Algorithmic Number Theory

Lecture notes for
Winter 2017/18
TU-Kaiserslautern

by
C. Fieker
Version of January 9, 2018

Contents

CHAPTER 1

Number Fields

1. Basics

In this lecture, a number field L is a finite extension of $\mathbb{Q}$. Using the primitive element theorem in Galois theory, we have $L = \mathbb{Q}[\alpha] \simeq \mathbb{Q}[t]/f$ for f a suitable itteducible polynomial - e.g. the minimal polynomial of α. In what follows, we mostly assume f to be monic and integral, ie. $f \in \mathbb{Z}[t]$ with leading coefficient 1.

Note: we do not assume $L \subseteq \mathbb{C}$.

Let K be a field (mostly $K = \mathbb{Q}$ or a number field or at least a field of characteristic 0, but (much) later $K = \mathbb{F}_p(t)$) and let L/K be finite, $n := [L : K]$, i. e. L is a K-vectorspace with basis $\alpha_1, \ldots, \alpha_n$. For all $\beta \in L$ we have a map

$$\varphi_\beta : L \to L : x \mapsto \beta x$$

which is K-linear, hence we have $M_\beta \in K^{n\times n}$ such that

$$\beta(\alpha_1, \ldots, \alpha_n) = (\alpha_1, \ldots, \alpha_n)M_\beta$$

(careful: the left hand side is using products in L while the right hand side is using operations in K only. The α_i are just basis elements)

M_β is called *representation matrix* (or (right) regular representation) of β. $f_\beta := \det(xI_n - M_\beta) \in K[x]$ is called *characteristic polynomial* of β. Note that f_β does not depend on the chosen basis, while M_β obviously does. We have

$$f_\beta := x^n + b_{n-1}x^{n-1} + \ldots + b_0$$

and $\operatorname{Tr}\beta := \operatorname{Tr}_{L/K}\beta := \operatorname{Tr}_K^L\beta := -b_{n-1} = \operatorname{Tr} M_\beta$, $N\beta := N_{L/K}\beta := N_K^L\beta := (-1)^n b_0 = \det M_\beta$.

LEMMA 1.1: The map $L \to K^{n\times n} : x \mapsto M_x$ is a K-algebra homomorphism, i. e. $M_x + M_y = M_{x+y}$ and $M_xM_y = M_{xy}$.
We have $\operatorname{Tr}(x + y) = \operatorname{Tr}(x) + \operatorname{Tr}(y)$ and $N(xy) = N(x)N(y)$ as well as $\operatorname{Tr}(\mu x) = \mu \operatorname{Tr}(x)$, $\operatorname{Tr}(\mu) = n\mu$ and $N(\mu x) = \mu^n N(x)$ for $\mu \in K$. Thus Tr is K-linear.

LEMMA 1.2: Let L/K be a finite extension, $\alpha \in L$ and f_α be the characteristic polynomial. Then $f_\alpha = m_\alpha^r$ for some irreducible polynomial m_α, the minimal polynomial of α.

PROOF. Let the minimal polynomial $m_\alpha = \sum a_i t^i$ for some $a_i \in K$. Since a minimal polynomial is irreducible, $K[t]/m_\alpha \cong K[\alpha]$ is a subfield of L of degree $[K[\alpha] : K] = \deg m_\alpha$, hence $[L : K[\alpha]] = n/\deg m_\alpha =: r$ for $n := [L : K]$. Fix a $K[\alpha]$-basis $\beta_1, \ldots, \beta_r$ for L. Then $(\alpha^i\beta_j)_{i,j}$ is a K-basis for L. Let M_α be the representation matrix for $\alpha \in K[\alpha]$, ie

$$\alpha(1, \ldots, \alpha^{n-1}) = M_\alpha(1, \ldots, \alpha^{n-1})$$

now, obviously

$$\alpha(\beta_j, \ldots, \beta_j\alpha^{n-1}) = M_\alpha(\beta_j, \ldots, \beta_j\alpha^{n-1})$$

for all j, hence

$$\alpha(\beta_1, \ldots, \beta_1\alpha^{n-1}, \beta_2, \ldots, \beta_r\alpha^{n-1}) = \operatorname{diag}(M_\alpha, \ldots, M_\alpha)(\beta_1, \ldots, \beta_r\alpha^{n-1})$$

and the characteristic polynomial of the diagonal block matrix is as claimed. □

DEFINITION 1.3: Let $\alpha_1, \ldots, \alpha_n \in L$ be arbitrary. Then $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) := \det((\operatorname{Tr}(\alpha_i\alpha_j))_{i,j})$ is called the *discriminant* of $\alpha_1, \ldots, \alpha_n$.

THEOREM 1.4: Let $\alpha_1, \ldots, \alpha_n$ be a K-basis for L. Then $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$ iff $\operatorname{Tr}(a) = 0$ for all $a \in L$.

PROOF. Assume first that $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$. This implies that the columns of the matrix $(\operatorname{Tr}(\alpha_i\alpha_j))_{i,j}$ are K-linear dependent thus we can find $c_i \in K$, not all zero, such that

$$\sum_{j=1}^{n} c_j \operatorname{Tr}(\alpha_i\alpha_j) = 0$$

holds for all i. Set $\gamma := \sum c_j\alpha_j \in L \setminus \{0\}$. Let now $x \in L$ be abitrary. Then there is some $y \in L$, $y = \sum y_i\alpha_i$, such that $x = y\gamma$ holds. Now

$$\operatorname{Tr}(x) = \operatorname{Tr}(y\gamma) = \sum_i \operatorname{Tr}(y_i\alpha_i\gamma) = \sum_i y_i \sum_j c_j \operatorname{Tr}(\alpha_i\alpha_j) = 0$$

The reverse is trivial. □

REMARK 1.5: If L/K is separable then Tr is non-trivial. Since we are mainly interested in characteristic 0, we will always assume this.

LEMMA 1.6: Let $(\alpha_1, \ldots \alpha_n) = (\beta_1, \ldots, \beta_n)M$ for some $M \in K^{n\times n}$ and $\alpha_i, \beta_j \in L$. Then

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

PROOF. □

By the primitive element theorem in Galois theory, we have $L = K[\alpha]$ for some suitable α. Hence $L \cong K[t]/f$ for $f \in K[t]$ the minimal polynomial of α. In some suitable field Λ (eg. the algebraic closure of L)

$$f(t) = \prod(t - \alpha^{(i)})$$

This defines field embeddings

$$(.)^{(i)} : L \to \Lambda : \sum a_j\alpha^j \mapsto \sum a_i(\alpha^{(i)})^j$$

We $\beta \in L$, we call $\beta^{(i)}$ the conjugates of β. In general we will have $\beta^{(i)} \notin L$ however. (Frequently, in the literature, $\alpha = \alpha^{(1)}$)

LEMMA 1.7 (Vandermonde): Let $a_1, \ldots, a_n \in K$ be arbitrary. Let $M = (m_{i,j})_{i,j} \in K^{n\times n}$ be defined by $m_{i,j} := a_i^{j-1}$. Then $\det M = \prod_{i<j}(a_j - a_i)$

PROOF. Induction by n. Tedious, but easy. □

THEOREM 1.8: Let $\beta \in L$ be arbitrary. Then

(1) For the characteristic polynomial we have $f_\beta = \prod(t - \beta^{(i)})$
(2) $N_{L/K}(\beta) = \prod \beta^{(i)}$
(3) $\mathrm{Tr}(\beta) = \sum \beta^{(i)}$

Note, that this gives an algorithm to compute those quantities - if the conjugates are available.

PROOF. We fix a basis $1, \alpha, \ldots, \alpha^{n-1}$ for $L = K(\alpha)$ and compute the representation matrix M_β for this basis, thus

$$\beta(1, \ldots, \alpha^{n-1}) = M_\beta(1, \ldots, \alpha^{n-1})$$

Applying the conjugate map, we get

$$\beta^{(i)}(1, \ldots, (\alpha^{(i)})^{n-1}) M_\beta(1, \ldots, (\alpha^{(i)})^{n-1})$$

since $M_\beta \in K^{n\times n}$ it is invariant under conjugation. Now this clearly states that $(1, \ldots, (\alpha^{(i)})^{n-1})$ is an Eigenvector to the Eigenvalue $\beta^{(i)}$. Those Eigenvectors form the columns of a Vandermonde matrix, hence are linear independent. (The determinant of the Vandermonde matrix is non-zero since the conjugates of a primitive element are pairwise distinct as the definining polynomial is separable) If we transform M_β to this new basis, it becomes $\mathrm{diag}(\beta^{(1)}, \ldots, \beta^{(n)})$ and the statements follow. □

LEMMA 1.9: Let $\alpha_1, \ldots, \alpha_n \in L$ be arbitrary, then we have

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det((\alpha_i^{(j)})_{i,j})^2$$

PROOF. Let $A := (\alpha_i^{(j)})_{i,j}$. Then $A^t A = (\mathrm{Tr}(\alpha_i \alpha_j))_{i,j}$. □

Let $f \in K[t]$ be a monic polynomial, $f(t) = \prod(t - x_i)$ in some suitable splitting field. Then

$$\mathrm{disc}(f) := \prod_{i<j}(x_i - x_j)^2$$

is the discriminant of f. It is non-zero iff all roots are distinct.

LEMMA 1.10: Let $f \in K[t]$ be irreducible and monic, $L := K[t]/f$ and $\rho \in L$ be a root of f. Then

$$\mathrm{disc}(1, \rho, \ldots, \rho^{n-1}) = \mathrm{disc}\, f = (-1)^{\binom{n}{2}} N_{L/K}(f'(\rho))$$

PROOF. Using Vandermonde 1.7 again and 1.9:

$$\mathrm{disc}(f) = \prod_{i<j}(x_i - x_j)^2 = \det((x_i^{j-1})_{i,j})^2 = \mathrm{disc}(1, \rho, \ldots, \rho^{n-1})$$

Now, using $f(t) = \prod(t - \rho^{(i)})$ and hence $f'(t) = \sum_l \prod_{j\neq l}(t - \rho^{(j)})$

$$\begin{aligned} N(f'(\rho)) &= \prod f'(\rho)^{(i)} = \prod f'(\rho^{(i)}) \\ &= \prod_i \sum_l \prod_{j\neq l}(\rho^{(i)} - \rho^{(j)}) \\ &= \prod_i \prod_{j\neq i}(\rho^{(i)} - \rho^{(j)}) \end{aligned}$$

All that remains is to "sort" the factors to have $i < j$ - and that accounts for the additional term. □

REMARK 1.11: There exists some $\alpha \in L$ such that $\mathrm{Tr}_{L/K}(\alpha) \neq 0$ since $\mathrm{disc}(f) \neq 0$.

LEMMA 1.12: $\alpha_1, \ldots, \alpha_n \in L$ are K-linear indepdendent iff $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \neq 0$.

PROOF. In 1.4 we showed that if the α_i form a basis and if the trace is non-trivial, then $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \neq 0$ as well, so by 1.11, the first implication is complete.

Let now $\sum b_i \alpha_i = 0$ for some $c_i \in K$, i. e. the α_i be dependent. Then $\sum b_i \alpha_i^{(j)} = 0$ for all j, hence $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(\alpha_i^{(j)}) = 0$ and we're done. □

LEMMA 1.13: Let $L/E/K$ be a finite tower of fields (i. e. $[L : E] =: m$ and $[E : K] =: n$ are finite) and $\alpha \in L$. Then $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{E/K}(\mathrm{Tr}_{L/E}(\alpha))$ and $N_{L/K}(\alpha) = N_{E/K}(N_{L/E}(\alpha))$

PROOF. Let $L = K[\beta]$ and $E = K[\alpha]$. Then, in some suitable extension

$$f_{K,\beta} = m_{K,\beta} = \prod (t - \beta^{(i)})$$

To avoid confusion and to distinguish conjugates of E and L, we define maps $\varphi_{L,i} : L \to \Lambda : \beta \mapsto \beta^{(i)}$ Similarly, we define maps $\varphi_{E,i} : E \to \Lambda$. Now, obviously the restriction $\varphi_{L,i}|_E$ is $\varphi_{E,j}$ for some j. Let $A_j := \{i \mid \varphi_{L,i}|_E = \varphi_{E,j}\}$. This defines a partitioning of $\{1, \ldots, mn\}$. Now, for the characteristic polynomial f_α of $\alpha \in L$ we have by 1.2 and degree considerations $f_\alpha = m_\alpha^m$. Since $f_\alpha(t) = \prod(t - \varphi_{L,i}(\alpha)) = \prod(t - \varphi_{E,i}(\alpha))^m$ we see that all sets A_j have size m.

Let $g(t) := f_{E,\beta} \in E[t]$, then $g | f_{K,\beta} \in E[t]$ since β is a root of both and g is the minimal polynomial. Now $\varphi_{L,i}(g(\beta)) = (\varphi_{L,i}(g))(\varphi_{L,i}(\beta)$, and since $g \in E[t]$, we have $\varphi_{L,i}(g) = \varphi_{E,j}(g)$ for all $i \in A_j$, hence we have

$$\varphi_{E,j}(g)(t) = \prod_{i \in A_j} (t - \varphi_{L,i}(\beta))$$

and finally, since we have the partitioning,

$$f_{K,\beta} = \prod \varphi_{E,i}(g)$$

Now the statements for the norm and trace follow from here. □

2. Modules - Basics

Note, especially in the beginning, a ring here is not assumed to be commutative or unitary. However, the most important example and the key application for the semester is for R to be $\mathbb{Z}$ or rings derived from here (localisations, quotients, completions).

Also, due to the non-commutativity of the ring, we are going to mention left or right modules and ideals.

DEFINITION 1.14: Let R be a ring. A (left) *R-module* M is an Abelian group together with a operation: $\circ : R \times M \to M$ such that $(rs) \circ m = r \circ (s \circ m)$, $(r+s) \circ m = r \circ m + s \circ m$ and $r \circ (m+n) = r \circ m + r \circ n$.
M is called *unitary* if R contains a $1 \neq 0$ and if $1 \circ m = m$ holds for all $m \in M$.
A subset U of some R-module M is called *submodule* if

(1) U is a subgroup of M,
(2) $RU \subseteq U$.

Let M and N be two R-modules. A group homomorphism $\varphi \in \mathrm{Hom}(M,N)$ such that $\varphi(rm) = r\varphi(m)$ holds for all $r \in R$ and $m \in M$ is called an (R-)module homomorphism. We write $\varphi \in \mathrm{Hom}_R(M,N)$ in this case.

(To summarise: A module is a "vectorspace over a ring".)

For any module M the intersection of any number of submodules is again a submodule, therefore for any subset $A \subseteq M$ there exists a minimal submodule of M containing A.

DEFINITION 1.15: Let M be an R-module. For $A \subseteq M$ let $\langle A \rangle = \langle A \rangle_R$ be the minimal submodule of M containing A.
M is called *finitely generated* if there there is some $A \subseteq M$ such that $\#A < \infty$ and $M = \langle A \rangle$.

For unitary M we have

$$\langle A \rangle = \{ \sum_{\text{fin.}} r_a a \mid a \in A, r_a \in R \}.$$

In general

$$\langle A \rangle = \cap_{A \leq U \leq M} U.$$

DEFINITION 1.16: For a family $(M_i)_{i \in I}$ of submodules of M, we define

$$\sum_{i \in I} M_i := \underset{i \in I}{+} M_i := \langle \cup_{i \in I} M_i \rangle$$

the *inner sum* of M_i. If we have $M_i \cap \langle \cup_{i \neq j} M_j \rangle = \langle M_j \mid i \neq j \rangle = \{0\}$, then the *(inner) direct sum* is defined as

$$\dot{+}_{i \in I} M_i := \langle M_i \mid i \in I \rangle.$$

THEOREM 1.17: Let R be commutative and unitary, M be a finitely generated unitary R-module, $\mathfrak{a} \trianglelefteq R$ be an ideal $\varphi \in \mathrm{End}_R(M)$ with $\varphi(M) \subseteq \mathfrak{a}M$. Then there exists $a_i \in \mathfrak{a}$ such that

$$\varphi^n + \sum_{i=0}^{n-1} a_i \varphi^i = 0.$$

PROOF. Fix any x_i such that $\langle x_i \mid 1 \leq i \leq n\rangle = M$. From $\varphi(x_i) \in \mathfrak{a}M$, we see that there are $a_{i,j} \in \mathfrak{a}$ such that $\varphi(x_i) = \sum_{j=1}^n a_{i,j}x_j$. (Note: The $a_{i,j}$ are not unique!) $f := \det(x\,\mathrm{id} - (a_{i,j})_{i,j}) = x^n + \sum_{i=0}^{n-1} a_i x^i \in x^n + \mathfrak{a}[x]$ now satisfies $f(\varphi) = 0$. For $A := (\varphi\delta_{i,j} - a_{i,j})_{i,j} \in R[\varphi]^{n\times n}$ we have

$$A(x_1, \ldots, x_n)^t = (\varphi(x_i) - \sum_{j=1}^n a_{i,j}x_j)_i = 0.$$

Let now B be the adjoint matrix, $B := (b_{i,j})_{i,j}$ and $b_{i,j} := (-1)^{i+j}\det((a_{l,m})_{i\neq l, j\neq m})$. Then $BA = \det(A)\,\mathrm{id}$, and thus

$$BA(x_1, \ldots, x_n)^t = 0 = \det(A)(x_1, \ldots, x_n)^t,$$

hence $f(\varphi) = \det(A) = 0 \in \mathrm{End}_R(M)$. □

3. Integrality - Part 1

In this section, let Λ be some integral domain, $1_\Lambda \neq 0$ and $R \subseteq S \subseteq \Lambda$ unitary subrings. Typically, $\Lambda = L$ will be a number field, $R = \mathbb{Z}$ and S some ring inside L.

DEFINITION 1.18: $a \in \Lambda$ is called integral over R if there is some monic $f \in R[t]$ such that $f(a) = 0$. A ring S is called integral over R if all $a \in S$ are integral.

THEOREM 1.19 (Kronecker): Elements $\alpha_1, \ldots, \alpha_r \in \Lambda$ are integral over R iff $R[\alpha_1, \ldots, \alpha_r]$ is a finitely generated R-module, ie $R[\alpha_1, \ldots, \alpha_r] = \sum R\omega_i$. Here, the sum is not necessarily direct.

Note that $\mathbb{Z}[t]$ is not finitely generated as a $\mathbb{Z}$-module! (It is however finitely generated as a $\mathbb{Z}$-algebra)

PROOF. Assume first, that all the α_i are integral. We now proceed via induction. Since α_1 is integral, there is some monic $f_1 \in R[t]$ such that $f_1(\alpha_1) = 0$. Since f_1 is monic we get $\alpha_1^n = -\sum_{i=0}^{n-1} f_{1,i}\alpha_1^i$ for $n := \deg f_1$. Now clearly $R[\alpha_1] = \langle \alpha_1, \ldots, \alpha_1^{n-1} \rangle$ is finitely generated. For the induction, assume that $S := R[\alpha_1, \ldots, \alpha_r] = \langle 1, \omega_1, \ldots, \omega_s \rangle_R$ is finitely generated. Now, as above, we find a monic polynomial $f_{r+1} \in R[t]$ such that $f_{r+1}(\alpha_{r+1}) = 0$, hence, $\alpha_{r+1}^m = \sum_{i=0}^{m-1} f_{r+1,i}\alpha_{r+1}^i$ and $S[\alpha_{r+1}] = \langle 1, \alpha_{r+1}, \ldots, \alpha_{r+1} \rangle_S$ is finitely generated as an S-module. By induction now

$$S[\alpha_{r+1}] = \sum_i S\alpha_{r+1}^i = \sum_i (\sum_j R\omega_j)\alpha_{r+1}^i = \sum R\omega_j\alpha_{r+1}^i$$

hence we have finite generation again.

If $S := R[\alpha_1, \ldots \alpha_r]$ is finitely generated, then we can for any $u \in S$ use 1.17 and the map $S \to S : s \mapsto su$ to find a monic polynomial having u as a zero. □

COROLLARY 1.20: (1) For $\alpha_1, \ldots, \alpha_r$ integral over R, we have $R[\alpha_1, \ldots \alpha_r]$ is integral and, specifically
(2) For integral α and β, both $\alpha\beta$ and $\alpha + \beta$ are integral.

THEOREM 1.21: Λ integral over S and S integral over R, then Λ is integral over R as well.

PROOF. Let $x \in \Lambda$ be arbitrary. Then there is some $S[t] \ni f = \sum f_i t^i$ such that $f(x) = 0$, hence x is integral over $R[f_0, \ldots, f_n]$, and $f_i \in S$ are integral over R, thus by 1.19, $R[f_0, \ldots, f_n, x]$ is finitely generated and thus x is integral over R. □

DEFINITION 1.22: Define $\mathrm{IntCls}(R, \Lambda) := \{x \in \Lambda | x \text{ is integral over } R\}$ this is called the *integral closure* of R in Λ. R is called *integrally closed* in Λ iff $\mathrm{IntCls}(R, \Lambda) = R$.

REMARK 1.23: $\mathrm{IntCls}(R, \Lambda)$ is a ring.

LEMMA 1.24: $\mathrm{IntCls}(R, \Lambda)$ is integrally closed in Λ, i. e.

$$\mathrm{IntCls}(R, \Lambda) = \mathrm{IntCls}(\mathrm{IntCls}(R, \Lambda), \Lambda)$$

PROOF. By 1.21. □

THEOREM 1.25: Let $K = Q(R)$, the quotient field of the factorial ring (UFD) R (think $R = \mathbb{Z}$, $K = \mathbb{Q}$). Then R is integrally closed in K, i. e. $R = \mathrm{IntCls}(R, K)$.

PROOF. Let $\alpha \in K$ be integral over R. Then $\alpha = a/b$ for some a, $b \in R$, wlog a and b are coprime i. e. $\langle a, n\rangle = R$, and we have some $f \in R[t]$ monic, such that $f(\alpha) = 0$. So

$$(\frac{a}{b})^n + \sum_{i=0}^{n-1} f_i(\frac{a}{b})^i = 0$$

and

$$a^n + \sum f_i b^{n-i} a^i = 0$$

after clearing of denominators, thus $b|a^n$. R is a UFD, hence $\pi|a$ for all primes $\pi|b$, so $a/b \in R$ as required. □

From now on, we assume R to be integrally closed in $Q(R) = K$.

REMARK 1.26: $K \cap \mathrm{IntCls}(R, L) = R$

LEMMA 1.27: Let $\beta \in L$ be arbitrary, then $\beta = s/u$ for some $u \in R$ and $s \in \mathrm{IntCls}(R, L)$

PROOF. Let $m > 0$ be minimal such that 1, β, ..., β^m are K-linearly dependent (i. e. m is the degree of the minimal polynomial of β). Since $K = Q(R)$, we see that $\{\beta^i | 0 \leq i \leq m\}$ is also R-linearly dependent (by clearing denominators), hence

$$\sum a_i \beta^i = 0$$

for suitable $a_i \in R$. By the above $a_m \neq 0$ since m was minimal. Now it is easy to see that $a_m\beta \in \mathrm{IntCls}(R, L)$ as claimed: Multiplying by a_m^{m-1} we get

$$\sum_{i=0}^{m} a_i a_m^{m-i-1} (a_m\beta)^i = 0$$

hence $a_m\beta$ is a root of the monic polynomial

$$x^m + \sum_{i=0}^{m-1} a_i a_m^{m-i-1}$$

□

REMARK 1.28 (Symmetric Polynomials): Let $f \in K[t]$ be arbitrary monic. Then, in some suitable splitting field

$$f(t) = \prod (t - \lambda_i)$$

Expanding the product we get

$$f(t) = \prod (t - \lambda_i) = t^n + \sum (-1)^{n-i} \sigma_{n-i}(\lambda_1, \ldots, \lambda_n) t^i$$

for some $\sigma_i \in \mathbb{Z}[t_1, \ldots, t_n]$. In fact

$$\sigma_i = \sum_{1 \leq i_1 < \ldots < i_i \leq n} \prod_j t_{i_j}$$

The σ_i are called *elementary symmetric polynomials*. Since $f \in K[t]$, we see that $\sigma_i(\lambda_1, \ldots, \lambda_n) \in K$!

LEMMA 1.29: $\beta \in L$ is integral over R iff $m_\beta \in R[t]$ is monic where m_β denotes the minimal polynomial of β over K.

PROOF. If m_β is monic, clearly β is integral. Hence assume now β is integral. Then, by definition, we have some monic polynomial $f \in R[t]$ such that $f(\beta) = 0$, hence $m_\beta | f$ in $K[t]$. All that remains is to show $m_\beta \in R[t]$ (rather than $K[t]$). Let M be a splitting field for M. Then clearly, all roots of m_β are integral over R (as the roots of the same monic polynomial, namely f). By the theorem on symmetric polynomials, all the coefficients of m_β are polynomials in the roots, hence integral. Now since R is integrally closed, $m_\beta \in K[t] \cap \mathrm{IntCls}(R, L)[t] = R[t]$. □

The same proof also shows that for any finite extension, the characteristic polynomial of an integral element is integral. We also see, that here R does not need to be PID – it is sufficient to be integrally closed for the proof to work. For $\mathbb{Z}$, this is essentially the classical Gauss-Lemma.

COROLLARY 1.30: Let $\alpha \in \mathrm{IntCls}(R, L)$, then $N_{L/K}(\alpha)$, $\mathrm{Tr}_{L/K}(\alpha) \in R$

COROLLARY 1.31: Let $\alpha_i \in \mathrm{IntCls}(R, L)$ then $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \in R$

LEMMA 1.32: Let $\alpha \in \mathrm{IntCls}(R, L)$ then $\alpha | N(\alpha)$ in $R[\alpha]$.

PROOF. Let $f \in R[t]$ be the characteristic polynomial of α over L. Then, $f(t) = \sum_{i=0}^{n} f_i t^i$ with $f_n = 1$ and $f_0 = \pm N(\alpha)$, hence $0 = f(\alpha) = \alpha(\sum_{i=1}^{n} f_i \alpha^{i-1}) \pm N(\alpha)$ □

COROLLARY 1.33: $\varepsilon \in \mathrm{IntCls}(R, L)$ is a unit in $R[\varepsilon]$ iff $N(\varepsilon) \in R^\times$

Note: Since $R \subseteq \mathrm{IntCls}(R, L)$, we know that $\mathrm{IntCls}(R, L)$ is a R-module. Next we need to investigate this structure better.

LEMMA 1.34:

(1) There exists a K-basis for L contained in $\mathrm{IntCls}(R, L)$.
(2) Let $\omega_1, \ldots, \omega_n \in \mathrm{IntCls}(R, L)$ be any K-basis for L and $d := \mathrm{disc}(\omega_1, \ldots, \omega_n)$. Then $d\,\mathrm{IntCls}(R, L) \subseteq \sum R\omega_i$

PROOF. By 1.27, for any $\alpha \in L$ we have some $d_\alpha \in R$ such that $d_\alpha \alpha \in \mathrm{IntCls}(R, L)$, hence (1) follows by taking a common denominator.

Let now $(\omega_i)_i$ be any integral K-basis for L and $\alpha \in \mathrm{IntCls}(R, L)$ be arbitrary. Then $\alpha = \sum \alpha_i \omega_i$ for some $\alpha_i \in Q(R) = K$. Multiplying by ω_j we get $\omega_j \alpha = \sum \alpha_i \omega_j \omega_i$ and $\mathrm{Tr}(\omega_j \alpha) = \sum \alpha_i \,\mathrm{Tr}(\omega_i \omega_j)$. This shows

$$((\omega_i \omega_j)_{i,j} (\alpha_i)_i^t = (\mathrm{Tr}(\alpha \omega_j))_j^j$$

Cramer's rule now gives $d\alpha_i \in R$ since $\mathrm{Tr}(\alpha \omega_j) \in R$. □

What we would like to do now, is to show that the integral closure is a free R-module - however, that means we have to do modules first.

4. Free $\mathbb{Z}$-Modules

Let $(M_i)_{i\in I}$ be a family of R-modules (not submodules!), then we define in the usual way the (outer) *direct product* as

$$\prod_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i\}$$

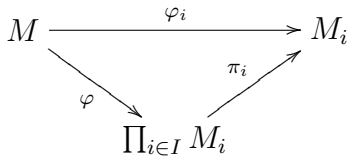
and the *direct sum* as

$$\oplus_{i\in I} M_i := \{x \in \prod_{i\in I} M_i \mid \text{only finitely many } m_i \neq 0\}.$$

Both are R-modules with the componentwise operation. They satisfy the universal property:

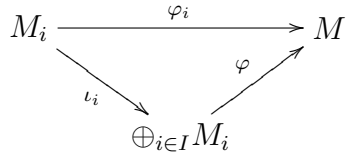
THEOREM 1.35: Let $(M_i)_{i\in I}$ be a family of R-modules.

(1) For every R-module M and every family $\varphi_i \in \mathrm{Hom}_R(M, M_i)$ of homomorphisms, there is exactly one $\varphi : M \to \prod_{i\in I} M_i$ such that the following diagram commutes for all $i \in I$:



The $\pi_i : \prod_{i\in I} M_i \to M_i : (m_i)_i \mapsto m_i$ are the canonical projections.

(2) For every R-module M and every family $\varphi_i \in \mathrm{Hom}_R(M_i, M)$ of maps there is exactly one $\varphi : \oplus_{i\in I} M_i \to M$ such that the following diagram commutes for all $i \in I$:



The $\iota : M_i \to \oplus_{i\in I} M_i : m_i \mapsto (m_j)_j$ such that $m_j = 0$ for $i \neq j$ are the canonical injections.

Note: For finite index sets, the direct product is the same as the direct sum.

LEMMA 1.36: Let $U \leq M$ be a submodule of the R-module M. Using $\alpha\circ(x+U) := \alpha x + U$ the quotient group M/U gets the structure of an R-module, the so called *quotient module*.

LEMMA 1.37: Let M, $\tilde{M}$ be two R-modules and $\varphi : M \to \tilde{M}$ an R-module homomorphism. Then

(1) $\mathrm{im}(\varphi) \cong M/\ker(\varphi)$,
(2) $(U+V)/U \cong V/(U\cap V)$ for submodules U, V of M,
(3) $M/V \cong (M/U)/(V/U)$ for $U \leq V \leq M$.

PROOF. As usual. □

DEFINITION 1.38: For $A \subseteq M$ is $\mathrm{Ann}(A) := \alpha(A) := \{r \in R \mid \forall m \in A : rm = 0\}$ the *annihilator* of A. If $\mathrm{Ann}(M) = \{0\}$ then M is called *faithful*. $m \in M$ is called *torsion element* or short *torsion* if $\mathrm{Ann}(m) \neq 0$. $\mathrm{Tor}(M) := \{m \in M \mid \mathrm{Ann}(m) \neq 0\}$. M is called *torsion module* or short *torsion* if $\mathrm{Tor}(M) = M$ holds, M is called *torsion free* if $\mathrm{Tor}(M) = 0$ holds.

