number, we have

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

with $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. So choose $m \in \mathbb{Z}$ such that $m\alpha_i$ is an integer for all i. We have

$$m^n\alpha^n + m^n a_{n-1}\alpha^{n-1} + \cdots + m^n a_1\alpha + m^n a_0 = 0$$
$$(m\alpha)^n + m a_{n-1}(m\alpha)^{n-1} + \cdots + m^{n-1} a_1(m\alpha) + m^n a_0 = 0$$

so $m\alpha \in \mathcal{O}_K$. □

Chapter 6

Integral Bases

6.1 Overview

6.2 Details

Errors

1. Pretty sure that in the example 9.1. the sign of characteristic polynomial is swapped. We want the definition of characteristic polynomial to be in such a way that it only creates monic polynomials.
2. Proof of proposition 10 is wrong. The characteristic polynomial is not the same as the minimal polynomial see:

   https://feog.github.io/antchap1.pdf
3. Proof of prop 10 is missing
4. Proof of Lemma 11 is wrong because of the stuff above.
5. Second proof of lemma 11 is not complete.

6.2.1 Trace, Norm, and Characteristic Polynomial

Definition 9 (Trace, Norm, and Characteristic Polynomial)**.** Let K be an algebraic number field with degree n. Then, K can be viewed as an finite-dimensional vector space over $\mathbb{Q}$. If $\alpha \in K$, we can define a linear operator

$$\Phi_\alpha : K \longrightarrow K, \qquad v \mapsto \alpha v,$$

which may be represented by $n \times n$ matrix $A_\Phi = (a_{i,j})_{1 \le i,j \le n}$ by requiring

$$\alpha e_i = \sum_{j=1}^{n} a_{i,j} e_j, \qquad a_{i,j} \in \mathbb{Q}.$$

We define trace of α by $\mathrm{Tr}_K(\alpha) := \mathrm{Tr}(\Phi_\alpha)$, the norm of α by $N(\alpha) := \det(\Phi_\alpha)$ and the characteristic polynomial of α by $\chi_K(X) := \det(XI - \Phi_\alpha)$. If

Example 9.1. In this example, we will compute the traces, norms and characteristic polynomials of some elements in concrete algebraic number fields.

1. Let $K = \mathbb{Q}(i)$. If $\alpha = a + ib$ with $a, b \in \mathbb{Q}$, then the trace of α is $\mathrm{Tr}_K(\alpha) = 2a$, the norm of α is $\mathrm{N}_K(\alpha) = a^2 + b^2$, and the characteristic polynomial of α is $\chi_\alpha(X) = X^2 - 2aX + a^2 + b^2$.

Proof. A basis of K is $\{1, i\}$. Then Φ_α is defined by

$$1 + 0 \cdot i \mapsto \alpha = a + ib$$
$$0 + 1 \cdot i \mapsto \alpha i = -b + ia$$

and we may represent Φ by a 2×2 matrix

$$A_\Phi = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Therefore, $\mathrm{Tr}_K(\alpha) = 2a$, $\mathrm{N}_K(\alpha) = a^2 + b^2$, and $\chi_\alpha(X) = X^2 - 2aX + a^2 + b^2$. □

2. Let $K = \mathbb{Q}(\sqrt{2})$. If $\alpha = a + \sqrt{2}b$ with $a, b \in \mathbb{Q}$, then the trace of α is $\mathrm{Tr}_K(\alpha) = 2a$, the norm of α is $\mathrm{N}_K(\alpha) = a^2 - 2b^2$, and the characteristic polynomial of α is $\chi_\alpha = X^2 - 2aX + a^2 - 2b^2$.

Proof. A basis of K is $\{1, \sqrt{2}\}$. Define Φ_α by

$$1 + 0 \cdot \sqrt{2} \mapsto \alpha = a + \sqrt{2}b$$
$$0 + 1 \cdot \sqrt{2} \mapsto \sqrt{2}\alpha = 2b + \sqrt{2}a$$

then the matrix belonging to Φ_α is

$$A_\Phi = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}.$$

So we have $\mathrm{Tr}_K(\alpha) = 2a$, $\mathrm{N}_K(\alpha) = a^2 - 2b^2$, and $\chi_\alpha = X^2 - 2aX + a^2 - 2b^2$. □

3. Let $K = \mathbb{Q}(\sqrt{5})$. If $\alpha = a + \sqrt{5}b$, then $\mathrm{Tr}_K(\alpha) = 2a$ and $\mathrm{N}_K(\alpha) = a^2 - 5b^2$.

Proof. A basis[1] of K is $\{1, \sqrt{5}\}$. As before, the linear operator Φ is defined by

$$1 + 0 \cdot \omega \mapsto \alpha = a + \sqrt{5}b$$
$$0 + 1 \cdot \omega \mapsto \omega\alpha = 5b + \sqrt{5}a$$

and the matrix belonging to Φ is given by

$$A_\Phi = \begin{pmatrix} a & 5b \\ b & a \end{pmatrix}$$

hence it is $\mathrm{Tr}_K(\alpha) = 2a$, $\mathrm{N}_K(\alpha) = a^2 - 5b^2$, and $\chi_\alpha(X) = X^2 - 2aX + a^2 - 5b^2$. □

4. In more general terms, let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer. If $\alpha = a + \sqrt{d}b$, then $\mathrm{Tr}_K(\alpha) = 2a$ and $\mathrm{N}_K(\alpha) = a^2 - db^2$.

