

Part I

Cheet Sheet



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

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

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

**Theorem 1.** 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 2.** Symmetric polynomials and elementary symmetric polynomials.

**Theorem 3.** Let  $A$  be a ring. Every symmetric polynomial  $P(X_1, \dots, X_r)$  in  $A[X_1, \dots, X_r]$  can be represented with a linear combination of elementary symmetric polynomials with coefficients in  $A$ .

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

The above proof implies:

Let  $f(X) = X^n + a_1X^{n-1} + \dots + a_n \in A[X]$ , and let  $\alpha_1, \dots, \alpha_n$  be the roots of  $f(X)$  in some ring containing  $A$ , so that  $f(X) = \prod (X - \alpha_i)$  in the larger ring. Then

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

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

*Proof.* Clearly,

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

is a monic polynomial whose coefficients are symmetric polynomials in the  $\alpha_i$ , and therefore lie in  $A$ . But  $g(\alpha_1, \dots, \alpha_n)$  is one of the roots.  $\square$

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

## Dedekind's Proof

**Proposition 5.** Let  $L$  be a field containing  $A$ . An element  $\alpha$  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  $\alpha$ ).

*Proof.* • Let  $\alpha \in L$  be integral over  $A$ . The  $A$ -submodule  $A[\alpha]$  in  $L$  is generated by  $1, \alpha, \dots, \alpha^{n-1}$ , 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  $v_1, \dots, v_n \in M$ . 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  $\alpha$  and  $\beta$  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 6.** 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  $B$ .

# **Part II**

## **Exercise**



**Example 6.1.** 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  $N : R \rightarrow \mathbb{N}$  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

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

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.  $\square$

**Example 6.2.** 2.1.3. did it before

**Example 6.3.** 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  $\pi$  is irreducible and  $\pi$  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  $\pi$ .

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

**Example 6.4.** Show that if  $\pi$  is an irreducible element of a principal ideal domain, then  $(\pi)$  is a maximal ideal.

*Proof.* Assume  $(\pi)$  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.  $\square$

**Example 6.5.** If  $F$  is a field, prove that  $F[x]$  is Euclidean.

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

**Example 6.6.** 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  $\alpha$  and  $p_y$  to be the closest integer to  $\beta$  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 6.7.** Prove that if  $p$  is a positive prime, then there is an element  $x \in \mathbb{Z}/p\mathbb{Z}$  such that  $x^2 \equiv -1 \pmod{p}$  if and only if either  $p = 2$  or  $p \equiv 1 \pmod{4}$ .

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

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

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

2. If  $p = 2$ , then we are done. Now let  $x^2 \equiv -1 \pmod{p}$ . If  $p \equiv 3 \pmod{4}$ , we have

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

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

□

**Example 6.8.** 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  $x^3 - 1 \equiv 3 \pmod{4}$  which cannot be a square since all squares are congruent to either 0 or 1  $\pmod{4}$ . 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 6.9.** What are the primes of  $\mathbb{Z}[i]$ ?

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

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

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

**Example 6.10.** A positive integer  $a$  is the sum of two squares if and only if  $a = b^2 c$  where  $c$  is not divisible by any positive prime  $p \equiv 3 \pmod{4}$ .



*Proof.* I don't know. □

**Example 6.11.**  $\mathbb{Z}[\rho]$  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 inherited 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

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

I made some mistake, but should be right.

- (b) The multiplicative identity is 1

3. Distributive law is again inherited. □

**Example 6.12.** 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

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

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  $\pm 1$ ,  $\pm\rho$ , and  $\pm\bar{\rho}$ .



# Chapter 1

## Algebraic Numbers and Integers

**Example 6.13.** Show that

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

is an algebraic number, but not an algebraic integer.

*Proof.* First of all,  $\alpha$  is the root of

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

so it is an algebraic number.

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

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

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  $\alpha$  is not an algebraic integer.  $\square$

**Example 6.14.** 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  $q = 1$ .  $\square$



## Chapter 2

### 3

**Example 6.15.** 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  $\alpha$  is an algebraic number, we have

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

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

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

so  $m\alpha \in \mathcal{O}_K$ . □



## Chapter 3

# Integral Bases

### 3.1 Overview

### 3.2 Details

**Definition 7** (Trace and Norm). 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

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

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

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

We define trace of  $\alpha$  by  $\text{Tr}_K(\alpha) := \text{Tr}(\Phi_\alpha)$  and the norm of  $\alpha$  by  $N(\alpha) := \det(\Phi_\alpha)$ .