REMARK 1.39:
(1) In general, $\mathrm{Tor}(M)$ is no submodule of M.
(2) $\mathrm{Ann}(A)$ is a (left) ideal of R.
(3) if $M \neq 0$ and $\mathrm{Tor}(M) = \{0\}$ then R is a domain (i. e. has no zero-divisors).

LEMMA 1.40: Let R be a domain and M an R-module. Then $\mathrm{Tor}(M)$ is a submodule and $M/\mathrm{Tor}(M)$ is torsion free.

DEFINITION 1.41: A finite subset $\{x_1, \ldots, x_n\}$ of an R-module M is called *R-free* (free or R-linear independent) if $\sum_{i=1}^{r} \alpha_i x_i = 0$ with $\alpha_1, \ldots, \alpha_r \in R$ always implies $\alpha_1 = \ldots = \alpha_r = 0$. An arbitrary subset $S \subseteq M$ is called free if all finite subsets of S are free.
$S \subseteq M$ is called a basis of M if S is free such that $\langle S \rangle = M$ holds. A module with basis is called a free module.

A free module with basis is almost the same as a vector space. Some common properties are listed in the following theorem.

THEOREM 1.42: Let $X \subseteq M$, M a unitary R-module. The following are equivalent:
(1) For every R-module N and every map $\varphi : X \to N$ exists exactly one homomorphism $\Phi : M \to N$ extending φ. (Definition of homomorphisms via the basis)
(2) The map $rx \mapsto r$ is an R-module isomorphism between Rx and R for every $x \in X$. Furthermore $M = \dot{+}_{x \in X} Rx$.
(3) M is free with basis X.
(4) Every $m \in M$ has a unique representation $m = \sum_{\text{fin.}} r_x x$.
(5) $M \cong \oplus_{x \in X} R$, where the isomorphism is given as $(r_x)_x \mapsto \sum r_x x$.

For finite set X, we see that M is free iff $M \cong R^X = R^{\#X}$.

EXAMPLE 1.43:
(1) $\emptyset$ is free.
(2) M free implies M torsion free. The reverse is in general wrong.
(3) Vectorspaces are free unitary modules over fields.
(4) Let K be a field, V a K-vectorspace. Then V is an $\mathrm{End}(V)$-module via $\varphi \circ v := \varphi(v)$.
(5) A normal number field with Galois group G is a $\mathbb{Z}[G]$ module.
(6) In any commutative domain R an ideal $\mathfrak{a} \subseteq R$ is a free R-module (it is always an R-module) iff $\mathfrak{a} = (a)$, i. e. if $\mathfrak{a}$ is principal. This can be wrong if R has zero-divisors.
(7) Let $R \subseteq S$ be a unitary ring extension. Then S is a unitary R-module.

THEOREM 1.44: Let M be a free $\mathbb{Z}$-module, then all bases have the same size, called the rank of M.

PROOF. By Theorem 1.42.5, $M \cong \mathbb{Z}^{X_1} \cong \mathbb{Z}^{X_2}$. Just looking at the additive group, $(\mathbb{Z}^{X_i}, +)$ we see that $\#X_1 = \#X_2$ neccessarily. (As a proof: $(\mathbb{Z}^n/2\mathbb{Z}^n, +) = (\mathbb{Z}/2\mathbb{Z}, +)^n$ so counting show this immediately.) □

EXAMPLE 1.45: In general, the previous theorem is wrong in the non-commutative setting. One can construct a ring R such that $R^n \cong R^m$ for all n and m.

THEOREM 1.46: Let M be a free $\mathbb{Z}$-module of rank n. Then every submodule $U \leq M$ is free of rank $m \leq n$.

PROOF. Via induction. $n = 0$ is trivial.

Let $n \geq 1$, x_i a basis for M, so $M = \dot{+}_{i=1}^{n} \mathbb{Z}x_i$,

$$\tilde{M} := \dot{+}_{i=1}^{n-1} \mathbb{Z}x_i \subseteq M$$

and $\varphi_n : M \to \mathbb{Z} : \sum a_i x_i \mapsto a_n \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$.

By induction hypothesis we have $\tilde{U} := U \cap \tilde{M}$ is free of rank $\leq n-1$. If $U = \tilde{U}$, then we're done. Otherwise set

$$\mathfrak{a} := \varphi_n(U)$$

$\mathfrak{a}$ is an submodule of $\mathbb{Z}$, it is an ideal $\neq \{0\}$ in $\mathbb{Z}$, so $\mathfrak{a} = \langle a_n \rangle$, fix now any $y \in \varphi_n^{-1}(a_n)$.

Aim: $U = \tilde{U} \dot{+} \mathbb{Z}y$. Let $x \in \tilde{U} \cap \mathbb{Z}y$ be arbitrary, then x has a unique representation $x = \sum_{i=1}^{n-1} \tilde{\alpha}_i x_i$. On the other hand, $x = \alpha \circ y$ for some $\alpha \in \mathbb{Z}$, thus $x = \sum_{i=1}^{n} \alpha\alpha_i x_i$ hence $\alpha\alpha_n = 0$ and $\alpha = 0$, since $\alpha_n \neq 0$ and $\mathbb{Z}$ domain, we see $x = 0$. Therefore $\tilde{U} \cap \mathbb{Z}y = \{0\}$.

Let $u \in U$ be arbitrary, $u = \sum_{i=1}^{n} \beta_i x_i$. We can find $\tilde{\beta} \in \mathbb{Z}$ such that $\beta_n = \tilde{\beta}\alpha_n$. Now

$$u - \tilde{\beta}y = \sum_{i=1}^{n} (\beta_i - \tilde{\beta}\alpha_i) x_i = \sum_{i=1}^{n-1} (\beta_i - \tilde{\beta}\alpha_i) x_i \in \tilde{M}$$

and $u - \tilde{\beta}y \in \tilde{U}$ since u, $y \in U$ implying $u \in \tilde{U} + \mathbb{Z}y$ and $U \subseteq \tilde{U} + \mathbb{Z}y$. Obviously $\tilde{U} + \mathbb{Z}y \subseteq U$. □

EXAMPLE 1.47: Let $R = \mathbb{Z}/4\mathbb{Z}$, then $\langle (1,2) \rangle \subseteq R^2$ is free (of rank 1 and basis $\{(1,2\})$, while $\langle (2,2) \rangle$ is not free $(2(2,2) = (0,0))$ So this gives an example of a non-free submodule of a free module.

THEOREM 1.48: Finitely generated torsion free $\mathbb{Z}$-modules are free.

PROOF. We have (from the finitely generation)

$$M = \sum_{i=1}^{n} \mathbb{Z}x_i.$$

Among the subsets of $\{x_1, \ldots, x_n\}$ choose a free one with maximally many elements. Wlog $\{x_1, \ldots, x_s\}$ is such a maximal subset. If $n = s$, we are done, thus assume $s < n$. For every $j \in \{s+1, \ldots, n\}$ exist α_j, $\alpha_{ji} \in \mathbb{Z}\,(1 \leq i \leq s), \alpha_j \neq 0$ such that

$$\alpha_j x_j = \sum_{i=1}^{s} \alpha_{j,i} x_i$$

thus $\alpha_j x_j \in F$ for $F = \sum_{i=1}^{s} \mathbb{Z}x_i$.

Set $\alpha = \prod_{i=s+1}^{n} \alpha_i$, then $\alpha \neq 0$ and $\alpha x \in F$ for all $x \in M$ or, $\alpha M \subseteq F \subseteq M$. By Theorem 1.46 is αM free of rank $\leq s$ and $\varphi : M \to \alpha \cdot M : x \mapsto \alpha \cdot x$ is an homomorphism which is trivally surjective and injective due to the torsion freeness of M. Finally $M \simeq \alpha M$ is then free of rank s. □

REMARK 1.49: $\mathbb{Q}$ is torsion free as a $\mathbb{Z}$-module, but not free.

THEOREM 1.50: Let M be a finitely generated $\mathbb{Z}$-module. Then we have $M = \operatorname{Tor}(M) \oplus F$ where F is free and $F \simeq M/\operatorname{Tor}(M)$.

PROOF. By 1.40 and 1.48, $M/\operatorname{Tor}(M)$ is free with basis B. Now we look at the canonical projection:

$$\varphi : M \to M/\operatorname{Tor}(M) : x \mapsto x + \operatorname{Tor}(M).$$

For every $b \in B$ fix some $m_b \in \varphi^{-1}(b)$. Set $F := \sum_{b\in B} \mathbb{Z}m_b$, so F is a free submodule of M with basis $\{m_b \mid b \in B\}$. We need to show $M = \operatorname{Tor}(M) \oplus F$. We have $F = \tau(M/\operatorname{Tor}(M))$ with the isomorphism

$$\tau : M/\operatorname{Tor}(M) \to F : \sum_{b\in B} \alpha_b b + \operatorname{Tor}(M) \mapsto \sum_{b\in B} \alpha_b m_b.$$

For $m \in M$ we have $m = \tau(\varphi(m)) + (m - \tau(\varphi(m))) \in F + \operatorname{Tor}(M)$. Let now $x \in F \cap \operatorname{Tor}(M)$ fixed, than we have $x = \tau(\tilde{m})$ for some $\tilde{m} \in M/\operatorname{Tor}(M/R)$ hence

$$0 = \varphi(x) = \varphi(\tau(\tilde{m})) = \tilde{m} \Rightarrow x = \tau(\tilde{m}) = 0$$

showing $F \cap \operatorname{Tor}(M) = \{0\}$. □

5. Integrality - Part 2

LEMMA 1.51: Every finitely generated $\mathrm{IntCls}(\mathbb{Z}, L)$-module $L \supseteq U \neq \{0\}$ is a free $\mathbb{Z}$-module of rank $n = [L : K]$.

PROOF. Let $\omega_1, \ldots, \omega_n \in \mathrm{IntCls}(\mathbb{Z}, L)$ be a $\mathbb{Q}$-basis for L, $d := \mathrm{disc}(\omega_1, \ldots, \omega_n)$ and $\mu_1, \ldots, \mu_r$ be the set of $\mathrm{IntCls}(\mathbb{Z}, L)$ generators for U. Then, since U is also an $\mathbb{Z}$-module, we can find some $a \in \mathbb{Z}$ such that $a\mu_i \in \mathrm{IntCls}(\mathbb{Z}, L)$ hence $aU \subseteq \mathrm{IntCls}(\mathbb{Z}, L)$. By 1.34 we see $daU \subseteq d\,\mathrm{IntCls}(\mathbb{Z}, L) \subseteq \sum \mathbb{Z}\omega_i =: M$. This immediately implies that daU and hence U are free $\mathbb{Z}$-modules of rank at most n since M is. On the other hand, assume wlog $\mu_1 \neq 0$ then $(\mu_1\omega_i)_i$ are clearly independent and contained in U, so U has rank n as required. □

Note: since $\mathrm{IntCls}(\mathbb{Z}, L)$ as an $\mathrm{IntCls}(\mathbb{Z}, L)$ module is generated by $\{1\}$ we conclude that $\mathrm{IntCls}(\mathbb{Z}, L)$ is indeed a free $\mathbb{Z}$-module of rank n. Similarly, any ideal $A \subseteq \mathrm{IntCls}(\mathbb{Z}, L)$ is also free of rank n as a $\mathbb{Z}$-submodule.

DEFINITION 1.52: Any $\mathbb{Z}$-basis for $\mathrm{IntCls}(\mathbb{Z}, L)$ is called an *integral basis* for L (and for $\mathrm{IntCls}(\mathbb{Z}, L)$).

DEFINITION 1.53: Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\Lambda)$ and assume $[L : K] < \infty$. Then

$$\mathcal{C}_{\Lambda/\mathbb{Z}} := \{x \in L | \operatorname{Tr}_{L/K}(x\Lambda) \subseteq \mathbb{Z}\}$$

is called the *co-different* of $\Lambda/\mathbb{Z}$.

LEMMA 1.54: Let

$$\mathcal{C}_{\mathrm{IntCls}(R,L)/\mathbb{Z}} = \mathcal{C} = \{x \in L \mid \operatorname{Tr}(x\,\mathrm{IntCls}(\mathbb{Z}, L)) \subseteq \mathbb{Z}\}$$

the co-different of $\mathrm{IntCls}(\mathbb{Z}, L)$ over $\mathbb{Z}$. Then $\mathcal{C}$ is a $\mathrm{IntCls}(\mathbb{Z}, L)$-module containing $\mathrm{IntCls}(\mathbb{Z}, L)$.

THEOREM 1.55: Assume $(\omega_i)_i$ is an integral basis for $\mathrm{IntCls}(\mathbb{Z}, L)$, ie $\mathrm{IntCls}(\mathbb{Z}, L) = \dot{+}\mathbb{Z}\omega_i$ and that ω_i^* is the trace-dual basis ($\operatorname{Tr}(\omega_i\omega_j^*) = \delta_{i,j}$). Then $\mathcal{C} = \dot{+}\mathbb{Z}\omega_j^*$.

PROOF. Let $a \in \mathcal{C}$ arbitrary, then $a = \sum a_i\omega_i^*$ with some $a_i \in \mathbb{Q}$. But then $a_i = \sum a_j \operatorname{Tr}(\omega_i\omega_j^*) = \operatorname{Tr}\omega_i \sum a_j\omega_j^* = \operatorname{Tr}(\omega_i a) \in \mathbb{Z}$.

Now, let $a = \sum a_i\omega_i^*$ with $a_i \in \mathbb{Z}$ and $b \in \mathrm{IntCls}(\mathbb{Z}, L)$ be arbitrary, so $b = \sum b_i\omega_i$, $b_i \in \mathbb{Z}$. But now

$$\operatorname{Tr}(ab) = \operatorname{Tr}(\sum a_j\omega_j^* b_i\omega_i) = \sum a_j b_i \operatorname{Tr}(\omega_i\omega_j^*) = \sum a_i b_i \in \mathbb{Z}$$

hence $a \in \mathcal{C}$. □

LEMMA 1.56: Let $f(t) := \prod_{i=1}^n (t - x_i) \in K[t]$ be squarefree and $f(0) \neq 0$.

(1) *Lagrange Interpolation*

$$\sum_{i=1}^n \frac{x_i^k f(t)}{f'(x_i)(t - x_i)} = \begin{cases} t^k & \text{for } 0 \leq k < n-1 \\ t^n - f(t) & \text{for } k = n-1 \end{cases}$$

(2) *Euler*

$$\sum_{i=1}^n \frac{x_i^{k-1}}{f'(x_i)} = \begin{cases} 0 & \text{for } 0 \leq k \leq n-2 \\ 1 & \text{for } k = n-1 \end{cases}$$

PROOF. Taylor expansion shows

$$f(t) = f(x + (t-x)) = f(x) + \sum_{i=1}^{\infty} \frac{(t-x)^i}{i!} f^{(i)}(x)$$

Thus $f(t)/(t-x_i) = f(x_i)/(t-x_i) + f'(x_i) + (t-x_i)(\ldots) = f'(x_i) + (t-x_i)(\ldots)$ and in particular

$$(\frac{x_i^{k+1} f(t)}{f'(x_i)(t-x_i)})(x_i) = x_i^{k+1}$$

Now, the rhs and the lhs are both polynomials in t of degree $< n$, hence they are uniquely defined by the n evaluations at the x_i.

The second statement follows from the 1st by taking $t = 0$ and dividing by $f(0)$. □

THEOREM 1.57: Let $S = \mathbb{Z}[\alpha]$ and $\mathcal{C}_{S/\mathbb{Z}} := \{x \in L \mid \mathrm{Tr}(xS) \subseteq \mathbb{Z}\}$ the codifferent of S. Then

$$\mathcal{C}_{S/\mathbb{Z}} = \frac{1}{f'(\alpha)} S$$

PROOF. Let $g(t) := f(t)/(t-\alpha)$. By Taylor, as above, $g(t) = \sum_{i=1}^{\infty} (t-\alpha)^i \frac{f^{(i)}(\alpha)}{i!}$ Since $(t^j)^{(i)}/i! = \binom{j}{i} t^{j-i} \in \mathbb{Z}[t]$, $g(t) \in S[t]$. Now

$$\frac{\alpha^j g(t)}{f'(\alpha)} = \frac{\alpha^j f(t)}{f'(\alpha)(t-\alpha)}$$

so by 1.56,

$$\mathrm{Tr}(\frac{\alpha^j g(t)}{f'(\alpha)}) = \begin{cases} t^j \\ t^n - f(t) \end{cases}$$

On the other hand,

$$\frac{\alpha^j g(t)}{f'(\alpha)} = \frac{\alpha^j \sum g_i t^i}{f'(\alpha)} = \sum t^i \frac{\alpha^j g_i}{f'\alpha}$$

Taking traces and coefficient comparison shows that $g_i/f'(\alpha)$ is the dual basis to α^i, hence the statement follows. □

DEFINITION 1.58: Any $\alpha \in \mathrm{IntCls}(\mathbb{Z}, \bar{Q})$ is called *algebraic integer*. For any finite extension $L/\mathbb{Q}$, we define $\mathbb{Z}_L = \mathcal{O}_L = \mathrm{IntCls}(\mathbb{Z}, L)$ the *maximal order* of L or *ring of integers*.
An *order* S of a number field L is any unitary subring $S \subseteq L$ that is finitely generated as an $\mathbb{Z}$-module and $Q(S) = L$.
Let $S = \sum \mathbb{Z}\omega_i$ be any order with $\mathbb{Z}$-basis ω_i. Then $\mathrm{disc}(S) := \mathrm{disc}(\omega_1, \ldots, \omega_n)$. We define $\mathrm{disc}\, L := d_L := \mathrm{disc}\, \mathbb{Z}_L$ and note that, in general, discriminants might only be defined up to squares of units. In $\mathbb{Z}$, the units are ± 1 thus the square is 1.

REMARK 1.59: Let $f \in \mathbb{Z}[t]$ be monic and irreducible. Set $L := \mathbb{Q}[\alpha] := \mathbb{Q}[t]/f$. Then

(1) $\alpha \in \mathbb{Z}_L$, hence $\mathbb{Z}[\alpha]$ is an order, the so called *equation order* of f.
(2) $\mathbb{Z}_L \cap \mathbb{Q} = Z$
(3) For all $\beta \in \mathbb{Z}_L$, f_β, $m_\beta \in \mathbb{Z}[t]$
(4) $\mathbb{Z}_L$ is a free $\mathbb{Z}$-module of rank n, hence an order.

(5) Let $\alpha \in \mathbb{Z}_L$ such that $\mathrm{disc}(\alpha)$ is square-free (up to units). Then $\mathbb{Z}[\alpha] = \mathbb{Z}_L$. Note: in general such an α does not exist.

LEMMA 1.60: Let $N \subseteq M$ be free $\mathbb{Z}$-modules of the same rank n. Then $(M : N) < \infty$.

PROOF. Let n_i be a $\mathbb{Z}$-basis for N and m_i for M. Then we can find $a_{i,j} \in \mathbb{Z}$ s.th. $n_i = \sum a_{i,j} m_j$ as $N \subseteq M$. For $B = (b_{i,j})$ the adjoint matrix (cofactor matrix) we have $B(a_{i,j}) = I_n \det(a_{i,j})$ so that for $d := \det(a_{i,j})$ we get $dm_j = \sum b_{i,j} n_i$, so $dM \subseteq N \subseteq M$ and $M : N \leq M : dM = d^n < \infty$. □

LEMMA 1.61: Let $\mathcal{O}$ be an order in L. Then

(1) $\mathbb{Z} \subseteq \mathcal{O}$
(2) Let $\{0\} \neq \mathfrak{a} \leq \mathcal{O}$ be an ideal. Then $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank n.
(3) $\mathcal{O}$ is noetherian
(4) $\mathcal{O}/\mathfrak{a}$ is a finite ring.
(5) Every non-zero prime ideal in $\mathcal{O}$ is maximal.

PROOF. (1) is clear.

(2): Let $a \in \mathfrak{a}$ be arbitrary and $\mathcal{O} = \dot{+} R\omega_i$. Then $a\omega_i \in \mathfrak{a}$ are independent since ω_i are independent. Thus $\mathfrak{a}$ is free as a submodule of a free module of rank n and contains a free subset of size n.

(3) clear using (2)

(4) by (2) and Lemma 1.60

(5) The quotient ring modulo a prime ideal is an integral domain. By (4) it is finite provided the ideal is non-trivial, thus by a fundamental result in algebra, a field, which forces the ideal to be maximal. □

CHAPTER 2

Computation of the Maximal Order

1. Theory: Round-2

Given $L := \mathbb{Q}[t]/f$ for some monic $f \in \mathbb{Z}[t]$, we saw that $\mathbb{Z}_L = \mathrm{IntCls}(\mathbb{Z}, L)$ is a free $\mathbb{Z}$-module of rank $n = \deg f = [L : \mathbb{Q}]$. The task now is to find an algorithm to compute an integral basis. Once this is done, we can compute with elements in $\mathbb{Z}_L$ using the $\mathbb{Z}$-module structure.

We start with trivial observations about the index:

REMARK 2.1: (1) Let $M_1 \leq M_2 \leq M_3$ be free of the same rank. Then $(M_3 : M_1) = (M_3 : M_2)(M_2 : M_1)$
(2) Let $M \leq N$ be free of the same rank. Then $(N : M)N \subseteq M$.

DEFINITION 2.2: Let $\mathcal{O}$ be an order in L, $0 \neq m \in \mathbb{Z}$. Define

$$\mathcal{O}_m := \{x \in \mathbb{Z}_L | \exists k : m^k x \in \mathcal{O}\}$$

the *m-maximal overorder* of $\mathcal{O}$. Typically, m will be a prime.

LEMMA 2.3: For any order $\mathcal{O}$ in L and any $0 \neq m \in \mathbb{Z}$ we have that
(1) $\mathcal{O}_m$ is an order, hence a free $\mathbb{Z}$-module of rank n
(2) $(\mathcal{O}_m : \mathcal{O}) | m^k$ and $\gcd((\mathbb{Z}_L : \mathcal{O}_m), m) = 1$
(3) for $m = p$ a prime, (2) simplifies to $(\mathcal{O}_p : \mathcal{O}) = p^k$ and $p \not| (\mathbb{Z}_L : \mathcal{O}_p)$.

PROOF. Since, as sets, $\mathcal{O} \subseteq \mathcal{O}_m \subseteq \mathbb{Z}_L$, all we have to show is that $\mathcal{O}_m$ is a ring. Let x, $y \in \mathcal{O}_m$. Then we have k, l such that $xm^k \in \mathcal{O}$ and $ym^l \in \mathcal{O}$, hence $(x + y)m^{\max(k,l)} \in \mathcal{O}$ and $xym^{l+k} \in \mathcal{O}$ and $\mathcal{O}_m$ is a ring, hence an order, so $\mathcal{O}_m = \sum R\omega_i$. For every ω_i we have a k_i such that $\omega_i m^{k_i} \in \mathcal{O}$. Setting $k := \max(k_i | i)$, we see that $m^k \omega_i \in \mathcal{O}$ for all i, hence $m^k \mathcal{O}_m \subseteq \mathcal{O} \subseteq \mathcal{O}_m$. Thus $(\mathcal{O}_m : \mathcal{O})(\mathcal{O} : m^k \mathcal{O}_m) = (\mathcal{O}_m : m^k \mathcal{O}_m) = m^{kn}$.

Suppose, $c := \gcd((\mathbb{Z}_L : \mathcal{O}_m), m) \neq 1$. Then we can find some $x \in \mathbb{Z}_L$ such that $cx \in \mathcal{O}_m$, hence $cm^k x \in \mathcal{O}$, but this implies $m^{k+1} x \in \mathcal{O}$ and thus $x \in \mathcal{O}_m$. □

COROLLARY 2.4: Let $\mathbb{Z}_L \supseteq S \supseteq \mathcal{O}_m \supseteq O$ be orders and $m \in \mathbb{Z}$. Then $\gcd((\mathbb{Z}_L : S), m) = \gcd((S : \mathcal{O}_m), m) = 1$

LEMMA 2.5: Let $\mathcal{O} \subseteq S_1$, $S_2 \subset L$ be orders such that $\gcd((S_1 : \mathcal{O}), (S_2 : \mathcal{O})) = 1$. Then $S_1 + S_2$ is an order as well. Here, the sum is taken as $\mathbb{Z}$-modules.

PROOF. Let $p = (S_1 : \mathcal{O})$ and $q = (S_2 : \mathcal{O})$. Then $1 = ep + fq$. We need to show that $S_1 + S_2$ is a ring. Let $a, b \in S_1$ and $u, v \in S_2$ be arbitrary, so $a + u$ and $b + v$ are arbitrary elements in $S_1 + S_2$. Now

$$\begin{aligned}(a+u)(b+v) &= ab + uv + av + bu \\ &= ab + uv + av(ep+fq) + bu(ep+fq) \\ &= \underbrace{ab}_{\in S_1} + \underbrace{uv}_{S_2} + \underbrace{(ap)ve}_{\in \mathcal{O}S_2R} + \underbrace{af(qv)}_{S_2R\mathcal{O}} + \underbrace{(pb)ue}_{\mathcal{O}S_2R} + \underbrace{bf(qu)}_{} + S_1R\mathcal{O} \\ &\in S_1 + S_2\end{aligned}$$

□

Note: this lemma is wrong in general if the indices are not coprime.

LEMMA 2.6: Let $p, q \in \mathbb{Z}$ be coprime (not neccessarily prime), $\mathcal{O} \subset L$ an order. Then $\mathcal{O}_p + \mathcal{O}_q = \mathcal{O}_{pq}$.

PROOF. By 2.5, $\mathcal{O}_p + \mathcal{O}_q$ is an order.

Let now $x \in \mathcal{O}_{pq}$, then we can find k such that $(pq)^k x \in \mathcal{O}$, so $q^k x \in \mathcal{O}_p$ and $p^k x \in \mathcal{O}_q$. From $1 = ep^k + fq^k$ we see $x = x(ep^k + fq^k) = e(p^k x) + f(q^k x) \in \mathcal{O}_p + \mathcal{O}_q$ as required. □

COROLLARY 2.7: Let $d := \operatorname{disc}(\mathcal{O})$, then $\mathbb{Z}_L = \sum_{p^2|d} \mathcal{O}_p$ where the sum runs over all prime divisors of d.

PROOF. Let $S := \sum_{p^2|d} \mathcal{O}_p$, then this is an order by 2.5. Clearly, $S \subseteq \mathbb{Z}_L$ and, since all are orders, they are $\mathbb{Z}$-modules of full rank as well. Let $\omega \in \mathbb{Z}_L \setminus S$ be arbitrary then there is some $\mu \in R$ such that $\mu\omega \in S$. Since μ is not a unit, we can find a prime p such that $p|\mu$ thus $p|(S[\omega] : S)$, so $p^2| \operatorname{disc} S | \operatorname{disc} \mathcal{O}$. But this contradicts S being p-maximal by 2.6 □

So, the aim is to find (a basis for) $\mathcal{O}_p$ for a prime p.

LEMMA 2.8: Let Λ be a commutative ring and $S \subseteq \Lambda$ a multiplicative semigroup (i. e. for $u, v \in S$, we have $uv \in S$ as well). Set $\mathcal{M} := \{\mathfrak{a} \leq \Lambda | \mathfrak{a} \cap S \subseteq \{0\}\}$. Then $\mathcal{M}$ has a maximal element $\mathfrak{p}$ which is a prime ideal.

PROOF. Since $\mathcal{M}$ is non-empty ($\{0\} \in \mathcal{M}$) and inductively ordered, by Zorn's lemma there is a maximal element $\mathfrak{p}$ in $\mathcal{M}$. Let now $a, b \in \Lambda$ such that $ab \in \mathfrak{p}$. Assuming $a, b \notin \mathfrak{p}$ we get $(a\Lambda + \mathfrak{p}) \cap S \neq \emptyset \neq (b\Lambda + \mathfrak{p}) \cap S$ since $\mathfrak{p}$ was maximal. But now we find $s_1, s_2 \in S$, $c_1, c_2 \in \Lambda$ and $p_1, p_2 \in \mathfrak{p}$ such that $s_1 = ac_1 + p_1$ and similar for b.

$$S \ni s_1 s_2 = (ac_1 + p_1)(bc_2 + p_2) = \underbrace{ab}_{\in \mathfrak{p}} c_1c_2 + p_1bc_2 + p_2ac_1 + p_1p_2 \in \mathfrak{p}$$

which is absurd. So either a or b has to be in $\mathfrak{p}$, so $\mathfrak{p}$ is prime. □

LEMMA 2.9: Let Λ be commutative and unitary, then $x \in \Lambda$ is *nilpotent* (i. e. $\exists k : x^k = 0$) iff $x \in \cap_{\mathfrak{p} \leq \Lambda} \mathfrak{p}$ where the intersection runs over all prime ideals.

PROOF. Assume x nilpotent. Find the minimal k such that $x^k = 0$, then clearly $x^{k-1}x = 0 \in \mathfrak{p}$ for any prime ideal $\mathfrak{p}$. By induction thus $x \in \mathfrak{p}$.

Assume now $x \in \cap\mathfrak{p}$ and $x^k \neq 0$ for all k. Set $S := \{x^k | k > 0\}$, this is clearly a multiplicative semigroup, thus by 2.8 there is a prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \cap S = \emptyset$, however, since $x \in S$ and $x \in \mathfrak{p}$ this is a contradiction. □

LEMMA 2.10: Let Λ be commutative and unitary and $\mathfrak{a} \leq \Lambda$ an ideal. Then $\sqrt{\mathfrak{a}} := \{x \in \Lambda \mid \exists k : x^k \in \mathfrak{a}\}$ is an ideal in Λ as well, the so called *radical* of $\mathfrak{a}$.

PROOF. Since $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$, the set is non-empty. Let x, $y \in \sqrt{\mathfrak{a}}$, then we can find k, l such that x^k, $y^l \in \mathfrak{a}$. Set $r := k + l$

$$(x+y)^r = \sum \binom{r}{i} x^i y^{k+l-i}$$

and either $i \geq k$ and $x^i \in \mathfrak{a}$ or $k+l-i \geq l$ and $y^{k+l-i} \in \mathfrak{a}$ so all terms are in $\mathfrak{a}$, hence $x + y \in \sqrt{\mathfrak{a}}$. Finally, $r \in \Lambda$, then $(rx)^k = r^k x^k \in \mathfrak{a}$, so $rx \in \sqrt{\mathfrak{a}}$ as required. □

Note (reminder): Let R be a commutative and unitary ring (just to be safe), $\mathfrak{a}$ an ideal in R and $\varphi : R \to R/\mathfrak{a}$ the canonical projection. For any ideal $\mathfrak{b} < R$ clearly $\varphi(\mathfrak{b})$ is an ideal in $R/\mathfrak{a}$. Furthermore $\varphi(\mathfrak{b})$ is maximal (prime) iff $\mathfrak{b}$ is maximal (prime) and $\mathfrak{a} \subseteq \mathfrak{b}$. This correspondence is $1-1$.