Proof. A basis of K is $1, \sqrt{d}$. Let Φ_α be a linear operator defined by

$$1 + 0 \cdot \sqrt{d} \mapsto \alpha = a + \sqrt{d}b$$
$$0 + 1 \cdot \sqrt{d} \mapsto \sqrt{d}\alpha = db + \sqrt{d}a$$

which we may represent by a 2×2 matrix

$$A_\Phi = \begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

We have $\mathrm{Tr}_K(\alpha) = 2a$, $\mathrm{N}_K(\alpha) = a^2 - db^2$, and $\chi_\alpha(X) = X^2 - 2aX + a^2 - db^2$ matching the results in our previous examples. □

[1] The given basis is not an integral basis, but an integral basis is not required to find the field trace and field norm of an element.

5. Let $\mathbb{Q}(\sqrt[3]{2})$. If $\alpha = a + \sqrt[3]{2}b + \sqrt[3]{4}c$, then $\mathrm{N}_K(\alpha) = a^3 + 2b^3 + 4c^3 - 6abc$.

   Proof. A basis of K is $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. Let Φ_α be a linear operator defined by

   $$\begin{aligned} 1 + 0 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4} &\mapsto \alpha = a + \sqrt[3]{2}b + \sqrt[3]{4}c \\ 0 + 1 \cdot \sqrt[3]{2} + 0 \cdot \sqrt[3]{4} &\mapsto \sqrt[3]{2}\alpha = 2c + \sqrt[3]{2}a + \sqrt[3]{4}b \\ 0 + 0 \cdot \sqrt[3]{2} + 1 \cdot \sqrt[3]{4} &\mapsto \sqrt[3]{4}\alpha = 2b + \sqrt[3]{2}(2c) + \sqrt[3]{4}a \end{aligned}$$

   which we again represent by

   $$A_\Phi = \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}.$$

   We have $\mathrm{Tr}_K(\alpha) = 3a$, $\mathrm{N}_K(\alpha) = a^3 + 2b^3 + 4c^3 - 6abc$ and $\chi_\alpha(X) = X^3 - 3aX^2 + 3a^2X - 6bcX - a^3 - 2b^3 + 6abc - 4c^3$. □

Example 9.2. In this example, we will look at the cases when the field extension is given by a root of a polynomial [2].

1. Let $K = \mathbb{Q}(\theta)$ where θ is a root of $X^3 - X - 1$. If $\alpha = a + \theta b + \theta^2 c$, then $\mathrm{Tr}_K(\alpha) = 3a + 2c$ and $\mathrm{N}_K(\alpha) = a^3 + b^3 + 2a^2c - bc^2 + c^3 + a(-b^2 - 3bc + c^2)$.

   Proof. First, we have

   $$\begin{aligned} X^3 - X - 1 = 0 \quad &\Rightarrow \quad \theta^3 - \theta - 1 = 0 \\ &\Rightarrow \quad \theta^3 = \theta + 1 \end{aligned}$$

   so $[K : Q] \leq 3$.

   Assume $X^3 - X - 1$ is reducible, then by Rational Root Theorem, we have that there is a root $x = pq^{-1}$ with p is a factor of -1 and q is a factor of 1, but ± 1 is not a root of the polynomial. Thus, $X^3 - X - 1$ is irreducible.

   If θ^2 is rational, then the minimal polynomial of θ has a degree of 2 and divides $X^2 - X - 1$ which cannot be. Hence θ^2 is not rational and $\{1, \theta, \theta^2\}$ is a basis for K.

   Let $\alpha = a + \theta b + \theta^2 c$ be an element in K and define a linear operator Φ_α by

   $$\begin{aligned} 1 + 0 \cdot \theta + 0 \cdot \theta^2 \mapsto \alpha &= a + \theta b + \theta^2 c \\ 0 + 1 \cdot \theta + 0 \cdot \theta^2 \mapsto \theta\alpha &= \theta^3 c + \theta a + \theta^2 b \\ &= (\theta + 1)c + \theta a + \theta^2 b \\ &= c + \theta(a + c) + \theta^2 b \\ 0 + 0 \cdot \theta + 1 \cdot \theta^2 \mapsto \theta^2\alpha &= \theta^3 b + \theta^4 c + \theta^2 a \\ &= (\theta + 1)b + (\theta^2 + \theta)c + \theta^2 a \\ &= b + \theta b + \theta^2 c + \theta c + \theta^2 a \\ &= b + \theta(b + c) + \theta^2(a + c) \end{aligned}$$

   which we represent with a 3×3 matrix

   $$A_\Phi = \begin{pmatrix} a & c & b \\ b & a + c & b + c \\ c & b & a + c \end{pmatrix}$$

   so we have $\mathrm{Tr}_K(\alpha) = 3a + 2c$, $\mathrm{N}_K(\alpha) = a^3 + b^3 + 2a^2c - bc^2 + c^3 + a(-b^2 - 3bc + c^2)$, and $\chi_\alpha(X) =$ □

[2] The field extensions are defined by a single root of a polynomial, in other words, how the field extension looks exactly depends on the chosen root, and they are not a splitting field of the polynomial.