**Example 7.1.** Let  $K = \mathbb{Q}(i)$ , then  $\mathcal{O}_K = \mathbb{Z}[i]$ . If  $\alpha = a + ib$  with  $a, b \in \mathbb{Q}$ , then  $\text{Tr}_K(\alpha) = 2a$  and  $N_K(\alpha) = a^2 + b^2$ .

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

$$\begin{aligned} 1 + 0 \cdot i &\mapsto \alpha = a + ib \\ 0 + 1 \cdot i &\mapsto \alpha i = -b + ia \end{aligned}$$

and we may represent  $\Phi$  by a  $2 \times 2$  matrix

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

Therefore,  $\text{Tr}_K(\alpha) = 2a$  and  $N_K(\alpha) = a^2 + b^2$ . □

**Example 7.2.** Let  $K = \mathbb{Q}(\sqrt{2})$ , then  $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ . If  $\alpha = a + \sqrt{2}b$  with  $a, b \in \mathbb{Q}$ , then  $\text{Tr}_K(\alpha) = 2a$  and  $N_K(\alpha) = a^2 - 2b^2$ .

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

$$\begin{aligned} 1 + 0 \cdot \sqrt{2} &\mapsto \alpha = a + \sqrt{2}b \\ 0 + 1 \cdot \sqrt{2} &\mapsto \sqrt{2}\alpha = 2b + \sqrt{2}a \end{aligned}$$

then the matrix belonging to  $\Phi_\alpha$  is

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

So we have  $\text{Tr}_K(\alpha) = 2a$  and  $N_K(\alpha) = a^2 - 2b^2$ . □

**Lemma 8.** If  $K$  is an algebraic number field, and  $\alpha \in \mathcal{O}_K$  an element in its ring of integers, then  $\text{Tr}_K(\alpha)$  and  $N_K(\alpha)$  are in  $\mathbb{Z}$ .

*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  $\Phi : K \rightarrow K$  by  $v \mapsto \alpha v$ . If  $e_1, \dots, e_n$  is a basis of  $K$  viewed as a vector space over  $\mathbb{Q}$ , then we may represent  $\Phi$  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  $\Phi_A := (a_{i,j})$  □

**Example 8.1.** Let  $K = \mathbb{Q}(i)$ . Show that  $i \in \mathcal{O}_K$  and verify that  $\text{Tr}_K(i)$  and  $N_K(i)$  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  $\text{Tr}_K(i) = 0$ . Similary, its norm is  $N_K(i) = 1$ . □

**Example 8.2.** 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  $\text{Tr}_K(\alpha) = 2x$  and  $N_K = x^2 + 5y^2$ .

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

**Example 8.3.** 4.1.5 I'll skip this.

**Example 8.4.** Show that there exist  $\omega_1^*, \dots, \omega_n^* \in K$  such that

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

*Proof.* Let  $\omega_1, \dots, \omega_n$  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 9.** Let  $K$  be an algebraic number field of degree  $n$  and  $\mathcal{O}_K$  be its ring of integers. We say that  $\omega_1, \dots, \omega_n$  is an integral basis for  $K$  if  $\omega_i \in \mathcal{O}_K$  for all  $1 \leq i \leq n$  and  $\mathcal{O}_K = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n$ .

**Example 9.1.** Show that  $\det \text{Tr}(\omega_i \omega_j)$  is independent of the choice of integral basis.

**Definition 10 (Discriminant).** Let  $K$  be an algebraic number field of degree  $n$  and  $\omega_1, \dots, \omega_n$  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  $\omega_1, \dots, \omega_n$  and  $\theta_1, \dots, \theta_n$  be two integral basis for  $K$ . □

**Example 10.1.** Let  $d$  be a square-free integer and consider the algebraic number field  $K = \mathbb{Q}(\sqrt{d})$ . The discriminant of  $K$  is

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

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

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

We will look at each case one by one.

1. 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

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

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

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

and hence we have

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

Conclude the stated result above. □