LEMMA 2.11: Let Λ be commutative and unitary, $\mathfrak{a} \leq \Lambda$ an ideal and $x \in \Lambda$. Then $x \in \sqrt{\mathfrak{a}}$ iff $x \in \cap\{\mathfrak{p} \supseteq \mathfrak{a} \mid \mathfrak{p} \text{ is a prime ideal}\}$.

PROOF. Let $\varphi : \Lambda \to \Lambda/\mathfrak{a}$ be the canonical projection. Then $x \in \sqrt{\mathfrak{a}}$ iff $x^k \in \mathfrak{a}$ iff $0 = \varphi(x^k) = \varphi(x)^k$ iff $\varphi(x)$ is nilpotent in $\Lambda/\mathfrak{a}$. By 2.9, this holds iff $\varphi(x) \in \mathfrak{p}+\mathfrak{a}$, but the prime ideals in $\Lambda/\mathfrak{a}$ are in one-to-one correspondence to those in Λ containing $\mathfrak{a}$. □

Note (reminder): Let R be commutative and unitary, $\mathfrak{p}_i$ be pairwise co-maximal ideals, then the Chinese remainder theorem shows

$$R/\cap\mathfrak{p}_i = \sum R/\mathfrak{p}_i$$

and $\cap\mathfrak{p}_i = \prod \mathfrak{p}_i$. In particular, this version works for rings that are not PID (in contrast to AGS).

THEOREM 2.12: Let $p \in \mathbb{Z}$ be prime and $\mathcal{O} \subseteq L$ an order, then $\sqrt{p\mathcal{O}}$ is the intersection of all maximal ideals of $\mathcal{O}$ containing p. This are at most n ideals and $(\sqrt{p\mathcal{O}})^n \subseteq p\mathcal{O}$.

PROOF. The 1st part is clear: in $\mathcal{O}$ all (non-trivial) prime ideals are maximal so this follows from 2.11. Let $(\mathfrak{p}_i)_i$ the maximal ideals containing p. Since different maximal ideals are co-maximal as well, $\cap\mathfrak{p}_i = \prod \mathfrak{p}_i$ and we can form the chain

$$\mathcal{O} \supseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_1\mathfrak{p}_2 \supseteq \prod \mathfrak{p}_i \supseteq \ldots \supseteq p\mathcal{O}$$

The CRT shows $\mathcal{O}/\prod_{i=1}^{j} \mathfrak{p}_i = \dot{+}\mathcal{O}/\mathfrak{p}_i$, hence all the ideal-inclusions are proper. Since the index $(\mathbb{Z}^n \cong \mathcal{O} : p\mathcal{O} \cong (p\mathbb{Z})^n) = p^n$ we can use 2.1 to see $r \leq n$ since $(\prod_{i=1}^{j} \mathfrak{p}_i : \prod_{i=1}^{j+1} \mathfrak{p}_i)|p^n = (\mathcal{O} : p\mathcal{O})$. As p was prime, there can be at most n steps of index p.

Now define $\mathfrak{a}_i := (\sqrt{p\mathcal{O}})^i$ then,

$$\mathcal{O} \supseteq \mathfrak{a}_1 \supseteq \ldots \supseteq \mathfrak{a}_r \ldots \supseteq p\mathcal{O}$$

hence since $(\mathcal{O} : p\mathcal{O}) = p^n$, $(\mathfrak{a}_i : \mathfrak{a}_{i+1}) = p^?$ and there can be at most n non-trivial steps in the chain. If, at any step, we have $\mathfrak{a}_i = \mathfrak{a}_{i+1}$, then induction shows immediately $\mathfrak{a}_i = \mathfrak{a}_{i+k}$ for all k, hence the chain is stationary after n steps at most.

It remains to show $\mathfrak{a}_n = p\mathcal{O}$. From $\mathbb{Z}/p$ is finite, we see that $\mathcal{O}/p\mathcal{O}$ is finite as well. Since for any $y \in \sqrt{p\mathcal{O}}$ we have an $k > 0$ such that $y^k \in p\mathcal{O}$, and since $\mathcal{O}/p\mathcal{O}$ thus $\sqrt{p\mathcal{O}}/p\mathcal{O}$ is finite, we have a single $k > 0$ such that $y^k \in p\mathcal{O}$ for all $y \in \sqrt{p\mathcal{O}}$. Now an element $x \in (\sqrt{p\mathcal{O}})^l$ is of the form

$$x = \sum_{\text{fin.}} \prod_{i=1}^{l} x_i$$

Now, if $l >> 0$ is large enough, each such products will have repetitions - at least one x_i will occur with multiplicity $\geq k$, and $x_i^n \in p\mathcal{O}$, hence $x \in p\mathcal{O}$ as required. □

For the case of infinite quotients, we will use a different characterisation of the radical. We note that 2.12 actually gives an algorithm to compute the radical (which we will study shortly).

DEFINITION 2.13: Define $T_p := \{x \in \mathcal{O} \mid \mathrm{Tr}(x\mathcal{O}) \subseteq p\mathbb{Z}\}$ the *trace-radical*.

THEOREM 2.14 (Newton-identities): Let $\sigma_i \in \mathbb{Z}[t_1, \ldots, t_n]$ the elementary symmetric polynomials and $p_i := \sum_{j=1}^n t_j^i$ the *power-sums*. Then we have the following identities:

$$k\sigma_k = \sum_{i=1}^{k} (-1)^{i-1} \sigma_{k-i} p_i$$

This allows to recursively compute the σ_i from the p_i and vice-versa.

THEOREM 2.15: Assuming that $i = 1, \ldots, n$ can be inverted in $\mathbb{Z}/p$, we have $T_p = \sqrt{p\mathcal{O}}$

In particular for $p > n$ this will give an alternate algorithm to compute the radical.

PROOF. In 2.11 we showed that $\sqrt{p\mathcal{O}} = \cap\mathfrak{p}$ where $\mathfrak{p}$ runs over all prime ideals containing p. Let $\mathfrak{p}$ any such prime, Γ/K the normal closure of L/K and $s_i \in \mathrm{Aut}(\Gamma, K)$ such that the $s_i|L$ are pairwise different (so the s_i form a complete set of representatives for $\mathrm{Aut}(\Gamma/K)/\mathrm{Fix}(L)$ or a complete set of embeddings $L \to \Gamma$). Finally, $\mathfrak{q} \leq \mathbb{Z}_\Gamma$ should be a prime containing $\mathfrak{p}$. Now, let $x \in \sqrt{p\mathcal{O}}$ and $y \in \mathcal{O}$ arbitrary, then $xy \in \sqrt{p\mathcal{O}} \subseteq \mathfrak{p} \subseteq \mathfrak{q}$. So $\mathrm{Tr}(xy) = \sum s_i(xy) \in \sum s_i\mathfrak{q}$ Since also $\mathrm{Tr}(xy) \in R$ (x and y are integral), $\mathrm{Tr}(xy) \in \sum s_i\mathfrak{q} \cap R = pR$, showing $\sqrt{p\mathcal{O}} \subseteq T_p$.

Let now $x \in T_p$, then for all $y \in \mathcal{O}$ we have $\mathrm{Tr}(xy) \in pR$ thus $\mathrm{Tr}(x^k) \in pR$ for all $k > 0$. Now, let $m(t) = \prod(t - s_i(x))$ be the characteristic polynomial of x. Then 1.28 shows that the coefficients of m are just the elementary symmetric polynomials evaluated at the roots $s_i(x)$. Now, 2.14 shows that the elementary symmetric polynomials can be expressed through the power-sums, provided we can divide by $i = 1, \ldots, n$. Now $t_k(s_1(x), \ldots, s_n(x)) = \sum(s_i(x))^k = \sum s_i(x^k) = \mathrm{Tr}(x^k) \in pR$, hence all coefficients of m barring the leading coefficient, are in pR, hence $x^n = -\sum_{i=0}^{n-1} m_i x^i \in p\mathcal{O}$, showing $x \in \sqrt{p\mathcal{O}}$. □

DEFINITION 2.16: Let $\mathfrak{a}$, $\mathfrak{b} \leq \Lambda$ ideals. Then

$$[\mathfrak{a}/\mathfrak{b}] := \{x \in L \mid x\mathfrak{b} \subseteq \mathfrak{a}\} = \mathrm{Hom}(\mathfrak{b}, \mathfrak{a})$$

this is quite similar to the "colon ideal" in commutative algebra:

$$\mathfrak{a} : \mathfrak{b} := \{x \in \Lambda \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$$

In particular,

$$[\mathfrak{a}/\mathfrak{a}] = \mathrm{End}(\mathfrak{a})$$

is called the *ring of multipliers* of $\mathfrak{a}$.

LEMMA 2.17: If $\mathfrak{a} \leq \mathcal{O}$ is an ideal, then $[\mathfrak{a}/\mathfrak{a}]$ is an order containg $\mathcal{O}$

PROOF. Let x, $y \in [\mathfrak{a}/\mathfrak{a}]$, so $x\mathfrak{a}$, $y\mathfrak{a} \subseteq \mathfrak{a}$ hence $(xy)\mathfrak{a} \subseteq x\mathfrak{a} \subseteq \mathfrak{a}$ and $(x+y)\mathfrak{a} \subseteq x\mathfrak{a} + y\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{a} = \mathfrak{a}$. From $1 \in \mathcal{O}$ and $\mathcal{O}\mathfrak{a} \subseteq \mathfrak{a}$, we see $1 \in \mathcal{O} \subseteq [\mathfrak{a}/\mathfrak{a}]$.

To show that we have an order, we need to show finite generation. Clearly, for $N := (\mathcal{O} : \mathfrak{a})$ we have $Nx \in \mathfrak{a}$ for all $x \in \mathcal{O}$, in particular, $N = N1 \in \mathfrak{a}$. Now

$$[\mathfrak{a}/\mathfrak{a}] = \{x \in L \mid x\mathfrak{a} \subseteq \mathfrak{a}\} \subseteq \{x \in L \mid Nx \in \mathfrak{a}\} \subseteq \{x \in L \mid Nx \in \mathcal{O}\} = \frac{1}{N}\mathcal{O}$$

shows that $[\mathfrak{a}/\mathfrak{a}]$ is free as a submodule of a free module and has full rank, since it contains $\mathcal{O}$. □

LEMMA 2.18: $([\sqrt{m\mathcal{O}}/\sqrt{m\mathcal{O}}] : \mathcal{O}) | m^k$ for some k.

PROOF. We have

$$\begin{aligned}
[\sqrt{p\mathcal{O}}/\sqrt{p\mathcal{O}}] &= \{x \in L \mid x\sqrt{m\mathcal{O}} \subseteq \sqrt{m\mathcal{O}}\} \\
&\subseteq \{x \in L \mid x\sqrt{m\mathcal{O}} \subseteq \mathcal{O}\} \\
&\subseteq \{x \in L \mid xm \in \mathcal{O}\} = \frac{1}{m}\mathcal{O}
\end{aligned}$$

So, $\mathcal{O} \subseteq [\sqrt{p\mathcal{O}}/\sqrt{p\mathcal{O}}] \subseteq 1/m\mathcal{O}$, hence the statement about the index follows. □

THEOREM 2.19 (Local-Maximality): We have $\mathcal{O} = \mathcal{O}_p$ iff $\mathcal{O} = [\sqrt{p\mathcal{O}}/\sqrt{p\mathcal{O}}]$ for p a prime in R.

PROOF. By the previous lemma, 2.18, we have

$$\mathcal{O} \subseteq [\sqrt{p\mathcal{O}}/\sqrt{p\mathcal{O}}] \subseteq \mathcal{O}_p$$

Now, we want to show the following:

$$\mathcal{O} \subset \mathcal{O}_p \text{ implies } \mathcal{O} \subset [\sqrt{p\mathcal{O}}/\sqrt{p\mathcal{O}}]$$

By 2.12, we know that $(\sqrt{p\mathcal{O}})^n \subseteq p\mathcal{O}$, furthermore, for k large enough $p^k\mathcal{O}_p \subseteq p\mathcal{O}$ since $(\mathcal{O}_p : \mathcal{O}) = p^?$, so

$$(\sqrt{p\mathcal{O}})^{nk}\mathcal{O}_p \subseteq (p\mathcal{O})^k\mathcal{O}_p \subseteq (p^k\mathcal{O}_p) \subseteq p\mathcal{O} \subseteq \sqrt{p\mathcal{O}}$$

Now, let μ be minimal such that $(\sqrt{p\mathcal{O}})^\mu\mathcal{O}_p \subseteq \sqrt{p\mathcal{O}}$. If $\mu = 1$, then, by definition, $\mathcal{O}_p \subseteq [\ldots]$ and we're done. So, assume $\mu > 1$ and choose $x \in (\sqrt{p\mathcal{O}})^{\mu-1}\mathcal{O}_p \setminus \sqrt{p\mathcal{O}}$. Then $x\sqrt{p\mathcal{O}} \subseteq \sqrt{p\mathcal{O}}$, hence $x \in [\ldots]$. Furthermore, $x^2 \in (\sqrt{p\mathcal{O}})^{2\mu-2}\mathcal{O}_p \subseteq (\sqrt{p\mathcal{O}})^\mu\mathcal{O}_p \subseteq \sqrt{p\mathcal{O}}$. But his now shows that $x \notin \mathcal{O}$, since clearly $(\sqrt{p\mathcal{O}})^\mu\mathcal{O} \subseteq (\sqrt{p\mathcal{O}})^\mu \subseteq \sqrt{p\mathcal{O}}$ for all μ. Since x was in the ring of multipliers, we are done. □

We can summarise the theory into the following algorithm to, in principle, compute the maximal order.

ALGORITHM 2.20 (Round-2):

Input: some order $\mathcal{O} \subseteq L$
Output: $\mathbb{Z}_L$
1: compute $d := \operatorname{disc} \mathcal{O}$
2: for all p sth. $p^2|d$ do
3: $S := \mathcal{O}$
4: $T := [\sqrt{pS}/\sqrt{pS}]$
5: if $S = T$ then $\mathcal{O}_p := S$, else $S := T$, and go to 4
6: $\mathbb{Z}_L := \sum \mathcal{O}_p$

But now we'll have to look at some of the details of the algorithm.

2. Number Fields, Constructively

In order to discuss algorithms, we have to specify and fix representations. Let $L/\mathbb{Q}$ be a number field as a finite extension. By the primitive element theorem, $L = \mathbb{Q}[t]/f$ for some irreducible $f \in \mathbb{Q}[t]$. Let us now fix such an f.

Elements in L can now be represented as polynomials $\alpha \in \mathbb{Q}[t]$ of degree $\alpha < n = \deg f$. However, for efficiency, we usually choose to represent them as $1/d\beta$ and $\beta \in \mathbb{Z}[t]$. Using this representation, we can study the costs of basic operations: $\pm$ is just addition/ subtraction of polynomials, hence $O(n)$, linear in the degree (though be careful with denominators and coefficient explosion!) Multiplication will require a reduction (division) after the polynomial multiplication. Using "normal" multiplication/ long divsion, this will take $O(n^2)$ operations, using asymptotically fast techniques, this can drop to $O(n \log n)$. Division/ inversion can be done using the extended gcd algorithm, computing $1 = \gcd(\alpha, f) = e\alpha + gf$, which requires, classically, $O(n^2)$ operations or $O(n \log n)$ in the fast case. However, in general, the size of α^{-1} is n times the size of α. Norms can be computed using resultants, also in time $O(n^2)$, $O(n \log n)$ res. This is all still subject of active research. We employ

- (x)gcd algorithms
- sub-resultants
- modular methods
- p-adic lifting approaches
- fft/ dft
- power series with pre-computed inverses

It should be noted, that there are other representations as well, better suited for some applications then others. E.g. polynomials of degree $< 2n$ are uniquely defined by their values at $2n$ points. This allows for multiplication (without reduction) in time $O(n)$, reduction via matrix operations, can be achieved in $O(n^2)$ yielding the same complexity for the total operation as above. However, for the evaluation of scalar products, only one reduction is required.

The (potential) coefficient explosion in particular of the denominators is frequently no problem as the elements will be mostly in $\mathbb{Z}_L$ which means a bounded denominator.

We could also represent elements by their representation matrix, which requires n^2 coefficients rather than n or $2n$. However, to compute $\alpha\beta$ given M_β takes only n^2 operations, which is faster than the classical $O(n^2)$ of above. The representation matrix for the power-basis $(\alpha^i)_i$) can be computed using $O(n^2)$ operations: repeatedly multiplying by α and reducing with the polynomial. Division using representation matrices can be done using linear algebra, but here are the costs $O(n^3)$, dropping to $O(n^\omega)$ for fast matrix multiplication techniques.

Lastly, we can represent elements by their real or complex conjugates. This allows all basic operations to be performed in $O(n)$ - but the numerical problems make this not useful directly. By choosing a "different complex field", and omitting divisions the numerical problems can be avoided, but now one has a representation for elements of bounded "size" only. Aside from the numerical problems, we can convert between those and other representations using matrix-vector multiplication in $O(n^2)$ operations.

Elements or orders will be represented by their coefficients wrt a fixed basis $(\omega_i)_i$, so $\sum a_i\omega_i = (a_i)_i$ will be a "generic" element. We can of course extend this to field elements by allowing rational coefficients or a denominator. Mostly, we can also allow arbitrary field bases instead of order bases. To add/subtract elements is straighforward, however, multiplication is more involved:

$$(\sum a_i\omega_i)(\sum b_j\omega_j) = \sum a_ib_j\omega_i\omega_j = \sum a_ib_j(\sum \Gamma_{i,j,k}\omega_k),$$

where the $\Gamma_k \in \mathbb{Q}$ (or $\mathbb{Z}$ if we have an order basis) are the *structure constants*, defining the products of the basis elements. Since multiplication need 3 nested loops, it is easy to see, that the costs are $O(n^3)$ - however, this is not the full truth. The n^3 multiplications can be grouped into n^2 coefficient multiplication a_ib_j. Asymptotically, for large coefficients, those are the expensive ones. The structure constants are fixed and the remaining multiplications are multiplcations of large numbers a_ib_j times small ones $\Gamma_{i,j,k}$. Furthermore, by writing the basis ω_i in terms of any primitive element, we can change the basis into a good basis for multiplication in n^2 operations, multiply using polynomials, in $O(n^2)$ operations and change back, giving a total of $O(n^2)$ again.

The $\Gamma_{i,j,k}$ can be seen as the representation matrices of the basis elements themselves, hence individual representation matrices can be obtained as linear combinations in time $O(n^3)$. Once the matrices are known, a single product will only take $O(n^2)$ operations. Inversion and division can be handled via linear equation solving, again using $O(n^3)$ operations.

There are more and other representations suggested and even used, eg. the *multivariate representation* where the number field is represented as a quotient of a multivariate polynomial ring modulo a maximal ideal. For certain applications, this is far superior over the primitive element representation, however, in general this is slower.

Also, this "discussion" was counting algebraic operations only, thus ignoring the coefficient size or precision completely. In practice, the "best" representation depends on the actual problem and its constraints. However, so far, asymptotically the best generic representation is using primitive elements - if a primitive can be found easily.

THEOREM 2.21 (Sonn-Zassenhaus): Let L/K be a finite extension with basis b_1, ..., b_n. Then L/K admits a primitive element iff there are $e_i \in \{0, 1\}$ such that $\sum e_i b_i$ is primitive.

Since, in our situation in characteristic 0, we always have a primitive element, this gives a straight-forward (if possibly slow) algorithm to find a primitive element given a basis.

Ideals can be presented via a $\mathbb{Z}$-basis, using the structure as free $\mathbb{Z}$-modules. We'll come back to this later when we have to use more ideal operations. Here, the basis will be fully sufficient.

3. Algorithms for ℤ-modules

DEFINITION 2.22: Let R be commutative and unitary and $n \in \mathbb{N}$. The invertible matrices $U \in R^{n\times n}$ are called *unimodular*. $\mathrm{GL}(n, R)$ is the set of all unimodular matrices.

In the following algorithms, we will have to work not only over $R = \mathbb{Z}$, but also over $R = \mathbb{Z}/d\mathbb{Z}$ for various d. This will be neccessary for efficiency, in particular it automatically avoid *coefficient swell*, the phenomenon that, even for small results, intermediate steps might require insanely large numbers.

REMARK 2.23: Let $R = \mathbb{Z}/d\mathbb{Z}$, $\varphi : R \to \mathbb{Z} : x + d\mathbb{Z} \mapsto \gcd(x, d)$ and $\psi : R \to \mathbb{Z} : x + d\mathbb{Z} \mapsto \min\{|y| \geq 0 : x - y \in d\mathbb{Z}\}$ Then

(1) both φ and ψ are well defined
(2) both φ and ψ allow euclidean division: For all a, $b \in R$, $b \neq 0$ we can find q, r s.th. $a = bq + r$ and $\varphi(r) < \varphi(b)$ (or $\psi(r) < \psi(b)$). Thus R is essentially a euclidean ring - but be careful, it has zero-divisors. In particular, we can (and will) use the extended euclidean algorithm!
ψ mostly means to work in $\mathbb{Z}$, using lifted numbers, thus using the fact that $\mathbb{Z}$ is already euclidean while φ is more subtle.

EXAMPLE 2.24: Let $R = \mathbb{Z}/12\mathbb{Z}$, $a = 6$, $b = 4$ then $a = 1\cdot 4+2$, but also $a = 5\cdot 3-2$. Here, the euclidean division is by no means unique, in particular if we also swap φ and ψ.

LEMMA 2.25:
(1) $\mathrm{GL}(n, R)$ is a group.
(2) $A \in R^{n\times n}$ is unimodular iff $\det(A) \in R^*$.

PROOF. Well known. □

LEMMA 2.26: Let M be a free R-module of rank n. For any two bases $b_1, \ldots, b_n$ and $c_1, \ldots, c_n$ of M there exists some $U \in \mathrm{GL}(n, R)$ such that

$$(b_1, \ldots, b_n) = (c_1, \ldots, c_n) \cdot U.$$

LEMMA 2.27: Let R be either $\mathbb{Z}$ or $\mathbb{Z}/d\mathbb{Z}$ and a, b in R. Then there exists u, v, g, x, y in R s.th.

$$(g, 0) = (a, b)\begin{pmatrix} u & x \\ v & y \end{pmatrix} \quad \text{and} \quad \det\begin{pmatrix} u & x \\ v & y \end{pmatrix} = \pm 1.$$

PROOF. Since R is, in both cases euclidean, the usual extended gcd will do everything for us: $a_0 := a$, $a_1 := b$ and $A_1 := (a_0, a_1)$. Then each step will multiply A_i by $T_i := \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$ to obtain $A_{i+1} = A_i T_i = (a_i, a_{i-1} - q_i a_i)$ where $a_{i-1} = q_i a_i + r_i$ is the euclidean division. This process stops with $(g, 0)$. The accumulated product of the T_i has the desired properties.

□

EXAMPLE 2.28: Let $R = \mathbb{Z}/12\mathbb{Z}$ and $a = 6$, $b = 4$. Then $g = 2 = a - b$. Of course, $a/2 = 4/2 = 2$, but as correctly, $4/2 = 8$ since $2 \cdot 8 = 16 = 4$. So, divding by $g = 2$, we should get $1 = a/2 - b/2$, but $a/2 = 8$ and $b/2 = 2$ shows $1 = 4$ ....

This means that we cannot just compute the extended gcd in $\mathbb{Z}$ and obtain the cofactors using division as we would do over $\mathbb{Z}$.

In $\mathbb{Z}/d\mathbb{Z}$, we can actually "tweak" the division to always yield the correct result. In more general Euclidean rings, we cannot, so we have to rely on the extended Euclidean algorithm here.

LEMMA 2.29: Let R be as above. Then $aR+bR = gR$, $aR \cap bR = lR$, $abR = glR$. Furthermore: let $\begin{pmatrix} u & x \\ v & y \end{pmatrix}$ be as in 2.27, then $g = ua + vb$, $l = ax = -by$, $a = gy$, $b = -gx$ and $xR + yR = R$.

PROOF. **(Kaplansky)** Let $U := \begin{pmatrix} u & x \\ v & y \end{pmatrix}$ as in 2.27, then $\det U = \pm 1$, hence $U^{-1} = \pm \begin{pmatrix} y & -x \\ -v & u \end{pmatrix}$ giving $(g, 0)U^{-1} = (a, b) = (gy, -gx)$ showing a, $b \in gR$, so g is a "gcd" of a and b.

Now let $z \in aR \cap bR$ be arbitrary, so $z = \mu a = -\nu b$. Set

$$V := \begin{pmatrix} u & \mu \\ v & \nu \end{pmatrix} \text{ and } U^{-1}V =: \begin{pmatrix} e & f \\ h & i \end{pmatrix}.$$

Then $\begin{pmatrix} a & b \\ 0 & b \end{pmatrix} U = \begin{pmatrix} g & 0 \\ vb & yb \end{pmatrix}$. This shows $ax = -by$ (1-2-entry) and $ab = g(yb)$ hence $abR = glR$ (2-2 entry). Now $(a, b)V = (g, 0)$ as well, so $(g, 0)U^{-1}V = (a, b)V = (g, 0)$ hence $gf = 0$, implying $af = 0$ as well ($a = gy$)

Cleary $V = U(U^{-1}V) = \begin{pmatrix} u & x \\ v & y \end{pmatrix} \begin{pmatrix} e & f \\ h & i \end{pmatrix} = \begin{pmatrix} u & \mu \\ v & \nu \end{pmatrix}$, so $\mu = uf + xi$ and $z = \mu a = a(uf + xi) = axi = li$, so $z \in lR$, showing $aR \cap bR \subseteq lR$. The reverse inclusion is trivial, hence l is a "lcm" of a and b.

The last statement follows from the determinant: $uy - vx = \pm 1$ but $uy - vx \in xR + yR$. □

LEMMA 2.30: Let R be as above and $\langle a \rangle = \langle b \rangle$ for some elements a, $b \in R$. Then a and b are associate, i. e. there is some $u \in R^*$ s.th. $a = ub$.

For $R = \mathbb{Z}$ this is clear: we get $a \in b\mathbb{Z}$, hence $a = bx$ and $b \in a\mathbb{Z}$, implying $b = ay$, so $a = bx = axy$. The cancellation then gives $xy = 1$.

However, in $\mathbb{Z}/12\mathbb{Z}$, we have $4R = 8R = \{0, 4, 8\}$ and $8 = 2 \cdot 4$, $4 = 2 \cdot 8$ and $xy = 4$ is not a unit. On the other hand, we also have $8 = 5 \cdot 4$ and 5 is a unit.

PROOF. For $\mathbb{Z}$ this is clear, so assume $R = \mathbb{Z}/dZ$. Using the CRT, we get $d = \prod p^{n_p}$ and $\mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/p^{n_p}\mathbb{Z}$. If we can solve the problem for all $\mathbb{Z}/p^n\mathbb{Z}$, then the CRT will find a solution in R. So, wlog, $R = \mathbb{Z}/p^n\mathbb{Z}$. In R, all ideals are generated by p^k for $k < n$, all elements have a unique representation as $a = p^k e$ for $e \in (\mathbb{Z}/p^n\mathbb{Z})^*$. Thus from $aR = bR$ we get $a = be$ for a suitable $e \in (\mathbb{Z}/p^n\mathbb{Z})^*$ as required. □

LEMMA 2.31: Let R be as above and $a_1, \ldots, a_n \in R$. There exists some $U \in \mathrm{GL}(n, R)$ such that $(a_1, \ldots, a_n) \cdot U = (c, 0, \ldots, 0)$ for $c := \gcd(a_1, \ldots, a_n)$.

PROOF. Induction: $n = 1$ is trivial. $n = 2$ is just 2.27. By induction hypothesis, assume we have $T \in \mathrm{GL}(n, R)$ s.th. $(a_1, \ldots, a_n)T = (g, 0, \ldots, 0)$ for g (a/ the) gcd of $a_1, \ldots, a_n$. Then clearly, $\tilde{T} = \left(\begin{array}{c|c} T & 0 \\ \hline 0 & 1 \end{array}\right) \in \mathrm{GL}(n+1, R)$ and $(a_1, \ldots, a_n, a_{n+1})\tilde{T} = (g, 0, \ldots, 0, a_n)$.

Now, using 2.27 we find $\begin{pmatrix} u & x \\ v & y \end{pmatrix} \in \mathrm{GL}(2, R)$ s.th. $(g, a_{n+1}) \begin{pmatrix} u & x \\ v & y \end{pmatrix} = (\tilde{g}, 0)$.

Then $S := \tilde{T} \begin{pmatrix} u & 0 \ldots 0 & x \\ & \vdots & \\ u & 0 \ldots 0 & v \end{pmatrix} \in \mathrm{GL}(n+1, R)$ has all the properties. □

For a commutative unitary ring R we have an equivalence relation

$$a \sim b :\iff \exists u \in R^* : a = ub$$

Fix now a system of representatives $\mathcal{R} \subseteq R$ for the equivalence classes. For $R = \mathbb{Z}$ we will choose $\mathcal{R} = \mathbb{Z}^{\geq 0}$, for $R = \mathbb{Z}/m\mathbb{Z}$, we choose $\mathcal{R} = \{d | m \mid d > 0\} \cup \{0\}$.

Furthermore, for any $d \in R$, $d \neq 0$, we need to fix a system of representatives $\mathcal{R}_d$ for R/dR as well. Again, for the $\mathbb{Z}$ we can choose the positive (or symmetric) system of representatives.

EXAMPLE 2.32: Let $R = \mathbb{Z}/12\mathbb{Z}$

THEOREM 2.33 (Hermite Normal Form): Let R be a PIR. For every matrix $A \in R^{m \times n}$ exisists some $U \in \mathrm{GL}(n, R)$, such that $A \cdot U$ is a lower triangular matrix with "diagonal elements" in $\mathcal{R}$ and the off-diagonal elements are in $\mathcal{R}_d$ where d is the diagonal element to the right. $A \cdot U$ is called a *Hermite normal form* of A.

Note: in general, the matrix has a more complicated shape as not all diagonal elements will be non-zero. The "non-zero diagonal" will then be more like a staircase.

PROOF. Via induction, $n = 1$ begin trivial as we only have to normalise the entry to be in $\mathcal{R}$.