2. Let $K = \mathbb{Q}(\theta)$ where θ is a root of $f(X) = X^4 - X - 1$.

   Proof. If $X^4 - X - 1$ is reducible, then by Rational Root Theorem, there is a root pq^{-1} with $p, q \in \mathbb{Z}$ relatively prime such that p is a factor of -1 and q is a factor of 1. However, ± 1 is not a root because $f(\pm 1) = 1 \pm 1 - 1 = \pm 1$. We have that f is irreducible over the rational numbers.

   Since f is irreducible, if θ is a root of f, then f is the minimal polynomial of θ and we have a basis $\{1, \theta, \theta^2, \theta^3\}$ for K. Now let $\alpha = a + \theta b + \theta^2 c + \theta^3 d$ and define a linear operator Φ_α by

$$\begin{aligned}
1 + 0 \cdot \theta + 0 \cdot \theta^2 + 0\theta^3 \mapsto \alpha &= a + \theta b + \theta^2 c + \theta^3 d \\
0 + 1 \cdot \theta + 0 \cdot \theta^2 + 0\theta^3 \mapsto \theta\alpha &= \theta a + \theta^2 b + \theta^3 c + \theta^4 d \\
&= \theta a + \theta^2 b + \theta^3 c + (\theta + 1)d \\
&= d + \theta(a + d) + \theta^2 b + \theta^3 c \\
0 + 0 \cdot \theta + 1 \cdot \theta^2 + 0 \cdot \theta^3 \mapsto \theta^2\alpha &= \theta^2 a + \theta^3 b + \theta^4 c + \theta^5 d \\
&= \theta^2 a + \theta^3 b + (\theta + 1)c + (\theta^2 + \theta)d \\
&= c + \theta(c + d) + \theta^2(a + d) + \theta^3 b \\
0 + 0 \cdot \theta + 0 \cdot \theta^2 + 1 \cdot \theta^3 \mapsto \theta^3\alpha &= \theta^3 a + \theta^4 b + \theta^5 c + \theta^6 d \\
&= \theta^3 a + (\theta + 1)b + (\theta^2 + \theta)c + (\theta^3 + \theta^2)d \\
&= b + \theta(b + c) + \theta^2(c + d) + \theta^3(a + d)
\end{aligned}$$

   which we can represent by a 4×4 matrix

$$A_\Phi = \begin{pmatrix} a & d & c & b \\ b & a + d & c + d & b + c \\ c & b & a + d & c + d \\ d & c & b & a + d \end{pmatrix}.$$

   So we have $\mathrm{Tr}_K(\alpha) = 4a + 3d$ and the norm is too unholy to write it out here. □

Proposition 10. Let K be an algebraic number field and let $\alpha \in K$ be an algebraic number. If $\sigma_1, \ldots, \sigma_n$ are n distinct embeddings of K into $\mathbb{C}$ which fix K, then we have for the trace of α and the norm of α that

$$\mathrm{Tr}_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \qquad \mathrm{N}_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Proof. □

Proposition 11. If α is an algebraic number, then its characteristic polynomial is a multiple of its minimal polynomial, i.e. let K be an algebraic number field and let $\alpha \in K$ be an algebraic number, then

$$\chi_\alpha(X) = m_\alpha(X)h(X) \qquad h(X) \in \mathbb{Q}[X]$$

where χ_α is the characteristic polynomial of α and m_α is the minimal polynomial of α.

Proof. Let K be an algebraic number field and fix an algebraic number $\alpha \in K$. Both the characteristic polynomial and the minimal polynomial are monic by definition. If m_α is a minimal polynomial of α and has a degree of m, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = m$, so the characteristic polynomial χ_α is also of degree m.

An intermediate result that we will not prove (because I cannot be bothered by it) is $\chi_\alpha(\Phi_\alpha) = \Phi_{\chi_\alpha(\alpha)}$. By Cayley-Hamilton theorem we also have $\chi_\alpha(\Phi_\alpha) = 0$, so $\Phi_{\chi_\alpha(\alpha)} = 0$. If the linear operator defined by $v \mapsto \alpha v$ is identical to 0, then α must be 0, so $\chi_\alpha(\alpha) = 0$ which means that α is a root of its own characteristic polynomial.

The characteristic polynomial and the minimal polynomial share a root and because of minimality of the minimal polynomial, the minimal polynomial divides the characteristic polynomial, but because they are of the same degree, we have that these polynomials are identical. □

Example 11.1. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\alpha = \sqrt{2} + \sqrt{3}$. The minimal polynomial of α is