Assume now $n > 1$. For $c = \gcd(a_{11}, \ldots, a_{1n}) \in \mathcal{R}$ we can find by 2.31 some $U_1 \in \mathrm{GL}(n, R)$ such that

$$A \cdot U_1 = \left(\begin{array}{c|ccc} c & 0 & \ldots & 0 \\ \hline * & & \tilde{A} & \end{array}\right).$$

Using the induction hypothesis on $\tilde{A}$ we get a lower triangular matrix. It remains to use elementary matrices to reduce the off-diagonal elements and to achieve the diagonal elements to be in $\mathcal{R}$. □

REMARK 2.34: It R is free of zero divisors, then the Hermite normal form is actually unique. To see this, consider a series of projections, starting with a projection onto the 1st coordinate. Then clearly, the top left entry of the HNF will have to be the gcd of the 1st row - a generator for the ideal generated by the 1st row. Hence it is (essentially) unique. Now, for any element in R^n there is a unique multiple of the 1st column of the HNF that will zero the 1st entry, thus we can define a projection onto R^{n-1} this way. The same argument now shows the uniqueness of the next diagonal element.

The transformation matrix however is only rarely unique.

THEOREM 2.35 (Smith Normal Form): Let R be a PIR and $A = (a_{ij}) \in R^{m\times n}$ be arbitrary. Set $r = \min(m, n)$, then we can find $V \in \mathrm{GL}(m, R)$ und $U \in \mathrm{GL}(n, R)$, such that for $S(A) := (s_{i,j}) := V \cdot A \cdot U$ we have:

(1) $s_{i,j} = 0$ $(1 \le i \le m,\ 1 \le j \le n,\ i \ne j)$,
(2) $s_{i,i} | s_{j,j}$ $(1 \le i \le j \le r)$,
(3) $s_{i,i} \in \mathcal{R}$ $(1 \le i \le r)$,

$S(A)$ is unique and is called *Smith normal form* of A.

PROOF. The first step is to find $\tilde{V} \in \mathrm{GL}(m, R)$ und $\tilde{U} \in \mathrm{GL}(n, R)$, such that for $\tilde{V} \cdot A \cdot \tilde{U}$ condition (1) holds, i. e. the resulting matrix is diagonal. For $n = 1$ this is trivial via 2.31. Let now $n > 1$. Application of 2.33 alternatingly from the left (via transpose) and right will achieve

$$A \cdot \tilde{U}_1 = \left(\begin{array}{c|c} c_1 & 0 \\ \hline * & A_1 \end{array}\right),$$

and

$$\tilde{V}_2 \cdot A \cdot \tilde{U}_1 = \left(\begin{array}{c|c} c_2 & * \\ \hline 0 & A_2 \end{array}\right), \quad \tilde{V}_2 \cdot A \cdot \tilde{U}_1 \cdot \tilde{U}_2 = \left(\begin{array}{c|c} c_3 & 0 \\ \hline * & A_3 \end{array}\right), \quad \ldots$$

Since $c_{i+1} | c_i$ and $c_1 | a_{11}$ this process will terminate, due to R being Noetherian as a PIR, and the chain of ideals $\langle c_{i+1}\rangle \supseteq \langle c_i\rangle \supseteq \langle a_{1,1}\rangle$ is ascending.

Once the $\langle c_i\rangle$ are no-longer changing, we can just subtract suitable multiples of the 1st row or column to obtain

$$\left(\begin{array}{c|c} c_k & 0 \\ \hline 0 & A_k \end{array}\right).$$

The induction hypothesis applied to A_k will result in a diagonal matrix, hence (1) is satisfied.

Now we need to achieve the divisibility condition: To get $s_{ii} | s_{jj}$ $(1 \le i < j \le r)$ we apply row and column operations to replace s_{ii} by $\gcd(s_{ii}, s_{jj}) \in \mathcal{R}$ and s_{jj} by $\mathrm{lcm}(s_{ii}, s_{jj}) \in \mathcal{R}$:

Let $T = \begin{pmatrix} u & x \\ v & y \end{pmatrix}$ from 2.27 for (s_{ii}, s_{jj}). $G := \begin{pmatrix} s_{ii} & s_{ij} \\ 0 & s_{jj} \end{pmatrix}$ has determinant $s_{ii}s_{jj}$ and $GT = \begin{pmatrix} g & 0 \\ b & c \end{pmatrix}$ for some $b = vs_{jj}$ and $c = ys_{jj}$. By 2.29, g is a gcd and c a lcm. Thus $b = vs_{jj} \in \langle g\rangle$, so we can find a q s.th. $vs_{jj} = qg$ and thus $\begin{pmatrix} -q & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} g & 0 \\ b & c \end{pmatrix} = \begin{pmatrix} g & 0 \\ 0 & c \end{pmatrix}$ as required.

For the uniqueness let $d_i(A)$ be a gcd of all (i,i)–minors of A $(1 \le i \le r)$ then $d_{i-1}(A)|d_i(A)$ $(2 \le i \le r)$ by Laplace's formula. Furthermore $d_i(A)|d_i(A \cdot B)$ for $B \in R^{n\times n}$, since the columns of $A \cdot B$ are linear combinations of the columns of A, hence every minor of $A \cdot B$ is the product of minor of A. Argueing with rows, we get $d_i(A)|d_i(C \cdot A)$ for $C \in R^{m\times m}$ as well. Now we get

$$d_i(A)|d_i(A \cdot U)|d_i(V \cdot A \cdot U) = d_i(S(A))|d_i(V^{-1} \cdot S(A) \cdot U^{-1}) = d_i(A),$$

thus

$$d_i(A) = d_i(S(A)) = \prod_{j=1}^{i} s_{jj} \qquad (1 \le i \le r).$$

Since $s_{ii} = \frac{d_i(A)}{d_{i-1}(A)}$ $(1 \le i \le r, d_0(A) := 1)$ the proof is finished observing that the identities hold for the ideals, but by 2.30 the generators are all associated, so they can be chosen uniquely in $\mathcal{R}$. □

The diagonal elements of the Smith normal form are also known as *elementary divisors* .

LEMMA 2.36: Let $N \subseteq M$ be free modules over a PID and $\mathrm{rg}(N) =: n \le \mathrm{rg}(M) =: m$. (wlog: $N \subseteq R^n$, $M \subseteq R^m$)

(1) For every basis a_i $(1 \le i \le n)$ of M exists a basis b_j $(1 \le j \le m)$ for N and some lower triangular matrix A such that $(b_1, \ldots, b_n) = (a_1, \ldots, a_m)A$. The rows of A are unique modulo $a_{i,i}$.
(2) For every basis b_i $(1 \le i \le n)$ of N exists a basis a_j $(1 \le j \le m)$ of M and some lower triangular matrix A such that $(b_1, \ldots, b_n) = A(a_1, \ldots, a_m)$. The columns of A are unique modulo $a_{i,i}$.
(3) In N and M we can find bases a_i $(1 \le i \le n)$ and b_j $(1 \le j \le m)$ such that $b_i = \varepsilon_i a_i$ $(1 \le i \le n)$ $\varepsilon_i|\varepsilon_{i+1}$ $(1 \le i < n)$, $\varepsilon_0 := 1$. The ε_i are uniquely defined by N and M.

PROOF. □

Application:

Let $N \subseteq M$ be two R-modules over some PIR R. Then by 2.36(3) we can find bases (b_i) for M and (a_i) for N such that $a_i = \varepsilon_i b_i$ for $\varepsilon_i \in R$ - possibly some $\varepsilon_i = 0$ if the rank of M is smaller than the one of N. But then

$$N/M = (\dot{+}b_iR)/(\dot{+}a_iR) = \dot{+}(b_iR)/(a_iR) = \dot{+}(R/\varepsilon_i)$$

thus, for $\mathbb{Z}$-modules, we obtain the complete structure of the quotient module as an abelian group. In particular, we see that for modules of the same rank, $\varepsilon_n M \subseteq N$ as ε_n is the exponent of the quotient.

Furthermore, 2.36 (1) is used to effectively work in and with the quotient modules:

(1) After fixing systems of representatives for R/dR, we can use the triangular matrix to find unique representatives in the cosets. Let $m = \sum m_i b_i$ be arbitrary in M. Then $m - y_1a_1$ can arranged to have 1st coefficient in $R/d_{1,1}R$ where $(d_{i,j})_{i,j}$ is the lower triangular transformation matrix. Now $m - y_1a_1 - y_2a_2$ can arranged to have the 2nd coefficient in $R/d_{2,2}R$. As $d_{1,2} = 0$, this will not affect the 1st coefficient. Inductively, all coefficients are in the appropriate residue systems. Since each of the reductions is unique, so is the result. This

is sometimes written as $m \bmod (d_{i,j})_{i,j}$. Note that this depends on the bases of N and M. It can be made to depend on the basis of M only by forcing the transformation to be in HNF. Since this is unique, the reduction then is canonical.

(2) The size $|M/N|$ is the determinant of the triangular matrix, hence the product of the diagonal.

Lastly, let $M(A)$ the the R-submodule of R^n generated by the columns of the matrix A and let $\lambda \in R$ such that $\lambda R^n \subseteq M(A)$ (this forces A to be of full rank!). Then

(1) $M(A) = M(A|\lambda I_n)$
(2) Assuming A to be square, then $\det(A)R^n \subseteq M(A)$
(3) Let ε_n be the largest elementary divisor of A (hence the exponent of $R^n/M(A)$ as R-torsion module). Then $\varepsilon_n R^n \subseteq M(A)$.
(4) We have $\mu\lambda R^n \subseteq M(A)$ for all $\mu \in R$.

Under the assumptions, $R^n/M(A)$ is a $R/\lambda R$-module. If R is a PID, then $R/\lambda R$ is still a PIR, so we can compute the structure (or a minimal set of generators) of $R^n/M(A)$ using the Hermite or Smith techniques over $R/\lambda R$. In particular for $R = \mathbb{Z}$ we see that this way, regardless of the algorithm used, coefficient explosion can not happen. However, this will only compute say a $R/\lambda R$ set of generators for $R^n/M(A)$. In order to find generators for $M(A)$ we have to supplement a lift by generators of λR^n.

To see the problem: Let $A := \begin{pmatrix} 4 & 0 \\ 2 & 2 \end{pmatrix}$ Then clearly, $\lambda = 4$ is a possible choice. But over $\mathbb{Z}/4\mathbb{Z}$ we obtain $\begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix}$ which lifts not to a basis for $M(A)$. There are (at least) two ways to solve this. Firstly, we can work using a *multiple* of λ, λ^2 or even 2λ. It can be shown, that a suitable multiple will solve the problem. The second alternative is to follow the computation over $R/\lambda R$ by one over R. The idea being that most of the "hard work" will already have been done. The final computation thus being easy.

In both approaches an additional complication is the non-uniqueness of the HNF if R has zero-divisors.

4. Algorithms Round2

Given a prime $p \in \mathbb{Z}$ and some polynomial f defining the order $\mathcal{O} := \mathbb{Z}[t]/f$, in most cases the Round2 will show that $\mathcal{O}$ is already p-maximal, or, it will be p-maximal after one iteration (i. e. the ring of multipliers of $\sqrt{p\mathcal{O}}$ is p-maximal). In this special situation, there is a very fast way of performing the computations:

THEOREM 2.37 (Dedekind's criterion): Let $f \in \mathbb{Z}[t]$ be monic and irreducible, $p \in \mathbb{Z}$ a prime. Over $\mathbb{Z}/p[t]$ write

$$\bar{f} = \prod \bar{f}_i^{e_i}$$

with $f_i \in \mathbb{Z}[t]$ monic such that $\bar{f}_i \in (\mathbb{Z}/p)[t]$ is irreducible. Define $\bar{g} := \prod \bar{f}_i$ and $\bar{h} := \prod \bar{f}_i^{e_i-1}$, and g, $h \in \mathbb{Z}[t]$ monic and finally

$$\bar{T} := \gcd(\bar{g}, \bar{h}, \overline{\frac{1}{p}(f - gh)})$$

(1) $\mathcal{O} = \mathbb{Z}[t]/f$ is p-maximal iff $\bar{T} = 1$
(2) $\sqrt{p\mathcal{O}} = \langle p, g\rangle$
(3) $[\sqrt{p\mathcal{O}}/\sqrt{p\mathcal{O}}] = \langle \mathcal{O}, \frac{1}{p}U\rangle$ where $\bar{U} := \bar{f}/\bar{T}$ and $U \in \mathbb{Z}[t]$ monic.

Proof omitted: it is rather long and very technical, but not difficult. We also note, that this does not require a full $\bmod p$ factorisation: $\bar{g}$ is just the squarefree-part of $\bar{f}$ and $\bar{h} = \bar{f}/\bar{g}$.

EXAMPLE 2.38: $f := t^3 - t^2 - 2t - 8$, then a test $\bmod 3$ will show f to be irreducible. We have $d_f = -2^2 \cdot 503$, so only $\mathcal{O}_2$ is difficult. Applying Dedekind: $\bar{f} = \bar{t}^3 + \bar{t}^2 = \bar{t}^2(\bar{t} + 1)$, hence $\bar{g} = \bar{t}(\bar{t} + 1)$ and $\bar{h} = \bar{t}$, thus $f - gh = -2t^2 - 2t - 8$ and $\bar{T} = \gcd \bar{t}(\bar{t} + 1), \bar{t}, \bar{t}^2 + t) = \bar{t}$, and we're not 2-maximal. Now $\bar{U} = \bar{f}/\bar{T} = \bar{t}(\bar{t} + 1)$ hence $[\sqrt{2\mathcal{O}}/\sqrt{2\mathcal{O}}] = \langle \mathcal{O}, \frac{1}{2}t(t + 1)\rangle = \langle 1, t, t^2, 1/2(t^2 + t)\rangle = \langle 1, t, 1/2(t^2 + t)\rangle$ is a larger order. Since d_f was changed by a factor of 4, the result is 2-maximal and hence maximal.

We're now going to do the same example using "normal" Round2, i. e. without the Dedekind criterion. The 1st step is to compute the 2-radical. As $2 < 3 = \deg L$, we cannot use the trace-radical. We will use the fact that by 2.12, $\sqrt{p\mathcal{O}} = \{x \in \mathcal{O} | x^k \in p\mathcal{O}\}$ for all $k \geq n$. Furthermore, $p\mathcal{O} \subseteq \sqrt{p\mathcal{O}}$, so we're going to work in $V := \mathcal{O}/p\mathcal{O}$ again, here we have $\sqrt{p\mathcal{O}} + p\mathcal{O} = \{x \in V | x^k = 0\}$ and V is a $\mathbb{Z}/p\mathbb{Z}$-module. For $p = 2$, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field of positive characteristic p, hence $x \mapsto x^{p^l}$ is a $\mathbb{F}_p$-linear map. Choose l so that $p^l \geq n$ and define

$$\varphi : V \to V : x \mapsto x^{p^l}$$

then $\ker \varphi = \sqrt{p\mathcal{O}} + p\mathcal{O}$:

Here, $n = 3$, $p = 2$, so $l = 2$. We need to compute ω_i^4 for ω_i a basis of $\mathcal{O}$, so $1^4 = 1$, $\rho^4 = \rho\rho^3 = \rho(\rho^2+2\rho+8) = \rho^3+2\rho^2+8\rho = (\rho^2+2\rho+8)+2\rho^2+8\rho = 3\rho^2+10\rho+8 \equiv \rho^2 \pmod 2$. For $\omega_2 = \rho^2$, we get $\rho^8 = (\rho^4)^2 \equiv (\rho^2)^2 = \rho^4 \equiv \rho^2$.

Clearly, $\ker \varphi = \langle \rho + \rho^2\rangle$, hence $\sqrt{2\mathcal{O}} = \langle 2, \rho + \rho^2\rangle$. From here we can compute a basis.

Next, we need the ring of multipliers. Let A, $B \subseteq \mathcal{O}$ be ideals with $\mathbb{Z}$-bases a_i for A, b_i for B and ω_i for $\mathcal{O}$. Then $(a_1, \ldots, a_n) = (\omega_1, \ldots, \omega_n)M_A$ and $(\omega_1, \ldots, \omega_n)^t b_i =$

$M_{b_i}(\omega_1,\dots,\omega_n)^t$. So we have $x = \sum x_i\omega_i$, $xb_j = \sum y_i\omega_i$ and $(x_1,\dots,x_n)M_{b_j} = (y_1,\dots,y_n)$. Furthermore, $x = \sum x_i\omega_i \in A$ iff $(x_1,\dots,x_n) \in (\mathbb{Z}^n)^t M_A$. Now

$$\begin{aligned}
[A/B] &= \{x \in L | xB \in A\} \\
&= \{x \in L | \forall i : xb_i \in A\} \\
&= \{(x_1,\dots,x_n) \in K^n | \forall i : (x_1,\dots,x_n)M_{b_i} \in (\mathbb{Z}^n)^t M_A\} \\
&= \{(x_1,\dots,x_n) \in K^n | \forall i : (x_1,\dots,x_n)M_{b_i}M_A^{-1} \in (\mathbb{Z}^n)^t\} \\
&= \{(x_1,\dots,x_n) \in K^n | (x_1,\dots,x_n)(M_{b_1}M_A^{-1}|\dots|M_{b_n}M_A^{-1}) \in (\mathbb{Z}^{n^2})^t\}
\end{aligned}$$

Let $T \in \mathrm{Gl}(n^2,\mathbb{Z})$ arbitrary, then

$$= \{(x_1,\dots,x_n) \in K^n | (x_1,\dots,x_n)(M_{b_1}M_A^{-1}|\dots|M_{b_n}M_A^{-1})T \in (\mathbb{Z}^{n^2})^t\}$$

Specifically, let $(H|0)$ the column-HNF of the large matrix, then

$$\begin{aligned}
&= \{(x_1,\dots,x_n) \in K^n | (x_1,\dots,x_n)H \in (\mathbb{Z}^n)^t\} \\
&= \{(x_1,\dots,x_n) \in K^n | (x_1,\dots,x_n) \in (\mathbb{Z}^n)^t H^{-1}\}
\end{aligned}$$

We now specialise this to $A = B$ and note that $M_{a_i}M_A^{-1}$ has to be integral, i. e. $\in \mathbb{Z}^{n\times n}$ even though M_A^{-1} is not.

Continuing with the example:

$$A = \sqrt{2\mathcal{O}} = \langle 2, \rho + \rho^2\rangle$$

So $M_A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, $M_2 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, $M_{2\rho} = \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 16 & 4 & 2 \end{pmatrix}$ and $M_{\rho+\rho^2} = \begin{pmatrix} 0 & 1 & 1 \\ 8 & 2 & 2 \\ 16 & 12 & 4 \end{pmatrix}$.

Hence $M_2M_A^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 2 \end{pmatrix}$, $M_{2\rho}M_A^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 2 \\ 8 & 1 & 2 \end{pmatrix}$, $M_{\rho+\rho^2}M_A^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 4 & 0 & 2 \\ 8 & 4 & 4 \end{pmatrix}$

and $M_A^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 2 \end{pmatrix}$. So the big matrix will be

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & -1 & 2 & 4 & 0 & 2 \\ 0 & -1 & 2 & 8 & 1 & 2 & 8 & 4 & 4 \end{pmatrix}$$

The column-Hermite form is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

with inverse

$$\frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -1 & 1 \end{pmatrix}$$

So that the new order is

$$\mathcal{O}_2 = \mathbb{Z} + \mathbb{Z}\rho + \mathbb{Z}\frac{1}{2}(\rho^2 - \rho)$$

What's next? (i. e. next year or in projects) Complexity of the procedure:

THEOREM 2.39 (Chistov): The computation of a maximal order starting with a monic irreducible $f \in \mathbb{Z}[t]$ is polynomial time equivalent to finding the largest square-free factor of d_f

Looking at our algorithms, all is based on linear algebra hence polynomial time. Thus the procedure is essentially optimal. (There are other, even more optimal approaches, but in general, the hard bit is finding the primes p).

All we have done (well: most) applies as well to the situation where $\mathbb{Z}$ is replaced by any PID, for example $R = k[x]$ and in particular $R = \mathbb{F}_q[x]$. Then $R[t]/f$ is essentially a plane curve and can be analysed with tools from geometry as well.

Further generalisations are $R = \mathbb{Z}_K$ (which is harder as R is no PID in general), to allow polynomials that are only square-free or even non-commutative rings (representation theory).

CHAPTER 3

Lattices

1. Introduction

DEFINITION 3.1: Let $b_1, \ldots, b_k \in \mathbb{R}^n$ be $\mathbb{R}$-linear independent, then

$$\Lambda := \dot{+}\mathbb{Z}b_i$$

is called a *lattice* or, sometimes, a $\mathbb{Z}$-lattice in $\mathbb{R}^n$. $d(\Lambda) := (\det((b_i^t b_j)_{i,j}))^{1/2}$ is called *lattice discriminant*. We set $\Pi(\Lambda) := \{\sum \lambda_i b_i | 0 \leq \lambda_i < 1\}$ as the *fundamental domain* of Λ. A submodule $\Lambda' < \Lambda$ is called a sublattice if Λ' is a lattice as well.

REMARK 3.2: In general any measurable subset $\Pi \subset \mathbb{R}^n$ such that

$$\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = \dot{\bigcup}_{x \in \Lambda} x + \Pi$$

is a fundamental domain.

LEMMA 3.3: Let Λ be a lattice with basis $(b_i)_i$.

(1) $d(\Lambda) = \mathrm{Vol}_k(\Pi(\Lambda))$
(2) $\Lambda' \leq \Lambda$ a sublattice with basis $(c_i)_i$ and $(c_1, \ldots, c_n) = (b_1, \ldots, b_n)U$ with $U \in \mathbb{Z}^{n \times n}$, then $d(\Lambda') = \det(U) d(\Lambda)$
(3) $(\Lambda : \Lambda)_{\mathbb{Z}} = d(\Lambda')/d(\Lambda)$

PROOF. All this follows directly from measure theory and properties of the Lebesgue integral. □

ALGORITHM 3.4 (Quadratic Supplement):

Input: $A \in \mathbb{R}^{n \times n}$ positive definite
Output: $Q = (q_{i,j})$ triangular, such that

$$x^t A x = \sum_{i=1}^{k} q_{i,i}(x_i + \sum_{j=i+1}^{k} q_{i,j} x_j)^2$$

1: $Q := A$
2: for $i := 1, \ldots, k-1$ do
3: for $j = i+1, \ldots, k$ do
4: $q_{j,i} := q_{i,j}$, $q_{i,j} := q_{i,j}/q_{i,i}$
5: for $\mu, \nu = i+1, \ldots, k$ do
6: $q_{\mu,\nu} := q_{\mu,\nu} - q_{\mu,i} q_{i,\nu}$
7: for $j = 1, \ldots, i-1$ do
8: $q_{i,j} := 0$

PROOF. This is just quadratic supplement:

$$x^tAx = \sum_{i,j} x_i x_j A_{i,j}$$

Focusing on x_1:

$$x^tAx = x_1^2 A_{1,1} + x_1 \sum_{j>1} x_j (A_{1,j} + A_{j,1}) \sum_{i,j>1} x_i x_j A_{i,j}$$

Now, we complete the square:

$$\begin{aligned} x^tAx &= A_{1,1}(x_1^2 + 2x_1 \sum_{j>1} \frac{A_{1,j}}{A_{1,1}} x_j) + \sum_{i,j>1} x_i x_j A_{i,j} \\ &= A_{1,1}(x_1^2 + 2x_1 \sum_{j>1} \frac{A_{1,j}}{A_{1,1}} x_j + (\sum_{j>1} \frac{A_{1,j}}{A_{1,1}} x_j)^2) - A_{1,1}(\sum_{j>1} \frac{A_{1,j}}{A_{1,1}} x_j)^2 + \sum_{i,j>1} x_i x_j A_{i,j} \\ &= A_{1,1}(x_1 + \sum_{j>1} \frac{A_{1,j}}{A_{1,1}} x_j)^2 + \dots \end{aligned}$$

Where the $\dots$ indicate a x^tAx with a smaller matrix A. □

EXAMPLE 3.5: Let $A := \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ For $i = 1$:

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

For $i = 2$:

$$\begin{pmatrix} 2 & 1/2 & 1/2 \\ 1 & 3/2 & 1/2 \\ 1 & 1/2 & 3/2 \end{pmatrix} \to \begin{pmatrix} 2 & 1/2 & 1/2 \\ 1 & 3/2 & 1/3 \\ 1 & 1/2 & 3/2 \end{pmatrix} \to \begin{pmatrix} 2 & 1/2 & 1/2 \\ 1 & 3/2 & 1/3 \\ 1 & 1/2 & 4/3 \end{pmatrix}$$

And finally:

$$\begin{pmatrix} 2 & 1/2 & 1/2 \\ 1 & 3/2 & 1/3 \\ 1 & 1/2 & 3/4 \end{pmatrix} \to \begin{pmatrix} 2 & 1/2 & 1/2 \\ 0 & 3/2 & 1/3 \\ 0 & 0 & 4/3 \end{pmatrix}$$

ALGORITHM 3.6 (Enumeration):

Input: $A \in \mathbb{R}^{n \times n}$ pos. definite as well as $c > 0$
Output: all $x \in \mathbb{Z}^n$ such that $x^tAx \leq c$
1: use 3.4 to find Q
2: do a backtrack-search to find the points

EXAMPLE 3.7: It's actually easy, but easier to show than to formally state. We take the same matrix as in the previous example and $c := 3$, so

$$A := \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

and

$$x^tAx = \frac{4}{3}x_3^2 + \frac{3}{2}(x_2 + \frac{1}{3}x_3)^2 + 2(x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3)^2$$

Since this is a sum of 3 positive numbers, clearly we need $4/3x_3^2 \leq 3$, hence $x_3^2 \leq 9/4$, or $x_3 \in -1, \dots, 1$. For each of the possibilities we now need to work. Lets start with

$x_3 = 1$. Start with $x_3 = 1$ and thus $4/31^2 + 3/2(x_2 + 1/3)^2 \leq 3$ or $(x_2 + 1/3)^2 \leq 5/3$, hence $x_2 = 0$ or $x_2 = -1$. For $x_2 = 0$, we get $4/3+3/2(0+1/3)^2+2(x_1+0+1/2)^2 \leq 3$ or $(x_1 + 1/2)^2 \leq 3/2$, so $x_1 = -1, 0$.

Next we need to look at $x_2 = -1$, ...

THEOREM 3.8: Let Λ be a lattice, then Λ is discrete, i. e. for all $x \in \mathbb{R}^n$, $c > 0$, the set $\{z \in \Lambda | \|x - z\|\} < c\}$ is finite.

PROOF. Direct consequence of 3.6 with $A := (b_i^t b_j)_{i,j}$ for any basis (b_i) for the lattice since $\|z - x\|^2 = (z_1 - x_1, \ldots, z_k - x_k)A(z_1 - x_1, \ldots, z_k - x_k)^t$ □

COROLLARY 3.9: Let Λ be a lattice. Then there is some $\delta > 0$ such that

$$\forall x \neq y \in \Lambda : \|x - y\| > \delta$$

COROLLARY 3.10: Let Λ be a lattice and $x_n \in \Lambda$ be a sequence. If $x_n \to x$ for some $x \in \mathbb{R}^n$, then $x \in \Lambda$

2. Minkowski Theory

THEOREM 3.11 (Minkowski's convex body theorem): Let Λ be a n-dimensional (or *full* lattice) in $\mathbb{R}^n$ and $C \subseteq \mathbb{R}^n$ a convex and symmetric set and either

(1) $\operatorname{Vol} C > 2^n d(\Lambda)$
(2) $\operatorname{Vol} C = 2^n d(\Lambda)$ and C compact.

Then C contains a non-trivial lattice point $0 \neq x \in \Lambda \cap C$.

PROOF. Let $\Pi := \Pi(\Lambda)$ be a fundamental domain. Then $\mathbb{R}^n = \dot{\bigcup}(x + \Pi)$ and thus

$$\frac{1}{2}C = \frac{1}{2}C \cap \mathbb{R}^n = \dot{\bigcup}\frac{1}{2}C \cap (x + \Pi).$$

Assuming (1), we now get

$$\begin{aligned} \operatorname{Vol}(\Pi) &= d(\Lambda) < 2^{-n} \operatorname{Vol} C = \operatorname{Vol} \frac{1}{2}C \\ &= \operatorname{Vol}(\dot{\bigcup}\frac{1}{2}C \cap (x + \Pi)) \\ &= \sum \operatorname{Vol} \frac{1}{2}C \cap (x + \Pi) \\ &= \sum \operatorname{Vol}(\frac{1}{2}C - x) \cap Pi \end{aligned}$$

Suppose, the sets $1/2C - x$ are pariwise disjoint, then

$$\begin{aligned} &= \operatorname{Vol} \dot{\bigcup}(\frac{1}{2}C - x) \cap Pi \\ &= \operatorname{Vol} \Pi = d(\Lambda) \end{aligned}$$

Which is absurd, hence the sets cannot be all disjoint and we can find $x \neq y \in \Lambda$ such that

$$\frac{1}{2}C - x \cap \frac{1}{2}C - y \neq \emptyset$$

Thus c_1, $c_2 \in C$ sth $1/2c_1 - x = 1/2c_2 - y$ and $1/2c_1 - 1/2c_2 = x - y \in \Lambda \cap C$ is non-trivial. Here we need the symmetry to get $-1/2c_2 \in C$ and the convexity for $1/2c_1 + 1/2(-c_2) \in C$.

For the second claim, take any sequence $\delta_n \searrow 0$, then $\mathrm{Vol}(1+\delta_n)C > 2^n d(\Lambda)$, so by (1), there is a $x_n \in \Lambda \cap (1+\delta_n)C$. Since $x_n \in (1+\delta_1)C$ for all n and since C is compact, the sequence has to contain a converging subsequence. By 3.10 the limes is a lattice point as well, by construction it is in the intersection of all $(1+\delta_n)C$, hence in C. □

DEFINITION 3.12 (Successive Minima): Let Λ be a k-dimensional lattice in $\mathbb{R}^n$. Set

$$M_i := M_i(\Lambda) := \min\{\lambda > 0 | \exists x_1, \ldots, x_i \in \Lambda \ \mathbb{R}\text{-lin. indep. and } \|x_j\|^2 \leq \lambda\}$$

the i-th successive minimum of Λ

Obviously, $M_1 \leq M_2 \leq \ldots \leq M_k$.

LEMMA 3.13 (Enlarge Module): Let $M = \dot{+}_{i=1}^{n} \mathbb{Z}b_i \subseteq \Gamma$, $b_{n+1} \in \Gamma$ and $\sum_{i=1}^{n+1} m_i b_i = 0$, $\gcd(m_i | i) = 1$. Now, find $U \in \mathrm{Gl}(n+1, \mathbb{Z})$ such that $(m_1, \ldots, m_{n+1})U = (1, 0, \ldots, 0)$ using 2.31, and $U^{-1} =: V = (v_{i,j})$. Set $c_i := \sum_{j=1}^{n+1} v_{i,j}$ for $i = 1, \ldots, n+1$. Then

$$\langle M, b_{n+1} \rangle = \dot{+}_{i=2}^{n+1} \mathbb{Z}c_i$$

PROOF. Since U and V are unimodular, clearly $\langle b_i | 1 \leq i \leq n+1 \rangle = \langle c_i | 1 \leq i \leq n+1 \rangle$. By construction we have $UV = 1$ and $mU = (1, 0, \ldots, 0)$, so the 1st row of V is m and thus $c_1 = 1$, hence the statement follows. □

LEMMA 3.14 (Change of basis): Let $M = \dot{+}_{i=1}^{n} \mathbb{Z}b_i$. Furthermore, let $i \in \{1, \ldots, n\}$ and $c_i := \sum_{j=1}^{n} \gamma_j b_j \in M$ be given. Then we can supplement b_1, …, b_{i-1}, c_i to a basis of M iff $\gcd(\gamma_i, \ldots, \gamma_n) = 1$ holds.

PROOF. Let $\gcd(\gamma_i, \ldots, \gamma_n) = 1$ by 2.31 we can find some $U \in \mathrm{GL}(n-i+1, R)$ such that $(\gamma_i, \ldots, \gamma_n)U = (1, 0, \ldots, 0)$. Now

$$(b_1, \ldots, b_n) \left(\begin{array}{ccc|c} & & & \gamma_1 \\ & I_{i-1} & & \vdots \quad 0 \\ & & & \gamma_{i-1} \\ \hline 0 & & & U^{-t} \end{array}\right) = (b_1, \ldots, b_i, c, \ldots)$$

is a basis, since the matrix is unimodular.

On the other hand, if we can supplement to a basis, then we can revert the argument. □

LEMMA 3.15: Let Λ be a k-dimensional lattice in $\mathbb{R}^n$. Then

(1) There exist $y_i \in \Lambda$ lin. indep. such that $\|y_i\|^2 = M_i$
(2) Let $v \in \Lambda$ be such that $\|v\|^2 = M_1$, then there is a basis $v = b_1$, …, b_k for Λ.

PROOF. (1): induction on i. $i = 1$ is obvious. Now assume we have $y_1, \ldots, y_i$ such that $M_j = \|y_j\|^2$ for $j \leq i$ and we have $x_1, \ldots, x_{i+1}$ independent such that $\|x_j\|^2 \leq M_{i+1}$ for all j. Then there is some index l such that $y_1, \ldots, y_i, x_l$ are independent, wlog $l = i + 1$. Now either $\|x_l\|^2 = M_{i+1}$ and we're done, or $\|x_l\|^2 < M_{i+1}$, but then $M_{i+1-r} < M_{i+1-r+1} = \ldots = M_{i+1}$ but $y_1, \ldots, y_{i+1-r}, x_l$ are independent and too short.

(2): follows from 3.14 since for any minimal element, the gcd of the coefficients has to be 1. □

EXAMPLE 3.16: In general, we cannot find a basis consisting of minima: Let $\Lambda := \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 + \mathbb{Z}e^4 + 1/2\mathbb{Z}(e_1 + e_2 + e_3 + e_4 + e_5) \subseteq \mathbb{R}^5$. Then $e_5 \in \Lambda$, so clearly $M_i = 1$ for all i, however any basis must have the $1/2$ somewhere...

A slightly more careful analysis shows that for $n \leq 4$ we can always find a minimal basis, but for $n \geq 5$ in general not.

THEOREM 3.17: There exists $C_k \in \mathbb{R}$ such that for all k-dimensional lattices

$$M_1(\Lambda)^k \leq C_k^k d(\Lambda)^2$$

PROOF. We show that $C_k := (4/3)^{1/2(k-1)}$ works. Induction on k. For $k = 1$ this is trivial: $\Lambda = \mathbb{Z}b$, $M_1 = \|b\|^2$ and $d(\Lambda)^2 = \det b^t b = \|b\|^2$, so $C_1 = 1$ works.

Now, let $k > 1$ and fix a basis b_i with $\|b_1\|^2 = M_1$. Now

$$f(x) := f(x_1, \ldots, x_k) = \|\sum x_i b_i\|^2 = \sum x_i x_j b_i^t b_j$$

then, using the quadratic supplement,

$$f(x) = M_1(x_1 + \sum_{j=2}^{k} q_{i,j} x_j)^2 + g(x_2, \ldots, x_k)$$

for some quadratic form g. Let A be a matrix for f and B a matrix for g. Then $\det A = d(\Lambda)^2$ and $\det B = d(\Lambda)^2/M_1$. Let $y_2, \ldots, y_k \in \mathbb{Z}$ such that

$$g(y_2, \ldots, y_k) = \min\{g(x_2, \ldots, x_k) | 0 \neq (x_2, \ldots, x_k) \in \mathbb{Z}^{k-1}\}$$

The induction hypothesis shows

$$g(y_2, \ldots, y_k)^{k-1} \leq C_{k-1}^{k-1} d(\Lambda)^2 / M_1$$

Now choose $y_1 \in \mathbb{Z}$ such that $|y_1 + \sum_{i=2}^{k} q_{1,j} y_j| \leq 1/2$, then $\sum y_i b_i \neq \Lambda \setminus \{0\}$ and

$$M_1 \leq f(y) \leq 1/4 M_1 + (C_{k-1}^{k-1} d(\Lambda)^2 / M_1)^{1/(k-1)}$$

Hence (subtract $1/4 M_1$ and divide by $3/4$):

$$M_1 \leq \frac{4}{3}(C_{k-1}^{k-1} d(\Lambda)^2 / M_1)^{1/(k-1)}$$

Powering my $k - 1$ and multiplication by M_1:

$$M_1^k \leq (\frac{4}{3})^{k-1} C_{k-1}^{k-1} d(\Lambda)^2$$

Since $(\frac{4}{3})^{k-1} C_{k-1}^{k-1} = C_k^k$ we're done. Note $(k-1) + 1/2(k-2)(k-1) = (k-1)(1 + 1/2(k-2)) = (k-1)1/2k$. □

The *Hermite-constants* γ_k are defined as the smallest C_k such that the above theorem holds, i. e. γ_k is minimal sth.

$$M_1^k \leq \gamma_k^k d(\Lambda)^2$$

for all k-dim. lattices Λ. Clearly, $\gamma_k \leq C_k$.

THEOREM 3.18: Let Λ be a k-dim. lattice, then

$$\prod_{i=1}^{k} M_i \leq \gamma_k^k d(\Lambda)^2$$

PROOF. Let $y_i \in \Lambda$ be lin. indep. such that $\|y_i\| = M_i$ and $Q \in \mathrm{Gl}(k, \mathbb{Q})$ such that $(b_1, \ldots, b_k) = (y_1, \ldots, y_k)Q$, set $Y := (y_i^t y_j)_{i,j}$ and $B := (b_i^t b_j)_{i,j}$. For any $x \in \Lambda$ we now get two-representations:

$$x = \sum x_{b,i} b_i = \sum x_{y,i} y_i$$

where $x_{b,i} \in \mathbb{Z}$ and $x_{y,i} \in \mathbb{Q}$. Now

$$\begin{aligned} \|x\|^2 &= (x_{b,1}, \ldots, x_{b,k}) B (x_{b,1}, \ldots, x_{b,k})^t \\ &= (x_{y,1}, \ldots, x_{y,k}) Q B Q^t (x_{y,1}, \ldots, x_{y,k})^t \\ &= (x_{y,1}, \ldots, x_{y,k}) Y (x_{y,1}, \ldots, x_{y,k})^t =: f(x_{y,1}, \ldots, x_{y,k}) \end{aligned}$$

Next, we apply quadratic supplement to f to obtain

$$f(x_{y,1}, \ldots, x_{y,k}) = \sum q_{i,i} (x_{y,i} + \sum_{j>i} q_{i,j} x_{y,j})^2 =: \sum g_i(x_{y,i}, \ldots, x_{y,k})$$

and note that $\prod q_{i,i} = \det Y$. We now define a new quadratic form

$$h(x_1, \ldots, x_k) := \sum \frac{1}{M_i(\Lambda)} g_i$$

Let C be an associated matrix, then

$$\det C = \det Y \prod 1/M_i(\Lambda) = \det B / \det Q^2 \prod 1/M_i.$$

Now we apply the previous theorem to get

$$\min\{z^t Q C Q^t z : 0 \neq z \in \mathbb{Z}^k\}^k \leq \gamma_k^k \det(Q^2 C) = d(\Lambda)^2 / \prod M_i$$

So we still need to show is that the minimum is at least 1. Take any $0 \neq x \in \Lambda$, then $(x_{x,i}, \ldots, x_{x,k}) Q C Q^t (x_{x,i}, \ldots, x_{x,k})^t = h(x_{y,1}, \ldots, x_{y,k})$. Now find m maximal such that $x_{y,m} \neq 0$, then

$$\begin{aligned} h(x_{y,1}, \ldots, x_{y,k}) &= \sum_{i=1}^{m} \frac{1}{M_i} g_i(x_{y,i}, \ldots, x_{y,k}) \\ &\geq \sum_{i=1}^{m} \frac{1}{M_m} g_i(x_{y,i}, \ldots, x_{y,k}) \\ &= \frac{1}{M_m} \sum_{i=1}^{k} g_i(x_{y,i}, \ldots, x_{y,k}) \\ &= \frac{1}{M_m} f(x_{y,1}, \ldots, x_{y,k}) \\ &\geq \frac{M_m}{M_m} = 1 \end{aligned}$$

Here we used that x is lin. indep to y_1, …, y_{m-1} since $x_{y,m} \neq 0$, hence $f(x) \geq M_m$. □

3. LLL

Let $b_1, \ldots, b_k$ be a basis for $\Lambda \subseteq \mathbb{R}^n$, then we perform Gram-Schmidt orthogonalisation: Set $b_1^* := b_1$, $\mu_{i,j} := b_i^t b_j^* / \|b_j^*\|$, and $b_j^* := b_j = \sum \mu_{i,j} b_j^*$. Then (b_i^*) are an orthogonal basis (but in general not an orthonormal basis). We fix b_i, b_i^* and $\mu_{i,j}$ throughout this section.

THEOREM 3.19 (Hadamard inequality):

$$d(\Lambda) \leq \prod \|b_i\|$$

PROOF. From the construction of b_i^* we have $Q \in \mathrm{Gl}(n, \mathbb{Q})$ such that

$$(b_1^*, \ldots, b_k^*) = (b_1, \ldots, b_k)Q$$

and $\det Q = 1$. Furthermore: $\|b_i^*\| \leq \|b_i\|$ since

$$\begin{aligned} \|b_i\| &= \|b_i^* + \sum \mu_{i,j} b_j^*\| \\ &= \|b_i^*\| + \sum |\mu + i, j| \|b_j^*\| \geq \|b_i^*\| \end{aligned}$$

since the vectors are orthogonal. Finally

$$d(\Lambda)^2 = \det(b_i^t b_j) = \det Q^2 \det((b_i^*)^t b_j^*) = \prod \|b_i^*\|$$

and we're done. □

REMARK 3.20: (1) We have, in total,

$$d(\Lambda)^2 \leq \prod_{i=1}^{k} M_i \leq \gamma_k^k d(\Lambda)^2$$

(2) The exact values for γ_k^k are only known in a few cases:

n	1	2	3	4	5	6	7	8	24
γ_k^k	1	4/3	2	4	8	64/3	64	256	4^{24}

(3) The best general estimate is due to Blichfeld

$$\gamma_k^k \leq (\frac{2}{\pi})^k \Gamma(1 + \frac{k+2}{2})^2$$

(4) For $n = 24$, the extremal lattice giving γ_{24} is the (in)famous Leech-lattice. It boasts 196,560 shortest vectors (of length 2).

DEFINITION 3.21: A basis $b_1, \ldots, b_k$ is called *LLL-reduced* iff

(1) $|\mu_{i,j}| \leq 1/2$ for $1 \leq j < i \leq k$

(2) $\|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2 \geq \frac{3}{4} \|b_{i-1}^*\|^2$

LLL after the 3 inventors: A. Lenstra, H.W. Lenstra and L. Lovács. This was originally part of polynomial factorisation.

THEOREM 3.22: Let $b_1, \ldots, b_k$ be LLL-reduced. Then

(1) $\|b_j\|^2 \leq 2^{i-1} \|b_i^*\|$ for $1 \leq j < i \leq k$

(2) $d(\Lambda) = \prod \|b_i^*\| \leq \prod \|b_i\| \leq 2^{1/4k(k-1)} d(\Lambda)$

(3) $\|b_i\| \leq 2^{1/4(k-1)} d(\Lambda)^{1/k}$

(4) Let $x_1, \ldots, x_t \in \Lambda$ lin. indep., then for $j \leq t$:

$$\|b_i\|^2 \leq 2^{k-1} \max(\|x_1\|^2, \ldots, \|x_t\|^2)$$

In particular, b_1 is a "good" "approximation" to a shortest vector.

PROOF. The proof is long and tedious, but simple. Furthermore, we have already done it in PraMa, so I omit it. □

ALGORITHM 3.23 (LLL-Algorithm): A simple algorithm to compute the LLL reduced basis. By now, we actually have much more sophisticated algorithms available, but for not too large input this is still fine.

Input: $b_1, \ldots, b_k$ a basis for Λ
Output: a LLL-reduced basis $(c_i)_i$.
1: $c_i := b_i$, $C_i := \|c_i^*\|$, $m := 2$
2: $l := m - 1$
3: if $|\mu_{m,l}| > 1/2$, then $r := \lfloor \mu_{m,l} + 1/2 \rfloor$, $c_m := c_m - rc_l$ and update c_i^*, C_i accordingly. If $l < m - 1$ then goto 5
4: if $C_m < (3/4 - \mu_{m,m-1}^2) C_{m-1}$, then goto 6
5: $l := l - 1$. If $l > 0$ goto 3. If $m = k$ then end, else $m := m + 1$ and goto 2.
6: swap c_{m-1} and c_m and update the μ and C. If $m > 2$ then $m := m - 1$. Goto 2

In PraMa our proof was only valid for lattices in $\mathbb{Z}^n$ due to the lack of the successive minima. Here we can fill the gap.

PROOF. We only show the termination, as by construction the basis returned will be LLL-reduced.

Set $\Lambda_i := \dot{+}\mathbb{Z}c_i$ a sublattice of Λ, $D_i := d(\Lambda_i)^2 = \prod_{j=1}^{i} C_j$. By 3.17 we have

$$M_1(\Lambda) \leq M_1(\Lambda_i) \leq \gamma_i d(\Lambda_i)^{2/i} = \gamma_i D_i^{1/i}$$

In step 6, we change D_{m-1} by a factor of at least $3/4$ since the new C_{m-1} will be shorter by such a factor. Since we have a global lower bound on the D_i, this cannot happen too often. □

It is not too hard to believe that the algorithm takes only a polynomial number of steps, however to control the size (or precision) of the objects is harder.

There is a generalisation of the LLL, the MLLL (modified LLL) by M. Pohst that takes dependent input. While the algorithm is easy to state, the correct proof of termination is not.

4. Orders

Let $\mathcal{O} \subseteq L$ be an order and recall that we have the conjugates

$$(.)^{(i)} : L \to \begin{cases} \mathbb{R} & i \leq r_1 \\ \mathbb{C} \end{cases}$$

that we sorted to have $(.)^{(r_1+i)} = \overline{(.)^{(r_1+r_2+i)}}$.

Let $c_i := \begin{cases} 1 & i \leq r_1 \\ 2 & \text{otherwise} \end{cases}$ and define

$$T_2(\alpha) := \sum_{i=1}^{n} |\alpha^{(i)}|^2 = \sum_{i=1}^{r_1+r_2} c_i |\alpha^{(i)}|^2$$

the *T-two-norm* of α. Careful: this is *not* a norm in any normal sense, although $\sqrt{T_2}$ is a proper (euclidean) norm.

For any $\lambda_i > 0$ such that $\lambda_{r_1+i} = \lambda_{r_1+r_2+i}$, we also define

$$T_{2,\lambda}(\alpha) := \sum \lambda_i |\alpha^{(i)}|^2$$

In order to get lattices, we also define

$$\begin{aligned} \Psi_\lambda L \to \mathbb{R}^n : \alpha \mapsto (&\lambda_1 \alpha^{(1)}, \dots, \lambda_{r_1} \alpha^{(r_1)}, \\ &\lambda_{r_1+1} \Re(\alpha^{(r_1+1)}), \lambda_{r_1+1} \Im(\alpha^{(r_1+1)}), \dots, \lambda_{r_1+r_2} \Im(\alpha^{(r_1+r_2)})) \end{aligned}$$

and

$$\begin{aligned} \Psi_{\sqrt{2},\lambda} L \to \mathbb{R}^n : \alpha \mapsto (&\lambda_1 \alpha^{(1)}, \dots, \lambda_{r_1} \alpha^{(r_1)}, \\ &\sqrt{2}\lambda_{r_1+1} \Re(\alpha^{(r_1+1)}), \sqrt{2}\lambda_{r_1+1} \Im(\alpha^{(r_1+1)}), \dots, \sqrt{2}\lambda_{r_1+r_2} \Im(\alpha^{(r_1+r_2)})) \end{aligned}$$

to get

$$\|\Psi_{\sqrt{2},\lambda}(\alpha)\|^2 = T_{2,\lambda}(\alpha)$$

Theorem 3.24: Ψ_λ and $\Psi_{\sqrt{2},\lambda}$ are $\mathbb{Q}$-linear maps form $L \to \mathbb{R}^n$. For any order $\mathcal{O}$ the image $\Psi_\lambda(\mathcal{O}) =: \Lambda$ is a lattice with discriminant

$$d(\Lambda) = \frac{1}{2^{r_2}} \prod_{i=1}^{r_1} \lambda_i \prod_{i=1}^{r_2} \lambda_{r_1+i}^2 \sqrt{|\operatorname{disc}(\mathcal{O})|} = \frac{1}{2^{r_2}} \prod_{i=1}^{n} \lambda_i \sqrt{|\operatorname{disc}(\mathcal{O})|}$$

Proof. We know, $\operatorname{disc} \mathcal{O} = \det((\omega_i^{(j)})_{i,j})^2 =: \det \Omega^2$ for any integral basis. But for any complex z we have

$$\begin{pmatrix} z & \bar{z} \end{pmatrix} = \begin{pmatrix} \Re z & \Im z \end{pmatrix} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

Now

$$\begin{pmatrix}\Psi(\omega_1)\\ \cdots\\ \Psi(\omega_n)\end{pmatrix}\begin{pmatrix}1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 1 & 1 & & & \\ & & & i & -i & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & 1 \\ & & & & & & i & -i\end{pmatrix} = \Omega$$

Since $\det\begin{pmatrix}1 & 1\\ i & -i\end{pmatrix} = -2i$ we can easily read off the determinants. We note that the difference between Ψ and Ψ_λ is just a scaling by a diagonal matrix.

Since the determinants are non-zero, the vectors are $\mathbb{R}$-linear independent, hence the image is a lattice as claimed. □

LEMMA 3.25: For all $\alpha \in \mathcal{O}$ we have

$$(\prod \lambda_i |\alpha^{(i)}|^2)^{1/n} \leq \frac{1}{n} T_{2,\lambda}(\alpha)$$

Equality holds iff $\lambda_i|\alpha^{(i)}| = 1$ for all i.

PROOF. This is just the arithmetic-geometric means inequality. □

COROLLARY 3.26: (1) For all $\alpha \in \mathcal{O}$: $|N(\alpha)|^{2/n} \leq 1/nT_2(\alpha)$

(2) For all $0 \neq \alpha \in \mathcal{O}$:

$$n \leq T_2(\alpha)$$

(3) $M_1(\Psi_{\sqrt{2},1}(\mathcal{O})) = n$ since $T_2(1) = n$

CHAPTER 4

Units

1. Dirichlet

NOTATION 4.1: Let $L := \mathbb{Q}[\alpha] := \mathbb{Q}[t]/f$ be a number field. Then, in $\mathbb{C}$, the field of complex numbers, $f = \prod(t - x_i)$. We now sort the zeroes x_i to obtain $x_1, \ldots, x_{r_1} \in \mathbb{R}$ and $x_{r_1+1} = \bar{x}_{r_1+r_2+1}, \ldots x_{r_1+r_2} = \bar{x}_{r_1+2r_2} \in \mathbb{C} \setminus \mathbb{R}$. The pair (r_1, r_2) is called the *signature* of L.

For the rest of this chapter, we fix such a sorted set of conjugates.

LEMMA 4.2: Let $\mathcal{O}$ be some order in L, $c > 0$ be arbitrary and define $A := \{a \in \mathcal{O} \mid |a^{(i)}| \leq c \forall i\}$. Then A is a finite set.

PROOF. Follows from 3.24, only a re-statemant of the fact that $\Psi(\mathcal{O})$ is a lattice. □

LEMMA 4.3: Let $k \in \mathbb{N}$ be arbitrary and $\mathcal{O}$ any order in L. There there are only finitely many non-associate elements $a \in \mathcal{O}$ such that $|N(a)| = k$.

PROOF. Define $\mathfrak{a} := k\mathcal{O}$ and assume $a - b \in \mathfrak{a}$ and $|N(a)| = |N(b)| = k$. Then $a - b = rk$ and

$$\frac{a}{b} = \frac{rk + b}{b} = r\gamma + 1 \in R$$

since, by 1.32 $\gamma \in R$. Similarly, $b/a \in R$ as well, so a/b is a unit. Since $|\mathcal{O}/\mathfrak{a}| = k^n < \infty$ the lemma is proven. □

LEMMA 4.4: Let $\mathcal{O}$ be any order and $\alpha \in \mathcal{O}$, then the following are equivalent:

(1) There is some $k > 0$ such that $\alpha^k = 1$
(2) $|\alpha^{(i)}| = 1$ for all i
(3) $T_2(\alpha) = n$

REMARK 4.5: The set $TU(\mathcal{O}) := \{x \in \mathcal{O}^* | \exists k : x^k = 1\}$ is a finite cyclic subgroup of $\mathcal{O}$, the group of *torsion units*. (It's finite by the previous lemma and cyclic since it's finite and contained in L^*).

Since the group $\mathcal{O}^*$ is an abelian group, it is also a $\mathbb{Z}$-module. If we can show finite generation, this remark characterises the torsion submodule. The main problem is the free-part.

REMARK 4.6: If $r_1 > 0$, then $TU(\mathcal{O}) = \{\pm 1\}$ as the map $(.)^{(i)} : \mathcal{O} \to \mathbb{R}$ is injective and $TU(\mathbb{R}) = \{\pm 1\}$.

(In fact, this is true for almost all fields and orders, however, as the example of $\mathbb{Q}(\zeta_n)$ shows, clearly not always.)

DEFINITION 4.7: Let $\varepsilon_i \in \mathcal{O}^*$ be units. They are called *independent units* iff whenever for $m_i \in \mathbb{Z}$

$$\prod \varepsilon_i^{m_i} = 1$$

we automatically have $m_i = 0$ for all i. (so the ε_i are $\mathbb{Z}$-free in $\mathcal{O}^*$)

THEOREM 4.8: Let $1 \le i \le r_1 + r_2$ be fixed. Then there exists a unit $\varepsilon_i \in \mathcal{O}$ such that

$$\varepsilon_j^{(i)} \begin{cases} < 1 & j = i \\ > 1 & j \neq i \end{cases}$$

PROOF. Our proof will be a pure existence proof, although, by replacing Minkowski by LLL, it can be made constructive.

We will construct a sequence $\gamma_k \in \mathcal{O}$ such that

(1) $|\gamma_k^{(j)}| < |\gamma_{k+1}^{(j)}|$ for $i = j$
(2) $|\gamma_k^{(j)}| > |\gamma_{k+1}^{(j)}|$ for $i \neq j$
(3) $N(\gamma_k) \le C$ for some fixed C independent of k.

Once we have such a squence we will invoke 4.3 to find l and k such that γ_l and γ_k are associated. Their quotient is then the unit we want.

Let $c_{1,i} > 0$ be real numbers satisfying $\prod_{j=1}^n c_{1,j} = 2\sqrt{|d(\mathcal{O})|}$ and $c_{1,r_1+j} = c_{1,r_1+r_2+j}$. The set $C_1 := \{x \in \mathbb{R}^n | |x_j| \le c_{1,j}\}$ is clearly symmetric and convex. Furthermore, by construction, $\operatorname{Vol} C_1 = 2\sqrt{|d(\mathcal{O})|} = d(\Psi(\mathcal{O}))$. 3.11 then guarantees some non-trivial $\gamma_1 \in \mathcal{O}$ such that $\Psi(\gamma_1) \in C_1$. Now set $c_{2,j} := 1/2|\gamma_1^{(j)}|$ for all $j \neq i$ and $c_{2,i} \ge |\gamma_1^{(i)}|$ such that $\prod c_{2,j} = \prod c_{1,j}$ and $c_{2,r_1+j} = c_{r_1+r_2+j}$. This will also force (ii) to hold - eventually. Now 3.11 will find γ_2 with the required properties and we can iterate this procedure. □

This can be strengthend to:

THEOREM 4.9: Let $I \subset \{1, \dots, r_1 + r_2\}$ be a proper subset, then there exists a unit $\varepsilon_I \in \mathcal{O}$ such that

$$\varepsilon_I^{(i)} \begin{cases} < 1 & i \in I \\ \ge 1 & i \notin I \end{cases}$$

As we do not need this, we will not prove this. A constructive version of this was used originally to compute units, however, this is now superseded by the class group method later in the term. Unfortunately, the short version is still needed for the structure result. Once the structure is known, the computation will use different techniques.

In order to continue with the units, we need more lattices: Let $r := r_1 + r_2 - 1$ to define a new map:

$$L : K^* \to \mathbb{R}^r : \alpha \mapsto (c_i \log |\alpha^{(i)}|)_{1 \le i \le r}$$

This is a group homomorphism from K^* to $(\mathbb{R}^r, +)$. By 4.4 we have $\ker L|_{\mathcal{O}} = TU(\mathcal{O})$.

LEMMA 4.10: Let $\varepsilon \in \mathcal{O}^*$, then

$$\log|\varepsilon^{(r+1)}| = -1/c_{r+1}\sum_{i=1}^{r} c_i \log|\varepsilon^{(i)}|$$

PROOF. Trivial, since $|N(\varepsilon)| = 1$ □

LEMMA 4.11: Let $\varepsilon_i \in \mathcal{O}^*$ $(1 \leq i \leq r)$ be independent units and $\varepsilon \in \mathcal{O}^*$ an additional unit. Then $\{\varepsilon, \varepsilon_1, \ldots, \varepsilon_r\}$ is $\mathbb{Z}$-dependent.

PROOF. Clearly, $L(\varepsilon_1)$, ..., $L(\varepsilon_r)$, $L(\varepsilon)$ are $\mathbb{R}$-linear dependent (as $r+1$ vectors in $\mathbb{R}^r$), so we can write

$$L(\varepsilon) = \sum t_i L(\varepsilon_i)$$

for some $t_i \in \mathbb{R}$. Set now $m_i := -\lfloor t_i \rceil = -\lfloor t_i + 1/2 \rfloor$, then

$$L(\varepsilon) = \sum m_i L(\varepsilon_i) + \sum \underbrace{(t_i + m_i)}_{\in[1/2,1/2[} L(\varepsilon_i)$$

Set $\eta := \varepsilon \prod \varepsilon_i^{m_i}$, then

$$L(\eta) = \sum (t_i + m_i) L(\varepsilon_i)$$

hence $\|L(\eta)\| \leq 1/2 \sum \|L(\varepsilon_i)\|$ is bounded. Set

$$U_c := \{\varepsilon \in \mathcal{O}^* | \|L(\varepsilon)\| \leq c\}$$

then this is a finite set for all $c > 0$, since by 4.10 we get $\log|\varepsilon^{(r+1)}|$ is bounded as well, so all conjugates are bounded, hence since $\mathcal{O}$ is a lattice, this defines a finite set.

So far we have shown that for all $\varepsilon \in \mathcal{O}$ there is some linear combination of the ε_i such that

$$\varepsilon \prod \varepsilon_i^{m_i} \in U_c$$

where c is independent of ε. In particular, since U_c is finite, there are $i \neq j$ such that $\varepsilon^i \prod \varepsilon_i^{m_i} = \varepsilon^j \prod \varepsilon_i^{n_i}$, so

$$\varepsilon^{i-j} = \prod \varepsilon^{m_i - n_i}$$

as desired. □

THEOREM 4.12: Units ε_i are $\mathbb{Z}$-linear independent iff $L(\varepsilon_i)$ are $\mathbb{R}$-linear independent.

REMARK 4.13: For any independent set of units $\varepsilon_i \in \mathcal{O}^*$ $(1 \leq i \leq r)$ there is a finite set $U \subseteq \mathcal{O}^*$ of units, such that any unit ε can be decomposed into a product of ε_i and an additional unit $\in U$

LEMMA 4.14: (1) $M \in \mathbb{R}^{n\times n}$ be a *diagonally dominant matrix*, ie $|m_{i,i}| > \sum_{j\neq i} |m_{j,i}|$, then M has full rank.
(2) Let ε_i, $1 \leq i \leq r$ such that $\log|\varepsilon_i^{(i)}| > 1$ and $\log|\varepsilon_i^{(j)}| \leq 1$, $i \neq j$. Then the units are independent.

PROOF. (1) Assume $Mt = 0$ for $0 \neq t \in \mathbb{R}^n$. Fix k such that $|t_k|$ is maximal, then $\sum m_{k,i} t_i = 0 = t_k(m_{k,k} + \sum_{i\neq k} t_i/t_k m_{k,i})$ which is impossible since $|\sum_{i\neq k} t_i/t_k m_{k,i}| \leq \sum_{i\neq k} |m_{k,i}| < |m_{k,k}|$.