Proof. A basis of K is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Define a linear mapping Φ_α by

$$\begin{aligned}
1 + 0 \cdot \sqrt{2} + 0 \cdot \sqrt{3} + 0 \cdot \sqrt{6} &\mapsto (\sqrt{2} + \sqrt{3})1 = 0 + \sqrt{2} + \sqrt{3} + 0 \\
0 + 1 \cdot \sqrt{2} + 0 \cdot \sqrt{3} + 0 \cdot \sqrt{6} &\mapsto (\sqrt{2} + \sqrt{3})\sqrt{2} = 2 + 0 + 0 + \sqrt{6} \\
0 + 0 \cdot \sqrt{2} + 1 \cdot \sqrt{3} + 0 \cdot \sqrt{6} &\mapsto (\sqrt{2} + \sqrt{3})\sqrt{3} = 3 + 0 + 0 + \sqrt{6} \\
0 + 0 \cdot \sqrt{2} + 0 \cdot \sqrt{3} + 0 \cdot \sqrt{6} &\mapsto (\sqrt{2} + \sqrt{3})\sqrt{6} = 0 + 3\sqrt{2} + 2\sqrt{3} + 0
\end{aligned}$$

which is represented by

$$A_\phi = \begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

This gives us the minimal polynomial $m_\alpha(X) = X^4 - 10X + 1$ of α. □

Lemma 12. If K is an algebraic number field, and $\alpha \in \mathcal{O}_K$ an element in its ring of integers, then $\mathrm{Tr}_K(\alpha)$ and $\mathrm{N}_K(\alpha)$ are in $\mathbb{Z}$.

1. *Proof.* Let α be an algebraic integer. Since the characteristic polynomial of α is a multiple of the minimal polynomial, it has integer coeffcients. Denote the minimal polynomial by $m_\alpha = \sum_{i=0}^{n} a_i X^i$ for some $a_i \in \mathbb{Z}$ for $1 \leq i \leq n$. The trace is coeffcient of X^{n-1} in the characteristic polynomial [3], therefore it is an integer. Moreover, we have $N(\alpha) = (-1)^n \chi_\alpha(0) = (-1)^n a_0$ which again is an integer. □

2. *Proof.* Let K be an algebraic number field of degree n and fix an element $\alpha \in \mathcal{O}_K$ in its ring of integers. We define a linear operator $\Phi : K \longrightarrow K$ by $v \mapsto \alpha v$. If $e_1, \ldots, e_n$ is a basis of K viewed as a vector space over $\mathbb{Q}$, then we may represent Φ as a $n \times n$ matrix by

$$\alpha e_i = \sum_{j=1}^{n} a_{i,j} e_j$$

for all $1 \leq i \leq n$ and $a_{i,j} \in \mathbb{Q}$. Taking the conjugates, we get

$$\alpha^{(k)} e_i^{(k)} = \sum_{j=1}^{n} a_{i,j} e_j^{(k)}$$

and with Kronecker delta we can write

$$\sum_{j=1}^{n} \delta_{j,k} \alpha^{(j)} e_i^{(j)} = \sum_{j=1}^{n} a_{i,j} e_j^{(k)}.$$

Now set $\Phi_A := (a_{i,j})$ □

[3] I had no idea. Don't want to prove it now, but I'll look into this later.

Example 12.1. Let $K = \mathbb{Q}(i)$. Show that $i \in \mathcal{O}_K$ and verify that $\mathrm{Tr}_K(i)$ and $\mathrm{N}_K(i)$ are integers.

Proof. $X^2 + 1 \in \mathbb{Z}[X]$ has the root i, so i is in $\mathcal{O}_K$. Since the $\mathbb{Q}$-basis of $\mathbb{Q}(i)$ is $\{1, i\}$, we have

$$\Phi_i(a + ib) = -b + a_i$$

therefore, the matrix is

$$\Phi_i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and hence its trace is $\mathrm{Tr}_K(i) = 0$. Similary, its norm is $\mathrm{N}_K(i) = 1$. □

Example 12.2. Determine the algebraic integers of $\mathbb{Q}(\sqrt{-5})$.

Proof. A $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{-5})$ is $\{1, \sqrt{-5}\}$. Let $\alpha = x + \sqrt{-5}y \in \mathbb{Q}(\sqrt{-5})$. Then

$$\Phi_x(a + \sqrt{-5}b) = (x + \sqrt{-5}y)(a + \sqrt{-5}b) = xa - 5yb + (bx + ya)\sqrt{-5},$$

therefore,

$$\Phi_\alpha = \begin{pmatrix} x & y \\ -5y & x \end{pmatrix}$$

hence we have $\mathrm{Tr}_K(\alpha) = 2x$ and $\mathrm{N}_K = x^2 + 5y^2$.

If x is not an integer, then $2x$ must be, so we must have that $y^2 \equiv 3 \mod 4$, but this is impossible. Hence x, y are both integers, therefore, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. □

Corollary 2. An element u in a ring of integers $\mathcal{O}_K$ is a unit if and only if $N_K(u) = \pm 1$.

Proof.

1. "⇒": Let $u \in \mathcal{O}_K$ be a unit, then there is an element $v \in \mathcal{O}_K$ such that $uv = 1$. By the multiplicative property, we have

   $$1 = N_K(1) = N_K(uv) = N_K(u)N_K(v)$$

   and since $N_K(u)$ and $N_K(v)$ are both integers, the only possibilities are $N_K(u) = \pm 1$.