(2) Since $\sum_{i=1}^{r+1} c_i \log|\varepsilon^{(i)}| = 0$, the matrix $(L(\varepsilon_1), \ldots, L(\varepsilon_r)) \in \mathbb{R}^{r\times r}$ is diagonally dominant, hence of full rank, so the units are independent. □

THEOREM 4.15 (Dirichlet Unit theorem): Let $\mathcal{O}$ be an order, then there are units ζ, ε_1, ..., $\varepsilon_r \in \mathcal{O}^*$ such that

(1) $TU(\mathcal{O}) = \langle\zeta\rangle$
(2) $(\varepsilon_i)_i$ are free
(3) $\mathcal{O}^* = \langle\zeta, \varepsilon_1, \ldots, \varepsilon_r\rangle$

PROOF. We have shown in 4.13 that $\mathcal{O}/TU(\mathcal{O})$ is a finetely generated torsion free $\mathbb{Z}$-module, hence free. By 4.11 it is of rank at most r since any more are $\mathbb{R}$-linear thus $\mathbb{Z}$-linear dependent. Finally, by 4.14 we have r independent units, so $\mathcal{O}^*/TU(\mathcal{O})$ is free of rank r as stated. □

DEFINITION 4.16: The previous theorem also shows that $L(\mathcal{O}^*)$ is a lattice of rank r. We call $d(L(\mathcal{O}^*)) =: \operatorname{reg}\mathcal{O}$ the *regulator* of $\mathcal{O}$. In abuse of notation, $\operatorname{reg} L := \operatorname{reg}\mathbb{Z}_L$ as usual.
Furthermore, for any independent units ε_1, ..., ε_r we define $\operatorname{reg}(\varepsilon_1, \ldots, \varepsilon_r) := d(\langle L(\varepsilon_1), \ldots, L(\varepsilon_r)\rangle) = |\det(L(\varepsilon_1), \ldots, L(\varepsilon_r))|$
A maximal system of independent units ε_i is called *fundamental* if

$$\langle TU(\mathcal{O}), \varepsilon_i | i\rangle = \mathcal{O}^*.$$

REMARK 4.17: The regulator is actually well defined and does not depend on the ordering of the conjugates.

Algorithmically, computing $\mathcal{O}^*$ is broken down into several steps:

(1) Find (somehow) lots of units $\varepsilon \in \mathcal{O}^*$ - we'll come back to this later. One option clearly is to follow the proof above, but it's not very efficient.
(2) Find (somehow) the dependencies between the units, eg. using $\mathbb{R}$-linear algebra on the L-side
(3) Deduct a basis for the group generated by the units using the relations
(4) Decide that the group is complete - or enlarge it

Since the larger the unit group, the smaller its regulator, the last step can be achieved by using (universal) lower bounds for regulators paired with some enlargement technique.

2. Lower Regulator Bound

Define

$$L_2 : K^* \to \mathbb{R}^n : \alpha \mapsto (\log|\alpha^{(i)}|)_{1\le i\le n}$$

and fix some (unkown) system of fundamental units E_1, ..., E_r. Then for any unit $\varepsilon = \zeta^? \prod E_i^{m_i}$ we get

$$\|L_2(\varepsilon)\| = (m_i)_i^t A (m_i)_i$$

for some sym. pos. def. matrix $A = (L_2(E_i)^t L_2(E_j))_{i,j}$. Computing carefully (due to the missing c_i), one sees

$$\det A = \frac{n \operatorname{reg}^2 \mathcal{O}}{2^{r_2}}$$

and thus, using the successive minima:

$$\operatorname{reg}^2 \mathcal{O} \ge \frac{2^{r_2} \prod M_i(A)}{n\gamma_r^r}$$

So, to get a "good" lower bound for reg we need the minima - but the minima for an unknown lattice. So we need to explore the link between $\Psi(\mathcal{O})$ and $L_2(\mathcal{O}^*)$, since the former is known. Since log is monotonous, we expect a link.

LEMMA 4.18: Let

$$\begin{aligned} f: &\ x \mapsto \sum x_i^2 \\ g_1: &\ x \mapsto \sum x_i \\ g_2: &\ x \mapsto \sum \exp(2x_i) \\ g_3: &\ x \mapsto \sum \exp(-2x_i) \end{aligned}$$

Then the minimum of $f : \mathbb{R}^n \to \mathbb{R}$ under the constraints $g_1(x) = 0$, $g_{2,3}(x) \geq M$ and x has at least $\lceil n/2 \rceil$ pos. entries satisfies

$$\min f \geq \frac{n}{4} \log(\frac{M}{n} + \sqrt{(\frac{M}{n})^2 - 1}) = \frac{n}{4} \operatorname{arcosh}^2(\frac{M}{n})$$

A minimum x has at most 3 different values.

PROOF. Via Lagrange multipliers. □

LEMMA 4.19: Let $x = (x_1, \ldots, x_n)$ be such $x_1 =, \ldots, = x_i > 0$, $x_{i+1} =, \ldots, = x_{i+j} = 0$ and $x_{i+j+1} = \ldots = x_n < 0$ satisfying $g_1(x) = 0$, $g_{2,3}(x) \geq M$. Then

$$f(x) \geq \frac{n-j}{4} \operatorname{arcosh}^2(\frac{M-j}{n-j})$$

PROOF. Via last lemma. □

LEMMA 4.20: The function

$$j \mapsto \frac{n-j}{4} \operatorname{arcosh}^2(\frac{M-j}{n-j})$$

is decreasing for $M/n \geq 1 + \sqrt{2}$

PROOF. Simple exercise in calculus. □

THEOREM 4.21: Let $\varepsilon \in \mathcal{O}^*$ be unit such that $T_2(\varepsilon)$, $T_2(\varepsilon^{-1}) \geq M \geq 5/2n$. If at most j conjuagtes have $|\varepsilon^{(i)}| = 1$, then

$$\|L_2(\varepsilon)\| \geq \frac{n-j}{4} \operatorname{arcosh}^2(\frac{M-j}{n-j})$$

PROOF. Setting $x_i = \log |\varepsilon^{(i)}|$ this is just a re-statement of the previous lemmas. □

Set $S_M := \{x \in \mathcal{O} | T_2(x) \leq M\} \cup \{x \in \mathcal{O} | x^{-1} \in \mathcal{O}, T_2(x^{-1}) \leq M\}$, $M^* := \frac{n-j}{4} \operatorname{arcosh}^2(\frac{M-j}{n-j})$ for some suitable j, possible $j = n-2$ and finally

$$M_i^* := \begin{cases} \min(M^*, \min\{\lambda : \varepsilon_1, \ldots, \varepsilon_i \in S_\lambda \cap \mathcal{O}^* \text{indep.}) \\ M^* \end{cases}$$

THEOREM 4.22: Under the assumptions above, we have

$$\operatorname{reg}^2 \mathcal{O} \geq \prod M_i^* \frac{2^{r_2}}{n} \gamma_r^{-r}$$

Note: the above theorem is the best known general procedure to get "decent" lower bounds.

Note: one can show a universal lower bound:

$$\operatorname{reg} \mathcal{O} \geq 0.2052$$

for all orders $\mathcal{O}$ in any number field L.

3. p-maximal Unit Groups

How is this used?

Given a system of independent units $U = \langle \zeta, \varepsilon_i | i \rangle$ we want to know if $U = \mathcal{O}^*$ holds. Suppose $p|(\mathcal{O}^* : U)$, then we can find $\varepsilon \in \mathcal{O} \setminus U$ such that $\varepsilon^p \in U$.

DEFINITION 4.23: A subgroup $U \leq \mathcal{O}^*$ is called p-maximal iff

$$U = U_p := \{x \in \mathcal{O} | x^p \in U\}$$

Hence, the goal is to either compute U_p and/or verify $U = U_p$. Given that we don't know $\mathcal{O}^*$ we have to revert to the regulator bounds:

$$(\mathcal{O}^* : U) = \frac{\operatorname{reg} U}{\operatorname{reg} \mathcal{O}} \leq \frac{\operatorname{reg} U}{L}$$

where L is any lower bound for $\operatorname{reg} \mathcal{O}$. So, if $p|(\mathcal{O}^* : U)$, then $p \leq \operatorname{reg} U/L$ and we simply compute U_p for all such p, possibly enlarging U in the process.

To compute U_p, we are now going to revert this: $p|(\mathcal{O}^* : U)$ iff $U \neq U_p$, so we are systematically trying to find $x \in U$ such that

- $\sqrt[p]{x} \in \mathcal{O}$
- $x \notin U^p := \{y^p \mid y \in U\}$

Since clearly x works iff xy^p works, we "only" need to search in U/U^p which is a finite set.

LEMMA 4.24: The polynomial $f(t) := t^p - a \in L[t]$ is irreducible iff it has no roots.

PROOF. If we have a root, then clearly f is not irreducible. Now assume f has no roots and let $\Gamma := L[t]/f_i$ for an irreducible factor of f. Then, by assumption, $d := \deg f_i > 1$ and $N_{\Gamma/L}(t)^p = N(t^p) = N(a) = a^d$ showing that a^d is a p-th power as well. But either $p = d$ and f is irreducible, or $\gcd(p, d) = 1$, hence a is a p-th power and thus f has a root. □

THEOREM 4.25 (Frobenius, Cebotarev): Let K be a number field and $g \in \mathbb{Z}_K[t]$ be monic and irreducible of prime degree p. Then $\mathbb{Z}_K$ has infintely many prime ideals $\mathfrak{q}$ such that $\bar{g} \in (\mathbb{Z}_K/\mathfrak{q})[t]$ is irreducible.

PROOF. This comes from analytic theory, stronger statements are known. The frequency of such prime ideals does depend on the Galois group of g. □

There are even version of the theorem giving bounds on such ideals, however, those are too large to be useful here.

COROLLARY 4.26: Let $\varepsilon \in U \setminus U^p$, then ε is a p-th power in L iff $\bar{\varepsilon}$ is a p-th power for all $\mathfrak{p} \subset \mathbb{Z}_L$

Note: Since $(\mathbb{Z}_L^* : \mathcal{O}^*)$ is finite, we will have $\varepsilon \in \mathcal{O}^*$ such that ε is a p-th power in L, hence $\mathbb{Z}_L$, but not in $\mathcal{O}$.

We use this in the following algorithm:

ALGORITHM 4.27:

Input: A subgroup U of finite index in $\mathcal{O}^*$, a prime p.
Output: U_p
1: $V := U/U^p$
2: For lots of prime ideals $\mathfrak{q} \subset \mathcal{O}$ do
3: Let $\varphi_\mathfrak{q} : \mathcal{O} \to \mathcal{O}/\mathfrak{q} =: \mathbb{F}_\mathfrak{q}$ and $\tilde{\varphi}_\mathfrak{q} : U/U^p \to \mathbb{F}_\mathfrak{q}^*/(\mathbb{F}_\mathfrak{q}^*)^p$,
4: $V := V \cap \ker \tilde{\varphi}_\mathfrak{q}$
5: if V hasn't changed for several $\mathfrak{q}$, then leave the loop.
6: Fix a $\mathbb{F}_p$-free generating system $\bar{\eta}_i$ for V.
7: For each such η_i test if there is a $\gamma_i \in \mathcal{O}^*$ such that $\gamma_i^p = \eta_i$
8: $U_p = \langle U, \gamma_i | i \rangle$

The algorithm is obviously valid, but not complete. Missing are

(1) How do we find prime ideals $\mathfrak{q}$? We will answer this soon.
(2) How do we work in $\mathbb{F}_\mathfrak{q}$?
(3) There are lots of $\mathfrak{q}$ that are pointless to test, we need only $p|((\mathcal{O} : \mathfrak{q}) - 1)$
(4) How do we test for the γ?
(5) How many $\mathfrak{q}$ do we (expect to) need?

To compute the roots we can easily give a solution: Assume $\gamma^p = \eta$, then $|\gamma^{(i)}|^p = |\eta^{(i)}|$. Let $\lambda_i := \sqrt[-p]{|\eta^{(i)}|}$, then $T_\lambda(\gamma) = n$ and γ is a minimum of T_λ, hence the enumeration method will be able to find γ or show its non-existence.

Or:

Fix any prime ideal $\mathfrak{q}$ and compute all roots of $t^p - \eta$ in $\mathbb{F}_\mathfrak{q}$. For each such root r, use the Hensel/Newton procedure to compute γ such that $\gamma^p - r \in \mathfrak{q}^k$ for some huge k. Then use LLL to find a small representative $\tilde{\gamma}$ in the coset $\gamma + \mathfrak{q}^k$. If k is large enough, then $\tilde{\gamma}$ is unique the the root (if the root exists).

Both methods can be aided by a reduction procedure. The idea is to write a (large) unit η as a product

$$\eta = \prod \beta_i^{p^i}$$

where the β_i are "small". Then η is a p-power iff β_0 is. We'll come back to this later, as it will be useful in the context of class groups as well.

CHAPTER 5

Dedekind Domains and the Class Group

1. Dedekind Domains

DEFINITION 5.1: Let R be a comm. and unitary domain, $\{0\} \neq B \subseteq Q(R)$ such that $aB \leq R$ for some $0 \neq a \in R$, then B is called a *fractional ideal*. A fractional ideal A is called invertible if there is some fractional ideal B such that $AB := \{\sum_{\text{fin.}} a_i b_i \mid a_i \in A, b_i \in B\} = R$

The fractional ideals clearly form a semi-group, even a monoid. Note: fractional ideals are *no* ideals in the usual sense. In what follows, the term ideal will always mean fractional ideal. A normal ideal is called *integral*.

THEOREM 5.2: Let R be comm. and unitary, then the following are equivalent:

(1) The fractional ideals form a group
(2) Every integral ideal is the product of prime ideals
(3) R is noetherian, integrally closed and all non-zero prime ideals are maximal.

Such a ring is called *Dedekind* ring.

REMARK 5.3: If R is Dedekind, then it is a domain, since zero-divisors would produce non-invertible principal ideals.

REMARK 5.4: Maximal orders $\mathbb{Z}_L$ are Dedekind.

Let R be a Dedekind ring with field of quotients $Q(R)$, then we define

$$I_R := \{A \mid A \text{ is a fractional ideal}\}$$

and

$$P_R := \{\alpha R \mid \alpha \in Q(R)^*\}$$

Then clearly $P_R \leq I_R$, hence

$$\mathcal{C}_R := I_R / P_R$$

the *class group* is a well defined abelian group. For a number field L with maximal order $\mathbb{Z}_L$ we define $I_L := I_{\mathbb{Z}_L}$, $P_L := P_{\mathbb{Z}_L}$ and $C_L := C_{\mathbb{Z}_L}$ The main goal is to understand $\mathcal{C}_L$, in particular $h_L := |\mathcal{C}_L|$ the *class number*. We will show that $h_L < \infty$. But first we'll deal with fractional ideals in more detail.

LEMMA 5.5: $A \subseteq Q(R)$ is a fractional ideal iff A is an R-module and $aA \subseteq R$ for some $a \neq 0$.

LEMMA 5.6: Let A, B fractional ideals then

(1) $A + B$, AB and $A \cap B$ are fractional ideals
(2) $A' := [R : A] = \{x \in Q(R) \mid xA \subseteq R\}$ is a fractional ideal
(3) If $AB = R$, then $B = A'$
(4) $A = (c)$, then A is invertible $A' = (1/c)$
(5) the invertible ideals form a group

PROOF. (1) clear

(2) Obviously, A' is an R-module. Let $y \in A \setminus \{0\}$, then we can find $0 \neq z \in \mathcal{O}$ such that $zy \in A \cap \mathcal{O}$, but then $zyA' \subseteq \mathcal{O}$ as required.

(3) Clearly, $B \subseteq A'$ and

$$\mathcal{O} = AB \subseteq AA' \subseteq \mathcal{O}$$

thus $AA' = \mathcal{O}$ as well, so

$$A' = A'\mathcal{O} = A'AB = \mathcal{O}B = B$$

(4), (5) clear. □

REMARK 5.7: If R is PID, then every non-zero ideal is invertible.

LEMMA 5.8: Let R be an integral domain.
(1) Let $A_1, \ldots, A_r$ be ideals and Q a prime ideal such that $\prod A_i^{v_i} \subseteq Q$ for some $v_i \geq 0$. Then there is some k such that $A_k \subseteq Q$
(2) Let $\mathfrak{a}$ be an integral ideal and assume $\mathfrak{a} = \prod \mathfrak{p}_i^{v_i}$ for invertible prime ideals $\mathfrak{p}_i$ and $v_i \in \mathbb{Z}$. Then the factorisation is essentially unique (up to re-ordering).

PROOF. (1) Assume this is wrong, i. e. for all j we have $A_j \not\subseteq \mathfrak{q}$, then we can find $a_i \in \mathfrak{a}_i \setminus \mathfrak{q}$ and $\prod a_i^{v_i} \in \prod A_i^{v_i} \subseteq \mathfrak{q}$ contradicting $\mathfrak{q}$ being prime.

(2) Let $A = \prod \mathfrak{p}_i^{v_i} = \prod \mathfrak{q}_i^{u_i}$ be two factorisations. Let $\mathfrak{q}_1$ be a minimal prime ideal wrt. containment among the $\mathfrak{q}_i$. Then clearly $A = \prod \mathfrak{q}_i^{u_i} \subseteq \mathfrak{q}$, hence by (1), we have some $\mathfrak{p}_i \subseteq \mathfrak{q}_1$. Now we multiply both sides by $\mathfrak{q}_1'$ and recurse. □

REMARK 5.9: In a Dedekind ring R, every fractional ideal has a unique decomposition into prime ideals - with possibly negative exponents.

DEFINITION 5.10: Let R be a Dedekind domain and A, B fractional ideals. Then
(1) $A|B$ iff there is some $C \leq R$ such that $AC = B$
(2) C is called the *greatest common divisor*, gcd of A and B iff $C|A$, $|B$ and for all $D|A$, $D|B$ we also have $D|C$

LEMMA 5.11: Let R be a Dedekind ring and A, B fractional ideals.
(1) $A|B$ iff $B \subseteq A$
(2) $\gcd(A, B) = A + B$

PROOF. (1) If $A|B$ then we have $C \subseteq R$ such that $AC = B$, but clearly $B = AC \subseteq A$.

If $B \subseteq A$ then $BA' \subseteq AA' = R$, hence using $C := BA'$ we get $AC = AA'B = B$ as claimed.

(2) From (1): A, $B \subseteq \gcd(A, B)$, hence $A + B \subseteq \gcd(A, B)$ as well. On the other hand, A, $B \subseteq A + B$, hence $A + B|A$, B so $A + B|\gcd(A, B)$ or $\gcd(A, B) \subseteq A + B$ and equality everywhere. □

LEMMA 5.12: Let R be a Dedekind ring, then R is UFD iff $h_R = 1$, ie iff R is PID.

PROOF. We need to show that UFD implies PID if R is Dedekind. Specifically, we want to show that every prime ideals is principal. Let $0 \neq \mathfrak{p}$ be a prime ideal and choose $0 \neq p \in \mathfrak{p}$, then $pR \subseteq \mathfrak{p}$ and $p = \varepsilon \prod \pi_i^{k_i}$ Thus also $pR = \langle p \rangle = \prod \langle \pi_i \rangle^{k_i} \subseteq \mathfrak{p}$. By 5.8(1) we find $\langle \pi_\mu \rangle \subseteq \mathfrak{p}$ for some μ, sice $\langle \pi_\mu \rangle$ is a non-zero prime ideal, it is maximal (since R is Dedekind), so $\langle \pi_\mu \rangle = \mathfrak{p}$. Since the product of principal ideals is principal, and every ideal is a unique product of primes, every ideal is principal. □

THEOREM 5.13: Let $0 \neq A \subseteq R$ be an ideal in the Dedekind ring R and $0 \neq a \in A$ be arbitrary. Then there exists some $b \in A$ such that $A = \langle a, b \rangle$.

PROOF. We have $A = \prod \mathfrak{p}_i^{v_i}$ and, since $a \in A$, so $A | aR$ we get $aR = \prod \mathfrak{p}_i^{v_i + l_i} \prod \mathfrak{q}_i^{o_i}$. Now use the CRT to find $b \equiv x_i \bmod \mathfrak{p}_i^{v_i+1}$ for $x_i \in \mathfrak{p}_i^{v_i} \setminus \mathfrak{p}_i^{v_i+1}$ and $b \equiv 1 \bmod \mathfrak{q}_i$. Then $A = \langle a, b \rangle$. □

LEMMA 5.14: Let R be a Dedekind ring, A, $B \leq R$ non-trivial ideals. Then we can find $C \leq R$ such that $\gcd(C, AB) = R$ and AC is a principal ideal.

PROOF. Write $A = \prod \mathfrak{p}_i^{\mu_i}$ and $B = \prod \mathfrak{p}_i^{\nu_i}$, now choose $x_i \in \mathfrak{p}_i^{\mu_i} \setminus \mathfrak{p}_i^{\mu_i+1}$ and use CRT to find $x \equiv x_i \bmod \mathfrak{p}_i^{\mu_i+1}$, so that $x \in \mathfrak{p}_i^{\mu_i} \setminus \mathfrak{p}_i^{\mu_i+1}$ for all i. For the factorisation we therefore get $xR = \prod \mathfrak{p}_i^{\mu_i} \prod \mathfrak{q}_i^{l_i} =: AC$ □

LEMMA 5.15: Let R be a Dedekind ring, $\mathfrak{p}$ a non-zero prime ideal and $N \geq 0$, then

$$(R/\mathfrak{p}, +) \cong (\mathfrak{p}^n/\mathfrak{p}^{n+1}, +)$$

PROOF. Choose any $a \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$ and define

$$\varphi : (R, +) \to (\mathfrak{p}^n/\mathfrak{p}^{n+1}, +) : x \mapsto ax$$

which clearly is a group homomorphism with kernel

$$\ker \varphi = \{x \mid ax \in \mathfrak{p}^{n+1}\}$$

since $ax \in \mathfrak{p}^{n+1}$ is equivalent to $\mathfrak{p}^{n+1} | axR$ and since $\mathfrak{p}^n | aR$, $\mathfrak{p}^{n+1} \not| aR$ we get $\mathfrak{p} | xR$ or $x \in \mathfrak{p}$. Next, we'd like to show that φ is surjective. Let $y \in \mathfrak{p}^n$ be arbitrary. Since $\mathfrak{p}^n = \gcd(aR, \mathfrak{p}^{n+1}) = aR + \mathfrak{p}^{n+1}$ we can write $y = ax + p$ for some $p \in \mathfrak{p}^{n+1}$ as claimed. □

DEFINITION 5.16: Let R be a comm and unitary ring and $A \leq R$ an ideal. Then $N(A) := |R/A|$ (which can be infinite) is called the *norm* of A.

COROLLARY 5.17: Let R be a ring such that $N(A) < \infty$ for all non-trivial ideals A. Then

(1) $N(A) \in A$ since by construction, $N(A)$ is an exponent for the finite ring R/A giving $N(A)r \in A$ for all $r \in R$.
(2) If $\mathfrak{p}$ is a prime ideal, then $N(\mathfrak{p}) = p^k$ for some prime number p (since R/A is a finite integral domain, hence a field)

In particular, for any order $\mathcal{O}$ we know that $N(A)$ is finite.

THEOREM 5.18: Let A, B be ideals in the Dedekind ring R, then

$$N(A)N(B) = N(AB)$$

PROOF. Exercise. □

Remark: a slightly more careful analysis shows that the norm is multiplicative on *invertible* ideals in arbitrary orders.

LEMMA 5.19: Let $\mathfrak{p}$ be a non-zero prime ideal in some order $\mathcal{O}$, then
(1) $x^{N(\mathfrak{p})} \equiv x \bmod \mathfrak{p}$ for all $x \in \mathcal{O}$
(2) $N(\mathfrak{p}) = \min\{k \mid x^k \equiv x \bmod \mathfrak{p} \forall x \in \mathcal{O}\}$

PROOF. Under our assumption, $R/\mathfrak{p}$ is a finite field with p^k elements, thus $(R/\mathfrak{p})^*$ is a cyclic group of order $p^k - 1$. □

LEMMA 5.20: The set
$$\{A \leq \mathcal{O} \mid N(A) \leq B\}$$
is finite for all $B > 0$ and any order $\mathcal{O}$

PROOF. Let $(\omega_i)_i$ be a fixed basis for $\mathcal{O}$, then any ideal A can be represented using a unique HNF basis wrt ω_i. Since the product of the diagonal elements is the norm, the bound on the norm bounds all diagonal elements. The off-diagonal elements are rescticted by the diagonal, given a finite total number. □

Note: in the case of $\mathcal{O}$ being integrally closed (Dedekind) we can argue differently: We know that every prime ideal contains a prime-number, 2.12 shows that at most n prime ideals share the same prime number. The norm is multiplicative (in this case), so any ideal of norm $N(A) \leq B$ is the product of prime ideals containing primes $p \leq B$. So this involves only finitely many prime-numbers, hence finitely many prime ideals.

THEOREM 5.21: For any number field L there is a constant C_L such that for any ideal A we can find an integral ideal B such that

(1) $A = \alpha B$ for some $\alpha \in L$
(2) $N(B) \leq C_L$

PROOF. Wlog. assume that A is integral already. Set $B := A^{-1}$ such that $AB = \mathcal{O}$ and choose μ as the 1st basis element of a LLL basis for $\Psi(\mathcal{O})$. Then
$$T_2(\mu) = \|\Psi(\mu)\|^2 \leq 2^{(n-1)/2}(|d_L|)^{1/n}N(B)^{2/n}$$
thus, using 3.26:
$$|N(\mu)|^2 \leq (T_2(\mu)/n)^n \leq 2^{n(n-1)/2}|d_L|N(B)^2$$
Finally, note $A\mu \subseteq \mathcal{O}$ since $\mu \in A^{-1}$, $N(B) = 1/N(A)$ and
$$N(A\mu) = N(A)|N(\mu)| \leq 2^{n(n-1)/4}|d_L|^{1/2}$$
as claimed. □

COROLLARY 5.22: For any number field L, we have $h_L < \infty$.

PROOF. By 5.21 any ideal class has an integral representative of norm $\leq C_L$, by 5.20 this is a finite set. □

THEOREM 5.23 (Minkowski): Every ideal class in every number field L contains an integral representative A of norm

$$N(A) \leq \frac{n!}{n^n}(\frac{4}{\pi})^{r_2}\sqrt{|d_L|}$$

Note: $M_L := \frac{n!}{n^n}(\frac{4}{\pi})^{r_2}\sqrt{|d_L|}$ is called the *Minkowski-bound* of L. The (omitted) proof defines a fairly complicated convex symetric set C_L to invoke Minkowski's convex body theorem to replace the μ used in the proof of 5.21.

Note: in both 5.21 and 5.23, the constants are of the form $C = C(n)\sqrt{|d_L|}$. In fact all bounds known that do not depend on the GRH are of this form - with various $C(n)$s. Minkoswki is much better than the LLL-based one, but both are too large for interesting fields. We'll come back to this problem later.

COROLLARY 5.24: For all number fields $L \neq \mathbb{Q}$ we have $|d_L| > 1$

2. Primes in Extensions

In order to compute class groups, we need to get a handle on ideals, in particular on prime ideals in number fields.

LEMMA 5.25: For any $0 \neq a \in \mathcal{O} \subset L$ we have $|N(a)| = N(a\mathcal{O})$

PROOF. Let $\mathcal{O} = \dot{+}\mathbb{Z}\omega_i$, then $a\mathcal{O} = \dot{+}\mathbb{Z}a\omega_i$ hence $M_a = M_{a\mathcal{O}}$ and the statement follows. □

Note: for L/K a field extension, we also have $\mathbb{Z}_L \supset \mathbb{Z}_K$ and $\mathbb{Z}_L$ is a $\mathbb{Z}_K$ module (even a finitely generated one, as $\mathbb{Z}_L$ is fin. gen. over $\mathbb{Z}$), but no longer a free module, hence we have to be more careful with our module arguments.

LEMMA 5.26: Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}_K$ and $\mathfrak{q}$ be a prime in $\mathbb{Z}_L$, then the following are equivalent:

(1) $\mathfrak{p} \subseteq \mathfrak{q}$
(2) $\mathfrak{p} = \mathfrak{q} \cap K$
(3) $\mathfrak{p} = \mathfrak{q} \cap \mathbb{Z}_K$

In this case we say that $\mathfrak{q}$ lies *above* $\mathfrak{p}$ or that $\mathfrak{p}$ lies *below* $\mathfrak{q}$

PROOF. The only item worth mentioning is that we need that $\mathbb{Z}_K$ is integrally closed for (2) $\Rightarrow$ (3). □

DEFINITION 5.27: Let $\{0\} \neq \mathfrak{p}$ be a prime in $\mathbb{Z}_K$ and $\mathfrak{q} \leq \mathbb{Z}_L$ above, then

(1) $e := \max\{i \mid \mathfrak{q}^i | \mathfrak{p}\mathbb{Z}_L\}$ is called the ramification degree of $\mathfrak{q}$ over $\mathfrak{p}$, $e = e(\mathfrak{q}/\mathfrak{p})$
(2) $\mathfrak{q}$ is called *ramified* over $\mathfrak{p}$ iff $e(\mathfrak{q}/\mathfrak{p}) > 1$
(3) $\mathfrak{p}$ is called ramified in L/K iff exists some $\mathfrak{q}$ above $\mathfrak{p}$ such that $\mathfrak{q}$ is ramified over $\mathfrak{p}$

LEMMA 5.28: Let $\mathfrak{p}$ be a prime in $\mathbb{Z}_K$, then there exists some $\mathfrak{q}$ above $\mathfrak{p}$ in $\mathbb{Z}_L$.

PROOF. If $\mathfrak{p} = \{0\}$ the statment is trivial, hence assume $\mathfrak{p}$ to be non-trivial. In $\mathbb{Z}_K$ we have an ideal A such that $A\mathfrak{p} = \mathbb{Z}_{\mathbb{K}}$, hence we can find $\gamma \in A \setminus \mathbb{Z}_K$ such that $\gamma\mathfrak{p} \subseteq \mathbb{Z}_K$. So $\gamma\mathfrak{p}\mathbb{Z}_L \subseteq \mathbb{Z}_K\mathbb{Z}_L = \mathbb{Z}_L$. Suppose now that $\mathfrak{p}\mathbb{Z}_L$ is trivial, then $1 \in \mathfrak{p}\mathbb{Z}_L$, but then $\gamma \in \mathbb{Z}_L$, hence $\gamma \in \mathbb{Z}_K$ which is absurd. Since $\mathfrak{p}\mathbb{Z}_L$ is non-trivial, it has a non-trivial factorisation (or alternatively, there exists a maximal ideal containing $\mathfrak{p}\mathbb{Z}_L$). □

THEOREM 5.29: Let $\mathfrak{p}$ be a prime in $\mathbb{Z}_K$ and $\mathfrak{q} < \mathbb{Z}_L$ be a prime above it. Then

$$\chi : \mathbb{F}_\mathfrak{p} := \mathbb{Z}_K/\mathfrak{p} \to \mathbb{Z}_L/\mathfrak{q} =: \mathbb{F}_\mathfrak{q} : x + \mathfrak{p} \mapsto x + \mathfrak{q}$$

is a well defined field embedding, hence $\mathbb{F}_\mathfrak{p}$ is a subfield of $\mathbb{F}_\mathfrak{q}$. We call the degree $f := f(\mathfrak{q}/\mathfrak{p}) := \mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}$ the *inertia degree* of $\mathfrak{q}$ over $\mathfrak{p}$.

PROOF. Since $\mathfrak{p} \subseteq \mathfrak{q}$ the map is well defined and non-zero, hence injective as a map between fields. □

COROLLARY 5.30: Let $\mathfrak{p}$, $\mathfrak{q}$ as above, then $N(\mathfrak{q}) = N(\mathfrak{p})^f$

THEOREM 5.31: Let $\mathfrak{p}$ as above, then

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

with $e_i = e(\mathfrak{q}_i/\mathfrak{p})$ and

$$[L : K] = \sum e(\mathfrak{q}_i/\mathfrak{p}) f(\mathfrak{q}/\mathfrak{p}) =: \sum e_i f_i$$

PROOF. This actually holds in more generality, but here we're going to use the finiteness of the class group to get a short proof.

Clearly we have

$$N(\mathfrak{p}\mathbb{Z}_L) = N(\prod \mathfrak{q}_i^{e_i}) = \prod N(\mathfrak{q}_i)^{e_i} = N(\mathfrak{p})^{\sum f_i e_i}$$

. Since h_K is finite, we also have $\mathfrak{p}^{h_K} = \lambda\mathbb{Z}_K$ for some $\lambda \in K$, hence

$$N(\mathfrak{p}^{h_K}) = |N_{L/K}(\lambda)| = N(\mathfrak{p})^{h_K}$$

and

$$N((\mathfrak{p}\mathbb{Z}_L)^{h_K}) = |N_{L/K}(\lambda)| = N_{K/\mathbb{Q}})(\lambda)^{nh_K} = N(\mathfrak{p})^{nh_K} = N(\mathfrak{p})^{h_K \sum e_i f_i}$$

and we're done. □

DEFINITION 5.32: Let $\mathfrak{p}\mathbb{Z}_L = \prod_{i=1}^g \mathfrak{q}_i^{e_i}$. Then

(1) $\mathfrak{p}$ is called *inert* iff $g = 1$
(2) $\mathfrak{p}$ is called *totally split* iff $g = n$
(3) $\mathfrak{p}$ is called *split* iff $g > 1$
(4) $\mathfrak{p}$ is called *ramified* iff some $e_i > 1$
(5) $\mathfrak{p}$ is called *totally ramified* iff $e_1 = n$
(6) $\mathfrak{p}$ is called *unramified* iff all $e_i = 1$
(7) $\mathfrak{q}_i$ is called unramified iff $e_i = 1$, ramified otherwise

LEMMA 5.33: Let $\sigma \in \mathrm{Aut}(L, K)$ be a K-automorphism of L and $\mathfrak{q}$ be a prime ideal in $\mathbb{Z}_L$ lying above $\mathfrak{p}$. Then

(1) $\sigma\mathfrak{q}$ is a prime ideal above $\mathfrak{p}$ as well
(2) $f(\sigma\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p})$
(3) $e(\sigma\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p})$

PROOF. Since $\mathfrak{p} \subseteq K$ we have $\mathfrak{p} = \sigma\mathfrak{p}$, thus (1) follows. For (2) we notice that σ induces a field-isomorphism from

$$\mathbb{F}_{\mathfrak{q}} \to \mathbb{F}_{\sigma\mathfrak{q}} : x \mapsto \sigma x$$

From $\mathfrak{p}\mathbb{Z}_L = \prod \mathfrak{q}_i^{e_i} = \sigma\mathfrak{p}\mathbb{Z}_L = \prod \sigma(\mathfrak{q}_i)^{e_i}$ we get (3). □

LEMMA 5.34: Let L/K be Galois, then the Galois group acts transitively on the prime ideals over the same prime, i. e. let p be a prime ideal in $\mathbb{Z}_K$ and $P_1, \ldots, P_g$ the primes above p. Then for any i, j we have a $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(P_i) = P_j$

PROOF. It is clear that Gal is acting on $\mathbb{Z}_L$ transporting prime ideals onto prime ideals. Now assume the statement of the lemma is wrong, then we can find $i \neq j$ such that

$$\underbrace{\{\sigma(P_i) \mid \sigma \in \mathrm{Gal}(L/K)\}}_{=:A} \cap \underbrace{\{\sigma(P_j) \mid \sigma\}}_{=:B} = \emptyset$$

The the CRT allows us to find $x \in \mathbb{Z}_L$ such that $x \equiv 1 \bmod P_a$, $P_a \in A$ and $x \equiv 0 \bmod P_b$ for $P_b \in B$. But this implies $\sigma(x) \equiv 1 \bmod P_i$ for all σ, hence $N(x) \equiv 1 \bmod \cap_\sigma P_i \cap Z_K = p$ and $N(x) \equiv 0 \bmod \cap\sigma P_j \cap Z_K = p$ as well. □

DEFINITION 5.35: Let $\mathcal{O}_1 \subseteq \mathcal{O}_2$ be orders, then

$$\mathcal{F} := \{x \in \mathcal{O}_2 \mid x\mathcal{O}_2 \subseteq \mathcal{O}_1\}$$

is called the *conductor* of $\mathcal{O}_1$ in $\mathcal{O}_2$. For $\mathcal{O}_2 = \mathbb{Z}_L$ we call $\mathcal{F}$ simply the conductor of $\mathcal{O}_1$.

LEMMA 5.36: Let $\mathcal{O}_1 \subseteq \mathcal{O}_2$ be orders, and $\mathcal{F}$ the conductor, then $\mathcal{F}$ is an ideal in both $\mathcal{O}_1$ and $\mathcal{O}_2$. Furthermore, among all those ideal, $\mathcal{F}$ is maximal.

PROOF. We note $\mathcal{O}_1 \subseteq \mathcal{O}_2$ and $1 \in \mathcal{O}_2$ as this give $\mathcal{F} \subseteq \mathcal{O}_1$. For the maximality we note for any ideal $A \subseteq \mathcal{O}_1$ that is an ideal in $\mathcal{O}_2$ as well we have

$$A\mathcal{O}_2 \subseteq A \subseteq \mathcal{O}_1$$

so $A \subseteq \mathcal{F}$. □

LEMMA 5.37: Let $\mathcal{F}$ be the conductor of $\mathcal{O}$ in $\mathbb{Z}_L$ and define

$$D_L := \{A \leq \mathbb{Z}_L \mid 0 \neq A, A + \mathcal{F} = \mathbb{Z}_L\}$$
$$D_{\mathcal{O}} := \{A \leq \mathcal{O} \mid 0 \neq A, A + \mathcal{F} = \mathcal{O}\}$$

then

(1) D_L and $D_{\mathcal{O}}$ are multiplicative monoids.
(2) For all $A \in D_L$ we have $\mathbb{Z}_L/A \sim \mathcal{O}/A$
(3) Every $A \in D_{\mathcal{O}}$ has a unique factorisation into prime ideals in $D_{\mathcal{O}}$
(4) D_L and $D_{\mathcal{O}}$ have cancellation.

PROOF. (1): Let A, $B \in D_{\mathcal{O}}$, then

$$\mathcal{O} = \mathcal{O}\mathcal{O} = (A + \mathcal{F})(B + \mathcal{F}) = AB + \mathcal{F}(A + B + \mathcal{F}) = AB + \mathcal{F}$$

(2) Define $\varphi : D_{\mathcal{O}} \to D_L : A \mapsto A\mathbb{Z}_L$, then φ is welldefined:

$$\mathbb{Z}_L = \mathcal{O}\mathbb{Z}_L = (A + \mathcal{F})\mathbb{Z}_L = A\mathbb{Z}_L + \mathcal{F}\mathbb{Z}_L = \varphi(A) + \mathbb{Z}_L$$

so $\varphi(A) \in D_L$. Clearly, φ is multiplicative.

Next, we show that φ is injective: Let A, $B \in D_{\mathcal{O}}$ with $\varphi(A) = \varphi(B)$. Since $\varphi(A) \in D_L$, we have $A\mathbb{Z}_L + \mathcal{F} = \mathbb{Z}_L$, so $A\mathbb{Z}_L \cap \mathcal{F} = A\mathbb{Z}_L\mathcal{F}$. Now

$$\begin{aligned} A &\subseteq \varphi(A) \cap \mathcal{O} = A\mathbb{Z}_L \cap (A + \mathcal{F}) = A + (A\mathbb{Z}_L \cap \mathcal{F}) \\ &= A + A\mathcal{F}\mathbb{Z}_L = A + A\mathcal{F} = A + A = A \end{aligned}$$

And the same for B. Now we can conclude

$$A = \varphi(A) \cap \mathcal{O} = \varphi(B) \cap \mathcal{O} = B$$

Finally surjectivity: Let $A \in D_L$ be arbitrary, then

$$(A \cap \mathcal{O}) + \mathcal{F} = (A \cap \mathcal{O}) + (\mathcal{F} \cap \mathcal{O}) = (A + \mathcal{F}) \cap \mathcal{O} = \mathbb{Z}_L \cap \mathcal{O} = \mathcal{O}$$

showing $A \cap \mathcal{O} \in D_{\mathcal{O}}$. Since A and $\mathcal{F}$ as well as $A \cap \mathcal{O}$ and $\mathcal{F}$ are comaximal, we have

$$A\mathcal{F} = A \cap \mathcal{F} = (A \cap \mathcal{O}) \cap \mathcal{F} = (A \cap \mathcal{O})\mathcal{F}$$

and thus

$$\begin{aligned} A &= A\mathcal{O} = A(A \cap calO + \mathcal{F}) = A(A \cap \mathcal{O}) + A\mathcal{F} \\ &= A(A \cap \mathcal{O}) + \mathcal{F}(A \cap \mathcal{O}) = (A \cap \mathcal{O})(A + \mathcal{F}) \\ &= (A \cap \mathcal{O})\mathbb{Z}_L = \varphi(A \cap \mathcal{O}) \end{aligned}$$

And φ is surjective as required.

(3) Define $\psi : \mathcal{O} \to \mathbb{Z}_L/A : x \mapsto x + A$, then $\ker \psi = \mathcal{O} \cap A$. Let $x \in \mathbb{Z}_L$ be aritrary. Since $A + \mathcal{F} = \mathbb{Z}_L$, we can find $y \in A$ and $z \in \mathbb{Z}_L$ such that $x = y + z$, thus $\psi(z) = z + A = z + y + A = x + A$, hence ψ is surjective. Since in orders, residue rings are finite, ψ is also injective.

(4) Let $A \in D_{\mathcal{O}}$ be arbitrary, then $\varphi(A) \in D_L$ has a unique factorisation into prime ideals:

$$\varphi(A) = A\mathbb{Z}_L = \prod P_i^{n_i}$$

Since $\varphi(A) \subseteq P_i$ we also have $P_i \in D_L$, so

$$A = \prod \varphi^{-1}(P_i)^{n_i}$$

Since φ is an isomorphism, the uniquness follows from $\mathbb{Z}_L$.

□

THEOREM 5.38 (Dedekind): Let $\varphi \in L$, $L = K[\varphi]$, $f \in \mathbb{Z}_K[t]$ the minimal polynomial of φ and $\mathcal{F}$ the conductor of $\mathcal{O} := \mathbb{Z}_K[\varphi]$ in $\mathbb{Z}_L$.

Now let P be a prime ideal in $\mathbb{Z}_K$ such that $P\mathbb{Z}_L + \mathcal{F} = \mathbb{Z}_L$ and $\bar{(.)} : \mathbb{Z}_K \to \mathbb{Z}_K/P = \mathbb{F}_P$ the canonical projection and the extension to the polynomial ring.

Assume $\bar{f} = \prod \bar{f}_i^{e_i}$, then

$$P\mathbb{Z}_L = \prod Q_i^{e_i}$$

for prime ideals $Q_i = \langle P, f_i(\varphi) \rangle$ and $f(Q_i/P) = \deg f_i$.

LEMMA 5.39: In the situation of 5.38 we define

$$\Phi : \mathbb{Z}_K[\varphi] \to \mathbb{F}_P[t]/\bar{f} : \varphi \mapsto t$$

then

$$\ker \Phi = P[\varphi]$$

and

$$\mathbb{Z}_K[\varphi]/P[\varphi] = \mathbb{F}_P[t]/\bar{f}$$

PROOF. Let $h[t] \in \ker \Phi$, then clearly $\bar{h} = \bar{q}\bar{f}$ for some $\bar{q} \in \mathbb{F}_P[t]$. Fixing (as usual) a monic lift, we write

$$h = qf + p$$

for $p[t] \in P[t]$, but then $h(\varphi) = \Phi(h) = p$, so $\ker \Phi \subseteq P[t]$. Since the reverse is obvious, this shows the claims. □

PROOF OF 5.38. By 5.39 we need to study the prime ideals in $\mathbb{F}_P[t]/\bar{f}$, but those are easy: primes in the quotient come from the $\bar{f}_i$, so $\langle P[\varphi], f_i(\varphi)\rangle$ are prime ideals in $\mathbb{Z}_K[\varphi]/P[\varphi]$. Define Q_i as in the theorem

$$Q_i := \langle p, f_i(\varphi)\rangle = f_i(\varphi)\mathbb{Z}_L + P\mathbb{Z}_L$$

By construction we also have $Q_i \in D_L$ since $P \subseteq Q_I$ and $\mathbb{Z}_L = P\mathbb{Z}_L + \mathcal{F} \subseteq Q_I + \mathcal{F} \subseteq \mathbb{Z}_L$. By 5.37 the prime ideals in D_L and $D_{\mathcal{O}}$ are in one-to-one correspondence. It remains to show the statements about the inertia and the ramification.

$$\begin{aligned} N(P)^{f(Q_i/P)} &= |\mathbb{Z}_K/P|^f = |\mathbb{Z}_L/Q_i| = N(Q_i) \\ &= |\mathcal{O}/(Q_i \cap \mathcal{O})| = |(\mathcal{O}/P[\varphi])/((Q_iO)/P[\varphi])| \\ &= |(\mathbb{F}_P[t]/\bar{f})/(\bar{f}_i\mathbb{F}_P[t]/\bar{f})| \\ &= |\mathbb{F}_P[t]/\bar{f}_i| = N(P)^{\deg f_i} \end{aligned}$$

For the ramification we start by showing $e_i \geq e(Q_i/P)$. We have

$$\begin{aligned} \prod_{i=1}^{r} Q_i^{e_i} &= \prod (p\mathbb{Z}_L + f_i(\varphi)\mathbb{Z}_L)^{e_i} \subseteq p\mathbb{Z}_L + \prod f_i^{e_i}(\varphi)\mathbb{Z}_L \\ &\subseteq p\mathbb{Z}_L + p\mathbb{Z}_K[\varphi]\mathbb{Z}_L \subseteq p\mathbb{Z}_L = \prod Q_i^{e(Q_i,P)} \end{aligned}$$

On the other hand, simply counting:

$$n = \sum e(Q_i/P)f(Q_i/P) \geq \sum e_i \deg f_i = \deg f = n$$

hence equality everywhere and $e_i = e(Q_i/P)$ □

COROLLARY 5.40: Let $L = K[\varphi]$, $\mathcal{O} := \mathbb{Z}_K[\varphi]$, $\mathcal{F}$ the conductor of $\mathcal{O}$ and $P \leq \mathbb{Z}_K$ a prime. Then if either

$$(\mathbb{Z}_L : \mathcal{O}) \not\subseteq P$$

or

$$d_f \notin P$$

where $f \in \mathbb{Z}_K[t]$ is the monic minimal polynomial of φ, then

$$P\mathbb{Z}_L + \mathcal{F} = \mathbb{Z}_L$$

PROOF. Since $d_f \in (\mathbb{Z}_L : \mathcal{O})$, (or $(\mathbb{Z}_L : \mathcal{O})|d_f$), the second implies the first, so it remains to show the first.

Let $\alpha \in \mathcal{F} \cap K$ such that $P + \alpha\mathbb{Z}_K = \mathbb{Z}_K$, then $P\mathbb{Z}_L + \mathcal{F} = \mathbb{Z}_L$ since

$$\mathbb{Z}_L = \mathbb{Z}_K\mathbb{Z}_L = (P + \alpha\mathbb{Z}_L)\mathbb{Z}_K = P\mathbb{Z}_K + \alpha\mathbb{Z}_L \subseteq P\mathbb{Z}_L + \mathcal{F} = \mathbb{Z}_L$$

implying equality everywhere. So we have $(\mathbb{Z}_L : \mathbb{Z}_K[\varphi]) \subseteq \mathcal{F}$, basically by definition showing the statement. □

COROLLARY 5.41: Let $L = K[\varphi]$ for $\varphi \in \mathbb{Z}_L$, $f \in \mathbb{Z}_K[t]$ the minimal polynomial and $P \subseteq \mathbb{Z}_K$ a prime such that $d_f \notin P$. Then P is unramified.

PROOF. $d_f \notin P$ implies that 5.38 can be used. P unramified is now equivalent to $\bar{f}$ being squarefree, but this is guaranteed by $d_f \notin P$ or $d_{\bar{f}} \neq 0$. □

We now want to do two things:

- Study the reverse, i. e. show that ramified primes are exactly those dividing d_L (for $K = \mathbb{Q}$ at least) and
- show that 5.38 does not always apply.

We start with an explicit example (slightly cheated)

EXAMPLE 5.42: Let $f := t^3 + t^2 - 2t + 8$. This is irreducible modulo 3, so it is irreducible. Running all our algorithms, we get

$$\mathbb{Z}_L = \mathbb{Z} + \mathbb{Z}\varphi + \mathbb{Z}\frac{1}{2}(\varphi^2 + \varphi)$$

so $\mathbb{Z}[\varphi]$ is not maximal. Let $\varphi_i : \mathbb{Z}_L \to \mathbb{F}_2$ be defined via

$$\varphi_1((\omega_i)_i) = (1, 0, 0)$$

$$\varphi_2((\omega_i)_i) = (1, 0, 1)$$

$$\varphi_3((\omega_i)_i) = (1, 1, 1)$$

It's a bit painful (by hand), but we can easily check that those three maps are ring homomorphisms. Since they are trivially surjective, we have three distinct prime ideals as their kernels. Hence

$$2\mathbb{Z}_L = P_1P_2P_3$$

Suppose, we had some $\alpha \in \mathbb{Z}_L$ such that $\mathbb{Z}[\alpha]$ would be 2-maximal. Then we could apply 5.38 to obtain the factorisation of $2\mathbb{Z}_L$ via the factorisation of the minimal polynomial of α. However, there are only 2 distinct linear polynomials over $\mathbb{F}_2$ available, hence the modulo 2 factorisation can never be squaree free.

It follows that for every $\alpha \in \mathbb{Z}_L$ that is primitive, we have $2|(\mathbb{Z}_L : \operatorname{disc}(\alpha))$.

So we need a different method to factorise primes as well.

We would like to study this failure of 5.38 in slightly more generality.

LEMMA 5.43: Let $L/\mathbb{Q}$ a number field, $p \in \mathbb{Z}$ a prime number and $\theta \in \mathbb{Z}_L$. Then

(1) $p \not| (\mathbb{Z}_L : \mathbb{Z}[\theta])$ iff for all $\varphi \in \mathbb{Z}[t]$ we have

$$\varphi(\theta) \in p\mathbb{Z}_L \iff \varphi \in p\mathbb{Z}[t]$$

(2) Let $\alpha \in \mathbb{Z}_L$ be such that $\alpha - \theta \in p\mathbb{Z}_L$, then

$$p|(\mathbb{Z}_L : \mathbb{Z}[\alpha]) \iff p|(\mathbb{Z}_L : \mathbb{Z}[\theta])$$

PROOF. (1) If $\varphi \in p\mathbb{Z}[t]$, then clearly $\varphi(\theta) \in p\mathbb{Z}_L$ as well. If $p|(\mathbb{Z}_L : \mathbb{Z}[\theta])$, then we can find $\alpha \in \mathbb{Z}_L \setminus \mathbb{Z}[\theta]$ such that $p\alpha \in \mathbb{Z}[\theta]$. Clearly, $p\alpha = \varphi(\theta)$ for some suitable $\varphi \in \mathbb{Z}[t]$ and $\varphi \notin p\mathbb{Z}[t]$ since $\alpha \notin \mathbb{Z}[\theta]$.

If $p \not| (\mathbb{Z}_L : \mathbb{Z}[\theta])$ and $\varphi(\theta) \in p\mathbb{Z}_L$. Then $\varphi(\theta) = \sum pt_i\omega_i$ for some basis of $\mathbb{Z}_L$ equivalently, $\varphi(\theta) \equiv 0 \bmod p\mathbb{Z}_L$. Since the base change from $(\omega_i)_i$ to $(\theta^{i-1})_i$ involves a transformation matrix $T \in \mathbb{Z}^{n\times n}$ that is invertable modulo p, the statement follows.

(2) From $\alpha - \theta \in p\mathbb{Z}_L$ we immediately get $\varphi(\alpha) - \varphi(\theta) \in p\mathbb{Z}_L$ as well, hence the statement follows from (1). □

LEMMA 5.44: Let p be a prime number, $P \subseteq \mathbb{Z}_L$ a prime ideal above p. Then $\mathbb{F}_P$ is a finite field. Let $\bar{\alpha} \in \mathbb{F}_P$ be a primitive element for $\mathbb{F}_P$ over $\mathbb{F}_p$, $\bar{g} \in \mathbb{F}_p[t]$ the minimal polynomial of $\bar{\alpha}$ and $g \in \mathbb{Z}[t]$ a monic lift. If $P^2|p\mathbb{Z}_L$, then we can find $\beta \in \mathbb{Z}_L$ such that $g(\beta) \in P \setminus P^2$

PROOF. Let $\alpha \in \mathbb{Z}_L$ be a any lift of α. If $g(\alpha) \notin P^2$ we're done. Otherwise fix any $\pi \in P \setminus P^2$ and show that $g(\alpha + \pi)$ works: Taylor's theorem:

$$g(\alpha + \pi) = g(\alpha) + \pi g'(\alpha) + \pi^2 \dots$$

Since $\bar{g}$ is irredicible, $\bar{\alpha}$ is only a single root of $\bar{g}$, hence $\bar{g}'(\bar{\alpha}) \neq 0$, so $\pi g'(\alpha) \in P \setminus P^2$, $g(\alpha)$ and the other terms are in P^2. □

LEMMA 5.45: Let β, P and g as in 5.44. Then for $1 \leq i \leq e(P/p)$ we have for $\varphi \in \mathbb{Z}[t]$, $\deg \varphi < n$:

$$\varphi(\beta) \in P^i \iff (\bar{g})^i | \bar{\varphi}$$

PROOF. $\varphi(\beta) \in P$ is equivalent to $\bar{\varphi}(\bar{\beta}) = 0$, hence $\bar{g}|\bar{\varphi}$. Let now $\bar{\varphi} = (\bar{g})^k \bar{h}$ for some $\bar{h} \in \mathbb{F}_p[t]$ coprime to $\bar{g}$. But then the same argument shows that $h(\beta) \notin P$, hence $\varphi(\beta) \in P^k \setminus P^{k+1}$ giving $k \geq i$ as claimed. □

THEOREM 5.46 (Dedekind): Let $p \in \mathbb{Z}$ be a prime number and $L/\mathbb{Q}$ a number field. Assume that

$$p\mathbb{Z}_L = \prod P_i^{e_i}$$

and there exists pairwise coprime irreducible polynomials $f_i \in \mathbb{F}_p[t]$ of degree $\deg f_i = f(Q_i/p)$. Then we can find $\alpha \in \mathbb{Z}_L$ such that

$$p \not| (\mathbb{Z}_L : \mathbb{Z}[\alpha])$$

So this is a reverse of the example, classifying completely when 5.38 might be applicable.

PROOF. Since f_i is irreducible of degree $f(Q_i/p)$, f_i has a root in $\mathbb{F}_{Q_i}$ which is primitive over $\mathbb{F}_p$. By 5.44 we can find β_i such that $f_i(\beta_i) \in Q_i \setminus Q_i^2$. Using the CRT we find $\beta \equiv \beta_i \bmod Q_i^2$.

Suppose $\varphi(\beta) \equiv 0 \bmod p$, then $\varphi(\beta) \equiv 0 \bmod Q_i^{e_i}$ by the CRT, so 5.45 implies $\bar{\varphi} \equiv 0 \bmod f_i^{e_i}$, so CRT again, $\bar{\varphi} \equiv 0 \bmod \prod f_i^{e_i}$. For degree reasons then $\bar{\varphi} = 0$ and hence $\varphi \equiv 0 \bmod p$. By 5.43, $p \not| (\mathbb{Z}_L : \mathbb{Z}[\beta])$. □

LEMMA 5.47: Let p be a prime ideal in $\mathbb{Z}_K$ and $p\mathbb{Z}_L = \prod_{i=1}^r Q_i^{e_i}$. Choose $\beta_{i,j} \in \mathbb{Z}_L$, $1 \le j \le f_i = f(Q_i|p)$ such that $(\bar{\beta}_{i,j})_j$ form a $\mathbb{F}_p$-basis for $\mathbb{F}_{Q_i} = \mathbb{Z}_L/Q_i$ and

$$\alpha_{i,j} \in (Q_i^{j-1} \setminus Q_i^j) \cap \bigcap_{k \neq i} Q_k^{e_k}$$

for $1 \le j \le e_i$, $1 \le i \le r$. Then the n-elements $\alpha_{i,j}\beta_{i,k}$ $1 \le i \le r$, $1 \le j \le e_i$ and $1 \le k \le f_i$ form a $\mathbb{F}_p$-basis for $\mathbb{Z}_L/p\mathbb{Z}_L$.

PROOF. Since $N(p\mathbb{Z}_L) = N(p)^n$, hence $\mathbb{Z}_L/p\mathbb{Z}_L$ is an $\mathbb{F}_p$-vectorspace of dimension n, it is sufficient to show that the elements are $\mathbb{F}_p$-linear independent. Assume now that we have $\gamma_{i,j,k} \in \mathbb{Z}_K$ such that

$$\sum_{i=1}^{r}\sum_{j=1}^{e_i}\sum_{k=1}^{f_i} \gamma_{i,j,k}\alpha_{i,j}\beta_{i,k} \in p\mathbb{Z}_L = \prod Q_i^{e_i}$$

Since $\alpha_{i,j} \in Q_l^{e_l}$ for all $l \neq i$, we see that

$$\sum_{j=1}^{e_i}\sum_{k=1}^{f_i} \gamma_{i,j,k}\alpha i, j\beta_{i,k} \in Q_i^{e_i}$$

thus

$$\sum_{j=1}^{l}(\alpha_{i,l}\sum_{k=1}^{f_i} \gamma_{i,j,k}\beta_{i,k}) \in Q_i^l$$

as well. (The full sum has to be in $Q_i^{e_i}$, but by construction, the $\alpha_{i,l} \notin Q_i^l$). We now fix some $1 \le i \le r$ and show by induction over l that $\gamma_{i,l,k} \in p$. From the last line and since $\alpha_{i,1} \notin Q_i$, we see that

$$\sum_{k=1}^{f_i} \gamma_{i,1,k}\beta_{i,k} \in Q_i$$

thus $\gamma_{i,1,k} \in p$ since β_i form a $\mathbb{F}_p$-basis for $\mathbb{F}_{Q_i}$. This starts the induction. Now let $l > 1$ then

$$\underbrace{\sum_{j=1}^{l-1}\sum_{k=1}^{f_i} \gamma_{i,j,k}\alpha_{i,j}\beta_{i,k}}_{\in p\mathbb{Z}_L \subseteq Q_i^l} + \alpha_{i,l}\sum_{k=1}^{f_i} \gamma_{i,l,k}\beta_{i,k} \in Q_i^l$$

The choice of $\alpha_{i,l}$ now implies

$$\sum_{k=1}^{f_i} \gamma_{i,j,k}\beta_{i,k} \in Q_i$$

hence, as above $\gamma_{i,l,k} \in p$. □

REMARK 5.48: Let $K = \mathbb{Q}$, $p \in \mathbb{Z}$ a prime number and $\alpha_i \in \mathbb{Z}_L$ a $\mathbb{F}_p$-basis for $\mathbb{Z}_L/p\mathbb{Z}_L$. Then clearly the α_i are $\mathbb{Q}$-linear independent.

LEMMA 5.49: Let K, p, α_i as above and $R := \sum \mathbb{Z}\alpha_i$. Then $p \not| (\mathbb{Z}_L : R)$.
Note: R will, in general, not be an order!

PROOF. Assume $p|(\mathbb{Z}_L : R)$, then we can find $\beta \in \mathbb{Z}_L \setminus R$ and $p\beta \in R$, hence

$$p\beta = \sum m_i \alpha_i$$

for $m_i \in \mathbb{Z}$. Since $\beta \notin R$, we find i such that $m_i \not\equiv 0 \bmod p$, thus

$$p\beta = \sum m_i \alpha_i \equiv 0 \bmod p\mathbb{Z}_L$$

is a non-trivial rep. of 0. □

LEMMA 5.50: Let $K = \mathbb{Q}$, $P = p\mathbb{Z}$ for a prime number and $(\gamma_i)_i = (\alpha_{i,j}\beta_{i,k})_{i,j,k}$ the elements form 5.47. For

$$\nu := \sum_{i=1}^{r} (e_i - 1) f_i = n - \sum f_i$$

we have $p^\nu | \operatorname{disc}((\gamma_i)_i)$

PROOF. Wlog: $\nu > 0$ (since for $\nu = 0$ the statement is trivial.) Let now $\mathbb{Z}_L \ni \gamma = \alpha_{i,j}\beta_{i,k}$ for $j > 1$, then $\gamma \in \bigcap Q_i$. For M the normal closure of L/K and $R \leq \mathbb{Z}_M$ a prime ideal containing p, we have $p\mathbb{Z}_M = \prod Q_i^{e_i} \mathbb{Z}_M$, hence we can find $1 \leq l \leq r$ such that $Q_l \subseteq R$, thus $\gamma \in R$. For φ a $\mathbb{Q}$-automorphism of M, $\varphi(R)$ is also a prime ideal in $\mathbb{Z}_M$ containing p, hence we can find $\tilde{l}$ such that $Q_{\tilde{l}} \subseteq \varphi(R)$, so $\gamma \in Q_{\tilde{l}} \subseteq \varphi(R)$, hence $\varphi^{-1}(\gamma) \in R$ for all such φ. As before, this shows that $\operatorname{Tr}(\gamma\alpha) \in R \cap \mathbb{Z}$ for all $\alpha \in \mathbb{Z}_L$. From $\#\{\alpha_{i,j}\beta_{i,k} | j \geq 2\} = \nu$ we get the claim, since the trace-matrix $(\operatorname{Tr}(\gamma_i\gamma_j))_{i,j}$ will have at least ν rows with all entries divisible by p. □

COROLLARY 5.51: Under the assumptions of 5.50 we get $p^\nu | \operatorname{disc} \mathbb{Z}_L$ or, in other words: every ramified prime divides the discriminant.