2. "⇐": Conversely, let u have the norm ± 1. Denote the characteristic polynomial of u by $\chi_u(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. It is

   $$N(u) = \pm 1 = \det(\Phi_u) = \det(0I - \Phi_u) = \chi_u(0) = a_0$$

   so we have

   $$u^n + a_{n-1}u^{n-1} + \cdots + a_1u \pm 1 = 0.$$

   Now let $v \in K$ be the multiplicative inverse of u, i.e. $uv = 1$. We want to show that v is in the ring of integers of K. Multiplying v^n on both sides of the equation above yields

   $$\begin{aligned} & u^nv^n + a_{n-1}u^{n-1}v^n + \cdots + a_1uv^n \pm v^n = 0 \\ \iff & 1 + a_{n-1}v + \cdots + a_1v^{n-1} \pm v^n = 0. \end{aligned}$$

   Thus $1 + a_{n-1}X + \cdots + a_1X^{n-1} \pm X^n$ is a polynomial in $\mathbb{Z}[X]$ that has v as a root. This polynomial can be converted to a monic polynomial depending on the sign of the monomial of the highest degree by multiplying -1 if necessary. Therefore, $u \in \mathcal{O}_K$.

□

6.2.2 Integral Basis

Example 12.3. 4.1.5 I'll skip this.

Example 12.4. Show that there exist $\omega_1^*, \ldots, \omega_n^* \in K$ such that

$$\mathcal{O}_K \subset \mathbb{Z}\omega_1^* + \cdots + \mathbb{Z}\omega_n^*.$$

Proof. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Q}$-basis for K. For any $\alpha \in K$, there is a nonzero integer $m \in \mathbb{Z}$ such that $m\alpha \in \mathcal{O}_K$. □

I'll skip exercises that require bilinear form for now.

Definition 13. Let K be an algebraic number field of degree n and $\mathcal{O}_K$ be its ring of integers. We say that $\omega_1, \ldots, \omega_n$ is an integral basis for K if $\omega_i \in \mathcal{O}_K$ for all $1 \leq i \leq n$ and $\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$.

Example 13.1. Show that $\det \mathrm{Tr}(\omega_i\omega_j)$ is independent of the choice of integral basis.

6.2.3 Discriminant

Definition 14 (Discriminant)**.** Let K be an algebraic number field of degree n and $\omega_1, \ldots, \omega_n$ an integral basis. The discriminant of K is defined as

$$d_K := \det\left(\omega_i^{(j)}\right)^2.$$

Proof. We show that the discriminant is well-defined. In other words, the discriminant is independent of the choice of integral basis.

Let $\omega_1, \ldots, \omega_n$ and $\theta_1, \ldots, \theta_n$ be two integral basis for K. □

Example 14.1. In this example, we will compute the discriminant of some concrete algebraic number fields.

1. Let d be a square-free integer and consider the algebraic number field $K = \mathbb{Q}(\sqrt{d})$. The discriminant of K is

$$\Delta_K = \begin{cases} d & \text{if } d \equiv 1 \mod 4 \\ 4d & \text{if } d \equiv 2, 3 \mod 4. \end{cases}$$

Proof. The ring of integers of K is $\mathbb{Z}[\alpha]$ where

$$\alpha := \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \\ \sqrt{d} & d \equiv 2, 3 \mod 4. \end{cases}$$

We will look at each case one by one.

(a) If $\alpha = 2^{-1}(1 + \sqrt{d})$, then a integral basis and its conjugate are

$$\left\{1, \frac{1+\sqrt{d}}{2}\right\} \text{ and } \left\{1, \frac{1-\sqrt{d}}{2}\right\},$$

therefore, the discriminant is

$$\Delta_K = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = \left(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2}\right)^2 = \left(-\frac{2\sqrt{d}}{2}\right)^2 = d.$$

(b) On the other hand, if $\alpha = \sqrt{d}$, then a integral basis and its conjugate are

$$\left\{1, \sqrt{d}\right\} \text{ and } \left\{1, -\sqrt{d}\right\}$$

and hence we have

$$\Delta_K = \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}^2 = \left(-2\sqrt{d}\right)^2 = 4d.$$

Conclude the stated result above. □

2. Let $K = \mathbb{Q}(\sqrt[3]{2})$, then the discriminant is $\Delta_K = -108$.

Proof. Denote $\alpha := \sqrt[3]{2}$. The ring of integers is[4] $\mathcal{O}_K = \mathbb{Z}[\alpha]$, so a integral basis is $\{1, \alpha, \alpha^2\}$. Moreover, the minimal polynomial of α is

$$m_\alpha(X) = X^3 - 2$$

[4] To prove this, there is a lot of work to be done and I will maybe do this someday.

which has the roots α, $\zeta_3\alpha$ and $\zeta_3^2\alpha$ where ζ_3 is the 3rd root of unity. This gives us the embeddings

$$\begin{array}{lll} \sigma_1 \equiv \mathrm{id}_K & \sigma_2(\alpha) = \zeta_3\alpha & \sigma_3(\alpha) = \zeta_3^2\alpha \\ & \sigma_2(\zeta_3\alpha) = \zeta_3^2\alpha & \sigma_3(\zeta_3\alpha) = \zeta_3\alpha \\ & \sigma_2(\zeta_3^2\alpha) = \alpha & \sigma_3(\zeta_3^2\alpha) = \alpha \end{array}$$

or shorter, $\sigma_1 : \alpha \mapsto \alpha$, $\sigma_2 : \alpha \mapsto \zeta_3\alpha$ and $\sigma_3 : \alpha \mapsto \zeta_3^2\alpha$. Applying the embeddings on the integral basis yields

$$\begin{array}{lll} \sigma_1(1) = 1 & \sigma_1(\alpha) = \alpha & \sigma_1(\alpha^2) = \alpha^2 \\ \sigma_2(1) = 1 & \sigma_2(\alpha) = \zeta_3\alpha & \sigma_2(\alpha^2) = \sigma_2(\alpha)\sigma_2(\alpha) = \zeta_3^2\alpha^2 \\ \sigma_3(1) = 1 & \sigma_3(\alpha) = \zeta_3^2\alpha & \sigma_3(\alpha^2) = \sigma_3(\alpha)\sigma_3(\alpha) = \zeta_3\alpha^2. \end{array}$$

Therefore, the discriminant is

$$\Delta_K = \left(\det \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \zeta_3\alpha & \zeta_3^2\alpha^2 \\ 1 & \zeta_3^2\alpha & \zeta_3\alpha^2 \end{pmatrix} \right)^2 = \left(-6i\sqrt{3}\right)^2 = -108.$$

□

3. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Proof. An integral basis[5] is

$$\left\{ 1, \sqrt{2}, \sqrt{3}, \underbrace{\frac{\sqrt{2}+\sqrt{6}}{2}}_{=:\alpha} \right\}.$$

We need to find 4 embeddings of K. σ_1 is, as always, the identity on K. σ_2 permutates $\sqrt{2}$ and σ_3 permutates $\sqrt{3}$. Then, $\sigma_4 = \sigma_2 \circ \sigma_3$. Therefore, we have

$$\begin{array}{llll} \sigma_1(1) = 1 & \sigma_1(\sqrt{2}) = \sqrt{2} & \sigma_1(\sqrt{3}) = \sqrt{3} & \sigma_1\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right) = \frac{\sqrt{2}+\sqrt{6}}{2} \\ \sigma_2(1) = 1 & \sigma_2(\sqrt{2}) = -\sqrt{2} & \sigma_2(\sqrt{3}) = \sqrt{3} & \sigma_2\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right) = \frac{-\sqrt{2}-\sqrt{6}}{2} \\ \sigma_3(1) = 1 & \sigma_3(\sqrt{2}) = \sqrt{2} & \sigma_3(\sqrt{3}) = -\sqrt{3} & \sigma_3\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right) = \frac{\sqrt{2}-\sqrt{6}}{2} \\ \sigma_4(1) = 1 & \sigma_4(\sqrt{2}) = -\sqrt{2} & \sigma_4(\sqrt{3}) = -\sqrt{3} & \sigma_4\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right) = \frac{-\sqrt{2}+\sqrt{6}}{2} \end{array}$$

So the discriminant of K is

$$\Delta_K = \left(\det \begin{pmatrix} 1 & \sqrt{2} & \sqrt{3} & \frac{\sqrt{2}+\sqrt{6}}{2} \\ 1 & -\sqrt{2} & \sqrt{3} & \frac{-\sqrt{2}-\sqrt{6}}{2} \\ 1 & \sqrt{2} & -\sqrt{3} & \frac{\sqrt{2}-\sqrt{6}}{2} \\ 1 & -\sqrt{2} & -\sqrt{3} & \frac{-\sqrt{2}+\sqrt{6}}{2} \end{pmatrix} \right)^2 = 48^2 = 2304$$

□

[5] Again, I will show this later, maybe. Apparantly, there is a general formula to find the ring of integers of two squareroots.

Definition 15. Let K be an algebraic number field of degree n and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K. For $a_1, \ldots, a_n \in K$ we can define the discriminant as

$$\Delta_K(a_1, \ldots, a_n) = [\det(\sigma_i(a_j))]^2.$$

Proposition 16. It is

$$\Delta_K(1, a, a^2 \ldots, a^{n-1}) = \prod_{i>j}(\sigma_i(a) - \sigma_j(a)).$$

Proof. Because $\sigma_i(a^j) = a^{j+i-1}$, we have

$$\begin{aligned}
\Delta_K(1, a, a^2, \ldots, a^{n-1}) &= \left[\det \begin{pmatrix} \sigma_1(1) & \sigma_1(a) & \sigma_1(a^2) & \cdots & \sigma_1(a^{n-1}) \\ \sigma_2(1) & \sigma_2(a) & \sigma_2(a^2) & \cdots & \sigma_2(a^{n-1}) \\ \sigma_3(1) & \sigma_3(a) & \sigma_3(a^2) & \cdots & \sigma_3(a^{n-1}) \\ \vdots & & & & \\ \sigma_n(1) & \sigma_n(a) & \sigma_n(a^2) & \cdots & \sigma_n(a^{n-1}) \end{pmatrix} \right]^2 \\
&= \left[\det \begin{pmatrix} 1 & a & a^2 & \cdots & a^{n-1} \\ 1 & a^2 & a^3 & \cdots & a^n \\ 1 & a^3 & a^4 & \cdots & a^{n+1} \\ \vdots & & & & \vdots \\ 1 & a^n & a^{n+1} & \cdots & a^{2n-1} \end{pmatrix} \right]^2 \\
&= \prod_{i>j}(\sigma_i(a) - \sigma_j(a))
\end{aligned}$$

by Vandermonde matrix. □

Remark. We denote $\Delta_K(1, a, a^2, \ldots, a^{n-1})$ by $\Delta_K(a)$.

Chapter 7

Dedekind Domains

Definition 17. An integral domain A is called Dedekind domain if one of the following equivalent conditions are met.

1. Every nonzero proper ideal of A factors into product of prime ideals.
2. A is
   (a) integrally closed,
   (b) Noetherian,
   (c) and every nonzero prime ideal of A is maximal.

Remark. We have the following chain of inclusions for ring structures.

Theorem 18. Every ring of integers $\mathcal{O}_K$ is a Dedekind domain.

Proof. Let $\mathcal{O}_K$ be the ring of integers of an algebraic number field K. We show that $\mathcal{O}_K$ is a Dedekind domain by proving $\mathcal{O}_K$ is integrally closed, Noetherian, and every nonzero prime ideal of A is maximal. □

Lemma 19. $\mathcal{O}_K$ is integrally closed.

Proof. □

Lemma 20. If $\mathfrak{a} \subset \mathfrak{b}$ are ideals of $\mathcal{O}_K$, then $\mathrm{N}(a) > \mathrm{N}(b)$.

Proof. We show that there is a map $\varphi : \mathcal{O}_K/\mathfrak{a} \longrightarrow \mathcal{O}_K/\mathfrak{b}$ that is surjective, but not injective [1]. Since both the domain and the codomain are finite sets, if such a map φ exists, then φ can be restricted to a subset of $\mathcal{O}_K/\mathfrak{a}$ such that the restricted φ becomes a bijection. From there, we conclude that $|\mathcal{O}_K/\mathfrak{a}| > |\mathcal{O}_K/\mathfrak{b}|$, i.e. $\mathrm{N}(a) > \mathrm{N}(b)$.

Define $\varphi : \mathcal{O}_K/\mathfrak{a} \longrightarrow \mathcal{O}_K/\mathfrak{b}$ as

$$\varphi(x + \mathfrak{a}) = x + \mathfrak{b}.$$

[1] I believe constructing a map in opposite direction and showing that this map is injective but not surjective might not work because proving that it is well-defined is difficult. Not sure.

Then, φ is well-defined, because if $x + \mathfrak{a} = y + \mathfrak{a}$, then $x - y \in \mathfrak{a}$, so $x - y \in \mathfrak{b}$ too and we have $x + \mathfrak{b} = y + \mathfrak{b}$. This map is also surjective because $x + \mathfrak{b} = \varphi(x + \mathfrak{a})$, but it is not injective because if $y \in \mathfrak{b}$ but not $y \in \mathfrak{a}$, then $\varphi(y + \mathfrak{a}) = y + \mathfrak{b} = 0 = \varphi(0 + \mathfrak{a})$. □

Lemma 21. $\mathcal{O}_K$ is Noetherian.

Proof. □

Lemma 22. A ring is a field if and only if it has no nontrivial ideals, i.e. the only ideals are the zero ideal and the ring itself.

Proof. □

Lemma 23. Every finite integral domain is a field.

Proof. □

Lemma 24. Every nonzero prime ideal in $\mathcal{O}_K$ is maximal.

Theorem 25. Every principal ideal domain is a Dedekind domain. A unique factorization domain is a Dedekind domain if and only if it is a principal ideal domain.

Proof.

1. Let A be a principal ideal domain. A is integrally closed because it is also a unique factorization domain which are integrally closed.
2. A is also Noetherian (easy).
3. And clearly all nonzero prime ideal of A is maximal.

□

Example 25.1. Not all Dedekind domains are principal ideal domains. $\mathbb{Z}[\sqrt{-5}]$ is Dedekind, but not PID.

Proof.

1. The algebraic number field $\mathbb{Q}(\sqrt{-5})$ has the ring of integers $\mathbb{Z}[\sqrt{-5}]$, so $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain.
2. We have the factorizations $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, therefore $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain, hence it cannot be a principal ideal domain.

□

Definition 26. A fractional ideal $\mathcal{A}$ of $\mathcal{O}_K$ is an $\mathcal{O}_K$-module contained in K such that there exists $m \in \mathbb{Z}$ with $m\mathcal{A} \subset \mathcal{O}_K$.

Proposition 27. A fractional ideal is finitely generated as an $\mathcal{O}_K$-module.

Proof. Let $\mathcal{A}$ be a fractional ideal of $\mathcal{O}_K$. By definition, there is an integer $m \in \mathbb{Z}$ such that $m\mathcal{A} \subset \mathcal{O}_K$. Since $\mathcal{O}_K$ is Noetherian, the submodule $m\mathcal{A}$ is finitely generated by say

$$\{ ma_1, \ldots, ma_n \} \tag{7.1}$$

for some $a_1, \ldots, a_n \in \mathcal{A}$, so $\mathcal{A}$ is finitely generated by $\{ a_1, \ldots, a_n \}$. □

Proposition 28. The sum and product of fractional ideals are again fractional ideals.

Proof. easy □

Lemma 29. Any proper ideal of $\mathcal{O}_K$ contains a product of nonzero prime ideals.

Proof. Let S be the set of proper ideals of $\mathcal{O}_K$ that do not contain a product of nonzero prime ideals. We want to show that S is empty. Assume it is not. Then, because $\mathcal{O}_K$ is noetherian, there is a maximal element of S say $\mathfrak{a}$. $\mathfrak{a}$ cannot be prime, because if it was, then $\mathfrak{a} \supset \mathfrak{a} \cdot \mathfrak{a}$. Therefore, there is an element $ab \in \mathfrak{a}$ with $a \notin \mathfrak{a}$ and $b \notin \mathfrak{b}$. This implies also that the two ideals $(\mathfrak{a}, a) \supsetneq \mathfrak{a}$ and $(\mathfrak{a}, b) \supsetneq$ are not in S by the maximality of $\mathfrak{a}$.

If $(\mathfrak{a}, a)$ and $(\mathfrak{a}, b)$ are not in S, then they contain a product of nonzero prie ideals, i.e.

$$(\mathfrak{a}, a) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \qquad (\mathfrak{a}, b) \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are nonzero prime ideals.

On the other hand, we have $(\mathfrak{a}, ab) = \mathfrak{a}$ since $ab \in \mathfrak{a}$, but then

$$\mathfrak{a} = (\mathfrak{a}, ab) \supseteq (\mathfrak{a}, a)(\mathfrak{a}, b) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_s \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_r$$

which would contradict that $\mathfrak{a}$ being contained in S, therefore S must be empty. □

Lemma 30. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. There exists $z \in K$ (with $z \notin \mathcal{O}_K$), such that $z\mathfrak{p} \subseteq \mathcal{O}_K$.

Proof. Take $x \in \mathfrak{p}$. From the previous lemma, we have that $(x) = x\mathcal{O}_K$ contains a product of prime ideals, i.e.

$$(x) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

and let r the least integer. Since $\mathfrak{p} \supseteq (x) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$, we have that $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i. But all nonzero prime ideals are maximal in $\mathcal{O}_K$, we have that $\mathfrak{p} = \mathfrak{p}_1$.

Now $\mathfrak{p}_2, \ldots, \mathfrak{p}_r \not\subseteq (x)$ because r was chosen to be minimal (why? check later).

Choose an element $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ with $b \notin x\mathcal{O}_K$, then

$$bx^{-1}\mathfrak{p} = bx^{-1}\mathfrak{p}_1$$

□

Definition 31 (Ideal Quotient)**.** Let A be a ring, and $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals. Their ideal quotient is defined by

$$(\mathfrak{a} : \mathfrak{b}) := \{ x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a} \}.$$

Moreover, we write

$$\mathfrak{p}^{-1} := (\mathcal{O}_K : \mathfrak{p}) = \{ x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}_K \}.$$

Theorem 32. Any ideal of $\mathcal{O}_K$ can be uniquely written as a product of prime ideals.

Proof. We prove two statements. Firstly that such a factorization exists, and secondly that if such a factorization exists, then it is unique up to the order of the factors.

1. **Existence.** Let S be the set of ideals of $\mathcal{O}_K$ that cannot be written as a product of prime ideals. Our goal is to show that S is empty. If S is not empty, then because $\mathcal{O}_K$ is noetherian, there exists a maximal element[2] of S say $\mathfrak{a}$. This ideal $\mathfrak{a}$ is not prime, because if it was, then $\mathfrak{a} \supseteq \mathfrak{a}\cdot\mathfrak{a}$ and $\mathfrak{a}$ would contain a product of prime ideals. Moreover, $\mathfrak{a}$ is contained in a maximal ideal $\mathfrak{m}$ of $\mathcal{O}_K$.

   Consider the ideal $\mathfrak{m}^{-1}\mathfrak{a}$. We want to show that $\mathfrak{m}^{-1}\mathfrak{a}$ is a proper ideal of $\mathcal{O}_K$ and that $\mathfrak{a}$ is a proper subset of $\mathfrak{m}^{-1}\mathfrak{a}$.

   For any prime ideal $\mathfrak{p}$, we have $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$ because if $y \in \mathfrak{p}^{-1}\mathfrak{p}$, then $y = x\mathfrak{p} \subseteq \mathcal{O}_K$. On the other hand, if $y \in \mathcal{O}_K$, then ??? idk.

   Consider $\mathfrak{m}^{-1}\mathfrak{a}$. It is

   $$\mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{m} = \mathcal{O}_K.$$

   Because for any $x \in \mathfrak{m}$ with $x \notin \mathfrak{a}$ we have

   $$\mathfrak{p}^{-1}x \subseteq \mathfrak{p}^{-1}\mathfrak{a} \Rightarrow x \in \mathfrak{m}^{-1}\mathfrak{m}\mathfrak{a} = \mathcal{O}_K\mathfrak{a} = \mathfrak{a}$$

□

[2]The maximal element $\mathfrak{a}$ need not be a maximal ideal. $\mathfrak{a}$ is an ideal which has no superset inside S, i.e. there are no $\mathfrak{b} \in S$ with $\mathfrak{a} \subseteq \mathfrak{b}$.