PROOF. Let γ_i be as above and set $R = \sum \mathbb{Z}\gamma_i$. Then by 5.48 R is a $\mathbb{Z}$-module of full rank and $p \not| (\mathbb{Z}_L : R)$. By 5.50 we get $p^\nu | \operatorname{disc}(R)$ thus $p^\nu | \operatorname{disc} \mathbb{Z}_L$ as well. □

LEMMA 5.52: Let $K = \mathbb{Q}$, $p \in \mathbb{Z}$ an unramified prime, then $p \not| \operatorname{disc} \mathbb{Z}_L$.

PROOF. Let $p\mathbb{Z}_L = \prod_{i=1}^{r} Q_i^{e_i}$ and $\alpha_{i,j}$, $\beta_{i,k}$ as in 5.47. Then, by construction $\gamma := \alpha_{i,j}\alpha_{\tilde{i},\tilde{j}} \in p\mathbb{Z}_L$ for all $i \neq \tilde{i}$, hence $\operatorname{Tr}(\gamma\alpha) \equiv 0 \bmod p$ for all $\alpha \in \mathbb{Z}_L$. This shows that the trace matrix modulo p is of the form $\operatorname{diag}(((\operatorname{Tr}(\alpha_{i,j}\beta_{i,k}\alpha_{i,\tilde{j}}\beta_{i,\tilde{k}})_{j,k,\tilde{j},\tilde{k}})_i))$ under suitable ordering of the basis elements. We also remark that $j = 1$ here as p is unramified. This shows $\operatorname{disc} R \equiv \prod \det(\operatorname{Tr}(\alpha_{i,1}\beta_{i,k}\alpha_{i,1}\beta_{i,\tilde{k}})_{k,\tilde{k}}) \bmod p$. It remains to be shows, that the smaller determinants are non-zero. Fix a normal closure M of L and the embeddings $\varphi_\mu : L \to M$ $1 \leq \mu \leq n$. Now we fix some i and choose R a prime ideal in $\mathbb{Z}_M$ above Q_i, then $\mathbb{F}_{Q_i} \subseteq \mathbb{F}_R$. Let $\pi : \mathbb{Z}_M \to \mathbb{F}_R$. Let

$$A_i := \operatorname{diag}(\varphi_1(\alpha_{i,1}), \ldots, \varphi_n(\alpha_{i,1})) \begin{pmatrix} \varphi_1(\beta_{i,1}) & \ldots & \varphi_1(\beta_{i,f_i}) \\ \vdots & & \vdots \\ \varphi_n(\beta_{i,1}) & \ldots & \varphi_n(\beta_{i,f_i}) \end{pmatrix}$$

Then $A_i^t A_i = (\operatorname{Tr}(\alpha_{i,1}\beta_{i,k}\alpha_{i,1}\beta_{i,\tilde{k}})_{k,\tilde{k}})$ and it remains to show that $\operatorname{rg}_{\mathbb{F}_p} \pi(A_i) = f_i$ since then the determinant is non-zero in $\mathbb{F}_{Q_i}$. Since the determinant is automatically in $\mathbb{F}_p$ it will imply that the determinants are not divisible by p. Now we note that

the $\beta_{i,1}, \ldots, \beta_{i,f_i}$ for a $\mathbb{F}_p$-basis for $\mathbb{F}_{Q_i}$ hence are $\mathbb{F}_p$-linear independent. Applying the Vandermonde determinant to a defining polynomial for $\mathbb{F}_{Q_i}$ we see that the Vandermonde matrix has full rank f_i, hence A_i has f_i independent rows. Scaling with the diagonal matrix does not change this as all entries there are invertible since $\alpha_{i,1} \notin Q_i$. Lastly, $\operatorname{rg} A^t A = \operatorname{rg} A$ in general. $\square$

CHAPTER 6

Computing the Class Group

1. The Beginning

Now it s about time to compute class groups. This time, we actually start with an algorithm and then worry about the details.

ALGORITHM 6.1:

Input: A number field L
Output: The class group Cl_L
1: Find a finite set $B \subset I_L$ such that $\langle B + P_L \rangle = \mathrm{Cl}_L$
2: Find enough elements $\alpha_i \in L^*$ such that $\alpha_i \mathbb{Z}_L \in \langle B \rangle$
3: $\mathrm{Cl}_L = \langle B \rangle / \langle \alpha_i \mathbb{Z}_L | i \rangle$

The correctness comes directly out of the map

$$\langle B \rangle \to \mathrm{Cl} : A \mapsto A + P_L$$

By definition, the kernel of the map consists exactly of those elements α_i found in step 2.

However, the algorithm needs some improvement. The only obvious step so far is (1): Defining B from the Minkowski bound will result in such a finite set and we know how to find (most) prime ideals. The rest needs some work, although this is already sufficient to find some class groups:

EXAMPLE 6.2: Let $L = \mathbb{Q}(i\sqrt{5}) = \mathbb{Q}[t]/t^2 + 5$. Then $\mathbb{Z}_L = \mathbb{Z}[t]/t^2 + 5$. The Minkowski constant is computed as $\sqrt{-D}(4/\pi)2!/4 = 2.85$ from $D = -20$, thus the class group is generated by ideals of norm ≤ 2. Splitting $2\mathbb{Z}_L$ using Dedekind, gives $t^2+5 \equiv t^2+1 = (t+1)^2 \bmod 2$, hence $2\mathbb{Z}_L = \langle 2, 1+i\sqrt{5} \rangle^2$, so B has only 2 elements.

Now we need to see if $P_2 := \langle 2, 1 + i\sqrt{5} \rangle$ is principal. If $P_2 = \langle \alpha \rangle$, then clearly $|N(\alpha)| = N(P_2) = 2$.

$$N(x + iy\sqrt{5}) = x^2 + 5y^2 = 2$$

has no solution, hence P_2 is non-principal, so $\mathrm{Cl}_L = \mathbb{Z}/2\mathbb{Z}$

EXAMPLE 6.3: Let $L = \mathbb{Q}(i\sqrt{14}) = \mathbb{Q}[t]/t^2 + 14$. Then $\mathbb{Z}_L = \mathbb{Z}[t]/t^2 + 14$. The Minkowski constant is computed as $\sqrt{-D}(4/\pi)2!/4 = 4.76$ from $D = -56$, thus the class group is generated by ideals of norm ≤ 4. Splitting $2\mathbb{Z}_L$ using Dedekind, gives $t^2 + 14 \equiv t^2 = t^2 \bmod 2$, hence $2\mathbb{Z}_L = \langle 2, i\sqrt{14} \rangle^2 =: P_2^2$, and $t^2 + 14 \equiv t^2 + 2 = (t + 1)(t + 2) \bmod 3$, $3\mathbb{Z}_L = P_{3,1}P_{3,2} := \langle 3, 1 + i\sqrt{14} \rangle \langle 3, 2 + i\sqrt{14} \rangle$. so B has 4 elements.

Looking for small norm elements:

$$N(x + iy\sqrt{14}) = x^2 + 14y^2$$

we wee that there are no elements of norm 2 or 3, hence P_2, $P_{3,1}$ and $P_{3,2}$ are non-principal. We also know that P_2 has order 2 (since $P_2^2 = \langle 2\rangle$ is clearly principal) and that $P_{3,1}P_{3,2} = \langle 3\rangle$. At this point, we could have $\mathrm{Cl}_L \in \{C_2, C_2 \times C_2, C_4\}$. Thus we need to see if $P_{3,1}^2$ is principal. However, the only elements of norm 9 are ± 3 which have the wrong decomposition (i. e. there is no element α such that $N(\alpha) = 9$ and $\langle\alpha\rangle = P_{3,1}^2$.

Clearly, the "same" idea allows us to compute class groups of all imaginary quadratic fields - albeit with a lot of work.

Example 6.4: Let $L = \mathbb{Q}(\sqrt{10}) = \mathbb{Q}[t]/t^2 - 10$. Then $\mathbb{Z}_L = \mathbb{Z}[t]/t^2 - 10$. The Minkowski constant here turns out to be 3.16, so we need to look at ideals of norm ≤ 3. As above

$$t^2 - 10 \equiv t^2 \bmod 2 \text{ and } t^2 - 10 \equiv t^2 + 2 = (t+1)(t+2) \bmod 3$$

so we have 4 ideals: $\{1\mathbb{Z}_L, P_2, P_{3,1}, P_{3,2}\}$ and need to test them for being principal. $N(x + y\sqrt{10}) = x^2 - 10y^2$ and we cannot simply search for small solutions. We can easily find $N(2 - \sqrt{10}) = -6$, so $\langle 2 - \sqrt{10}\rangle = P_2P_{3,i}$ for $i \in \{1, 2\}$. Applying the automorphism $\sqrt{10} \mapsto -\sqrt{10}$ we see that $P_2 \cong P_{3,i}$ for *both* $i = 1, 2$, so the class group is at most C_2. Now checking modulo 5 we get $x^2 - 10y^2 \equiv x^2 = \pm 2 \bmod 5$ which does not work since $1^2 = 1$, $2^2 = 4$, $3^2 = 4$ and $4^2 = 1 \bmod 5$. So the class group is indeed C_2.

The last example shows that we need a more sophisticated approach. Finding suitable "relations" is fine, but how can we proof non-existence?

In order to simplify the discussion, we introduce more notation:

For $\alpha \in L^*$ and P a prime ideal in $\mathbb{Z}_L$ there is a unique $v_P(\alpha)$ such that $P^{v_P(\alpha)}||\alpha\mathbb{Z}_L$ or, equivalently $\alpha \in P^{v_P(\alpha)} \setminus P^{v_P(\alpha)+1}$. We can extend v_P to all of L^* simply by setting $v_P(\alpha/\beta) = v_P(\alpha) - v_P(\beta)$. The unique ideal factorisation makes this work.

Example 6.5: Let $L = \mathbb{Q}$, thus $\mathbb{Z}_L = \mathbb{Z}$ and fix $p \in \mathbb{Z}$ a prime number. Writing $r/s \in \mathbb{Q}$ as $p^l\tilde{r}/\tilde{s}$ with $p \not| \tilde{r}$, $p \not| \tilde{s}$ we get $v_p(r/s) = l$.

$v_2(3/2) = -1$, $v_2(12/191) = 2$.

Lemma 6.6: Let P and v_P as above, then
(1) $\alpha \in \mathbb{Z}_L$, then $v_P(\alpha) \geq 0$
(2) $v_P(\alpha\beta) = v_P(\alpha)v_P(\beta)$
(3) $v_P(\alpha + \beta) \geq \min(v_P(\alpha), v_P(\beta))$, in fact if $v_P(\alpha) \neq v_P(\beta)$, then $v_P(\alpha + \beta) = \min(v_P(\alpha), v_P(\beta))$

Proof. Follows directly from the ideal properties. □

Using the Dedekind property, we also extend the v_P to all non-zero ideals of $\mathbb{Z}_L$. Finally, to simplify some discussions, $v_P(0) := \infty$. The map v_P is called *P-adic valuation.*

DEFINITION 6.7: Let $S \subset I_L$ be a set of prime ideals of $\mathbb{Z}_L$. Then

$$I_S := \langle S \rangle$$

,

$$\mathbb{Z}_{L,S} := \{x \in L^* | v_P(x) \geq 0 \text{ for } P \notin S\}$$

the so called S-integers and

$$U_S := \{\alpha \in L^* | \alpha \mathbb{Z}_L \in \langle S \rangle\}$$

the set of S-units.

From the lemma it is clear that $\mathbb{Z}_{L,S}$ is a ring and that $U_S = \mathbb{Z}_{L,S}^*$. In particular $S = \{\}$ gives $\mathbb{Z}_{L,\{\}} = \mathbb{Z}_L$.

EXAMPLE 6.8: In $\mathbb{Z}$ and $S := \mathbb{P} \backslash \{p\}$ we have $\mathbb{Z}_S = \{r/s | p \not| s\} = \mathbb{Z}_{(p)}$ the localisation of $\mathbb{Z}$ at p. Here, $\mathbb{Z}_S^* = \langle p \rangle$.

It can be shown that $\mathbb{Z}_{L,S}$ is again Dedekind, however, we're not using this here. ($\mathbb{P}_L = \{P \leq \mathbb{Z}_L | P \text{ is prime ideal}\}$)

LEMMA 6.9: Let $p \in \mathbb{Z}$ be a prime, $p\mathbb{Z}_L = \prod Q_i^{e_i}$. Then there exists $\alpha_i \in L^*$ such that

(1) $v_{Q_i}(\alpha_i) = -1$
(2) $v_{Q_j}(\alpha_i) = 0$ for all $i \neq j$
(3) $p\alpha_i \in \mathbb{Z}_L$

We will call α_i an *valuation element* for Q_i.

PROOF. Let $\pi_i \in Q_i \setminus Q_i^2$ and use CRT to find $\beta_i \equiv \pi_j^{e_j} \bmod Q_j^{e_j+1}$ and $\beta_i \equiv \pi_i^{e_i-1} \bmod Q_i^{e_i}$. Then $\alpha_i := \beta_i/p$ has all the required properties. □

We can use the same idea as the proof above to show the following:

COROLLARY 6.10 (Weak Approximation): Let $S \subset \mathbb{P}_L$ be finite and fix $v_s \in \mathbb{Z}$ for all $s \in S$. Then we can find $\alpha \in L^*$ such that $v_s(\alpha) = v_s$ for all $s \in S$ and $v_P(\alpha) \geq 0$ for all $P \in \mathbb{P}_L \setminus S$.

PROOF. We start by extending S: Let $T := \{Q \in \mathbb{P}_L | \exists P \in S : Q \cap \mathbb{Z} = P \cap \mathbb{Z}\}$ and setting $v_s = 0$ for all $s \in T \setminus S$. Next $d := \prod_{p \in \{p | \exists Q \in T : v_Q < 0, p \in Q\}} p^{v_Q}$. Finally, using CRT to find $\beta \in \mathbb{Z}_L$ such that $v_Q(\beta) = v_Q + v_Q(d)$ for all $Q \in T$. Then β/d works. □

We will use the valuation elements to compute valuations:

ALGORITHM 6.11:

Input: $0 \neq \alpha \in \mathbb{Z}_L$, $P \in \mathbb{P}_L$
Output: $v_P(\alpha)$
1: Let β be an valuation element to P.
2: $i := -1$
3: while $\alpha \in \mathbb{Z}_L$ do

4: $\alpha := \alpha\beta$
5: $i := i + 1$
6: return i

The correctness is clear - once we look at the valuations of elements. The algorithm also extends to ideals, either by working with generators or with ideals directly. It is also easy to extend this to fractional elements.

This algorithm is bad if the valuation is large:

(1) We need v_P iterations of the loop
(2) Since, in general, β has positive valuation at various other prime ideals, the norm of α as well as the coefficients, will grow.

EXAMPLE 6.12: Let $L := \mathbb{Q}[\sqrt{10}]$ and $P = P_2 = \langle 2, \sqrt{10}\rangle$. Then $5/\sqrt{10}$ is a valuation element, since $N(5\sqrt{10}) = -5/2$. Computing The valuation of $\alpha = 2^d$ this way results, in the last iteration, in $\alpha = 5^d$ which is much larger than 2^d.

For completeness $t^2 - 10 \equiv t^2 \bmod 5$, hence $5\mathbb{Z}_L = P_5^2 := \langle 5, \sqrt{10}\rangle^2$.

2. More on Ideals

So far we've represented ideals in term of (HNF) $\mathbb{Z}$-bases. Using those we sketched algorithms for addition, multiplication, divison (inversion) and possibly intersection.

We also saw that every ideal in the maximal order can be generated by just 2 elements. Now we want to investigate this further since

- Conceptually, storing only 2 elements is cheaper than storing n
- Some operations are much more efficient on 2 elements
- (Most) prime ideals come naturally with 2 elements

ALGORITHM 6.13:

Input: An integral ideal $A \leq \mathbb{Z}_L$ and $0 \neq \alpha \in A$
Output: Element $\beta \in A$ such that $A = \langle \alpha, \beta\rangle$
1: repeat
2: $\beta := \text{Random}(A)$
3: until $A = \langle \alpha, \beta\rangle$

It is clear that this algorithism is correct, sooner or later it will find a suitable 2nd generator. However, as stated it is actually not an algorithms at all as we cannot find random elements in A - an infinite set. In order to obtain a more realisitc algorithm we change the specifications:

ALGORITHM 6.14 (2-Element Presentation for Ideals):

Input: An integral ideal $A \leq \mathbb{Z}_L$ given via a $\mathbb{Z}$-basis $(\alpha_i)_i$ and $0 \neq a \in A \cap \mathbb{Z}$
Output: Element $\beta \in A$ such that $A = \langle a, \beta\rangle$
1: repeat
2: $\beta := \text{Random}(A/aA)$
3: until $A = \langle a, \beta\rangle$

Here a will usyally be the minimum $a = \min A \cap \mathbb{N}$ (thus $\langle a \rangle = A \cap \mathbb{Z}$) or the norm $a = N(A) = |Z_L/A|$ both of which are readily available if the basis is in HNF. Since A/aA is a finite ring, in fact $A/aA \equiv (\mathbb{Z}/a\mathbb{Z})^n$ via the ideal basis, we can easily pick β uniformly at random.

LEMMA 6.15: Let $\bar{\beta} \in A/aA$ be choosen uniformly at random and β any lift of it in $\mathbb{Z}_L$. Then the probability that $A = \langle a, \beta \rangle$ is at least

$$\prod_{P|a}(1 - \frac{1}{N(P)})$$

PROOF. We have $A = \prod Q^{v_Q(A)}$ and $aA\mathbb{Z}_L = \prod Q^{v_Q(a)+v_Q(A)}$, thus by the CRT,

$$A/aA = \oplus Q^{v_Q(a)}/Q^{v_Q(a)+v_Q(A)} = \oplus \mathbb{Z}_L/Q^{v_Q(a)}.$$

Now

$$\langle a, \beta \rangle = \gcd(a\mathbb{Z}_L, \beta\mathbb{Z}_L)$$

and thus $v_Q(\langle a, \beta \rangle) = \min(v_Q(a), v_Q(\beta))$, hence $A = \langle a, \beta \rangle$ iff the valuations match. Hence

$$\{\beta \in A/aA \mid A = \langle a, \beta \rangle\} \supseteq \{\beta \in A/aA \mid v_Q(\beta) = v_Q(A) \text{ for all } Q|a\}$$

From the CRT we now get

$$|\{\beta \in A/aA \mid v_Q(\beta) = v_Q(A) \text{ for all } Q|a\}| = |\{\beta \in \mathbb{Z}_L/a \mid v_Q(\beta) = 0 \text{ for all } Q|a\}|$$

Since $v_Q(\beta) = 0$ iff $\beta \notin Q$ we can now count $|\mathbb{Z}_L/Q^e| = N(Q)^e$ and $|\{x \in \mathbb{Z}_L/Q^e | x \in Q| = N(Q)^{e-1}$, hence $P(\beta \in \mathbb{Z}_L/Q^e | \beta \in Q) = 1/N(Q)$ and the statement follows. □

REMARK 6.16: Assume 2 is totally split in $\mathbb{Z}_L$ and $a = 2$, then the above probability is sharp. In this case, the algorithm is not going to be very successul $\prod(1 - 1/N(Q)) = 2^{-n}$ in this case.

On the other hand, if a contains no small prime ideals then this shows that the algorithm will find a second generator after very few attempts.

Apart from the situation where the random selection does not work (well), it is rather expensive to test $A = \langle a, \beta \rangle$ as this requires a full HNF computation. This partly motivates a variation of the 2-element presentation.

DEFINITION 6.17: For $a \in \mathbb{N}$, define $P(a) := \{P \in \mathbb{P}_L | a \in P\}$. Similarly for $S \subseteq \mathbb{P}_\mathbb{Z}$, define $P(S) := P_L := \{Q \in \mathbb{P}_L | Q \cap P \neq \emptyset\}$. Let A be a (fractional) ideal for $\mathbb{Z}_L$, then the *support* of A is defined as

$$\text{supp}(A) := \{P \in \mathbb{P}_L \mid v_P(A) \neq 0\}$$

Fix a finite set $S \subseteq \mathbb{P}_\mathbb{Z}$ of prime numbers. A tuple $(a, \alpha) \in \mathbb{N} \times L$ is called a *S-normal presentation* of an ideal A iff

(1) For all $Q \in P(S)$ we have $v_Q(a) \geq v_Q(A)$ and $v_Q(\alpha) = v_Q(A)$
(2) For $Q \notin P(S)$ we have $v_Q(a) = 0$

LEMMA 6.18: Let S be a finite set of primes, A some ideal and (a, α) a S-normal presentation for A. Then

(1) If $\text{supp}(A) \subseteq P(S)$, then $A = \langle a, \alpha \rangle$
(2) If $A = \langle a, \alpha \rangle$ then $N(A) = \gcd(a^n, N(\alpha))$

PROOF. Part (1) is trivial and part (2) is homework □

REMARK 6.19: Let p be a prime number and $p \in Q \in \mathbb{P}_L$. Then a second generator of a $P(p)$-normal presentation for Q^{-1} yields a valuation element.

LEMMA 6.20: Let $A \leq \mathbb{Z}_L$ be integral, $P(N(A)) \subseteq S$, then there exists a S-normal presentation, i. e. we can find a, α such that (a, α) is S-normal for A.

PROOF. Let $0 \neq a \in A \cap \mathbb{N}$, this satisfies all constraints on the 1st generator. The definition of S-normal presentation now imposes a finite number of conditions (valuations) at the primes in $P(S)$, so the approximation theorem 6.10 will find suitable α. □

The problem with this existence proof (as it is with the definition itself) is that we require the prime ideals in P_L explicitly for the tests. In the lemma, we saw that the 1st generator is easy to pick as $\min A \cap \mathbb{N}$ or any multiple. What we need is a way to check the 2nd generator more efficiently.

THEOREM 6.21: Let $0 \neq a \in \mathbb{N}$ and $\alpha \in \mathbb{Z}_L$. Then (a, α) is $P(a)$-normal for $A := \langle a, \alpha \rangle$ iff

$$\gcd(a, \frac{\min(\alpha\mathbb{Z}_L \cap \mathbb{N})}{\gcd(\min(\alpha\mathbb{Z}_L \cap \mathbb{N}), a)}) = 1$$

PROOF. Define $m := \min \alpha\mathbb{Z}_L \cap \mathbb{N}$, then $v_Q(m) \geq v_Q(\alpha)$ for all Q. Now we conclude

$$\gcd(a, \frac{m}{\gcd(m, a))} = 1$$

iff $\min(v_p(a), v_p(m) - \min(v_p(m) - v_p(a))) = 0$ for all $p \in \mathbb{P}_\mathbb{Z}$ hence also for $Q \in \mathbb{P}_L$.

Now suppose the gcd is 1, then either $v_Q(a) = 0$ or $v_Q(m) \leq v_Q(a)$ implying $v_Q(\alpha) \leq v_Q(m) \leq v_Q(a)$, hence we have a normal presentation by definition.

On the other hand, suppose (a, α) is $P(a)$-normal for A. We want to show that $v_p(m) \leq v_p(a)$ for all $p \in P(a)$. For this, we split $m = bd$ such that $v_p(b) = 0$ for $p \notin P(a)$ and $\gcd(b, d) = 1$, so $v_p(d) = 0$ for $p \in P(a)$. Since $v_P(A) = v_P(\alpha)$ for $P \in P(a)$, we see that $ad \in \alpha\mathbb{Z}_L$, hence $ad \in \alpha\mathbb{Z}_L \cap \mathbb{Z}$, thus $m|ad$. Finally, we get $b|a$ showing $v_P(m) = v_P(b) \leq v_P(a)$ for $P \in P(a)$ as required. □

REMARK 6.22: Let A be an integral ideal and $0 \neq a \in A \cap \mathbb{N}$. Then (a, α) for $\alpha \in A$ is a $P(a)$-normal presentation for A iff it is $P(a)$-normal for $\langle a, \alpha \rangle$ and furthermore $A = \langle a, \alpha \rangle$. It is easy to see that $\gcd(a^n, N(\alpha)) = N(A)$ is then sufficient as a test.

The importance of this criterium is three-fold

(1) Computing the minimum as $\text{den}(\alpha^{-1})$ allows for fast $O(n^2)$ algorithms to compute it
(2) To test $A = \langle a, \alpha \rangle$ is now a norm computation of elements ($N(\alpha)$) which can be done fast ($O(n^2)$) and a gcd
(3) There is no need for a factorisation

ALGORITHM 6.23 (2-Element Normal):

Input: A an integral ideal given via a $\mathbb{Z}$-basis and $a \in A \cap \mathbb{N}$
Output: $\alpha \in A$ such that (a, α) is a $P(a)$-normal presentation for A.

1: repeat
2: $\alpha := \text{Random}(A/a^2A)$
3: until (a, α) works.

LEMMA 6.24: Let α be chosen uniformly at random from A/a^2A. Then the probability that (a, α) is a $P(a)$-normal presentation for A is

$$\prod_{P|a}(1 - \frac{1}{N(P)})$$

PROOF. As above - $P(a)$ normal is just a valuation condition at the finitely many places in $P(a)$. The difference is that 6.15 gives a lower bound on the probability only. Analysing the proof, the elements counted there are exactly the ones giving a normal presentation, so we get the exact probability here. □

LEMMA 6.25: Let $A = \langle a, \alpha\rangle$ and $B = \langle b, \beta\rangle$ two ideals in P-normal representation (for the same set P). Then $\langle ab, \alpha\beta\rangle$ is a P-normal presentation for AB.

PROOF. Immediate from the valuations. □

Note: in general we have $\langle \alpha, \beta\rangle^d = \langle \alpha^d, \beta^d\rangle$ for any presentation (same for more than 2 generators), but this allows for fast multiplication as well. The downside here the need to have the same set of primes. In one important application however, this is automatically the case: CRT with prime ideals over the same prime number.

LEMMA 6.26: Let $P = \langle p, \alpha\rangle$ a prime ideal (eg. coming out of 5.38). Then

- if $e(P/p) > 1$, then (p, α) is $P(p)$-normal for P.
- if $e(P/p) = 1$ and $\alpha \notin P^2$ then (p, α) is $P(p)$-normal
- if $e(P/p) = 1$ and $\alpha \in P^2$ then $(p, p + \alpha)$ is $P(p)$-normal

We note, that to check $\alpha \in P^2$, it is sufficient to test $N(P)^2|N(\alpha)$.

LEMMA 6.27: Let $A = \langle a, \alpha\rangle$ an integral ideal in P-normal presentation. Then we can find $d \in \mathbb{N}$ such that $\langle 1, d\alpha^{-1}\rangle$ is a P-normal presentation for A^{-1}.

PROOF. Fix some arbitrary $b \in A \cap \mathbb{N}$ and split it as $b = cd$ with $v_Q(d) = 0$ for $Q \in P_L$ and $\gcd(c, d) = 1$, so $c \in \langle P\rangle$. Now since $\alpha|b = cd$ we have $v_Q(\alpha) \leq v_Q(d)$ for all $Q \notin P_L$. Since $v_Q(A^{-1}) = -v_Q(A) \leq 0$, and $v_Q(1) = 0$, the condition on the 1st generator is satisfied.

Now $v_Q(d\alpha^{-1}) = v_Q(d) - v_Q(\alpha) \geq 0$ for all $Q \notin P_L$ and $v_Q(d\alpha^{-1}) = -v_Q(\alpha) = -v_Q(A)$ for $Q \in P_L$. □

ALGORITHM 6.28 (Prime ideal testing):

Input: A an integral ideal
Output: `true` iff A is prime, `false` otherwise
1: $p := \min A \cap \mathbb{N}$
2: if p is not a prime, return `false`
3: factorise $p\mathbb{Z}_L = \prod Q_i^{e_i}$
4: if there is some i such that $A = Q_i$ return `true`
5: return `false`

3. Missing Prime Ideals

Now it's time to factorise the prime numbers not covered by 5.38. Unfortunately this is based on enitrely new ideas - or maybe not: it is meant to resemble the Berlekamp polynomial factorisation.

Let $\mathcal{O}$ be an order and p a prime number. The $\mathcal{O}/p\mathcal{O}$ is an $\mathbb{F}_p$-algebra, more specifically,

$$A := \mathcal{O}/\sqrt{p\mathcal{O}}$$

is a semi-simple $\mathbb{F}_p$-algebra. In fact, we know

$$\sqrt{p\mathcal{O}} = \cap Q_i$$

where Q_i runs over all prime ideals in $\mathcal{O}$ containing p and thus using CRT:

$$A = \mathcal{O}/\sqrt{p\mathcal{O}} = \oplus\mathcal{O}/Q_i = \oplus\mathbb{F}_{Q_i}$$

Note that $\mathbb{Z} \subseteq \mathcal{O}$ and thus induces an embedding $\mathbb{F}_p \subseteq A$.

Algorithm 6.29:

Input: A as above
Output: Either a proof that A is a field or a non-trivial idempotent ε such that $\varepsilon^2 = \varepsilon \neq 0, 1$

1: Set $\varphi : A \to A : x \mapsto x^p - x$ and compute $V := \ker \varphi$
2: if $\dim_{\mathbb{F}_p} V = 1$, then this proves A to be a field and we terminate.
3: Let $\alpha \in V \setminus \mathbb{F}_p$ and m_α it's minimal polynomial
4: Factorise $m_\alpha = m_1 m_2$ with non-constant coprime m_1, m_2
5: Find X, $Y \in \mathbb{F}_p[t]$ such that $Xm_1 + Ym_2 = 1$
6: Return $\varepsilon := (Xm_1)(\alpha)$

Proof. From the CRT it follows that φ is an $\mathbb{F}_p$-linear map with kernel

$$\ker \varphi = \oplus F_p$$

since $V_i := \ker \varphi|_{\mathbb{F}_{Q_i}} = \mathbb{F}_p$ for all i. This shows that steps (1) and (2) are correct and that we can find some α in step (3). In each component V_i of V, the minimal polynomial is linear, thus m_α as the lcm of the minimal polynomials in V_i is the product of pairwise coprime linears.

Now since $m_\alpha(\alpha) = 0$, we have $Xm_1 \equiv 1 - Ym_2 \bmod m_\alpha$, thus $\varepsilon^2 = (Xm_1)(Xm_1) = (Xm_1)(1 - Ym_2) = Xm_1 - XYm_1m_2 = Xm_1$ hence ε is idempotent. Furthermore, since $\gcd(X, m_2) = 1$, ε is non-zero and $1 - \varepsilon = Ym_2(\alpha) \neq 0$ by the same argument. □

Some comments:

- The idempotent is used to split $A = \varepsilon A + (1-\varepsilon)A$ into two smaller $\mathbb{F}_p$-algebras (or prove that A is a field). Using the algorithm again, we can split A into a direct sum of fields:

$$A = \mathcal{O}/I = \oplus\mathcal{O}/Q_i = \oplus\mathbb{F}_{Q_i}$$

- To compute the minimal polynomial of α we use the $\mathbb{F}_p$-vectorspace structure: writing $\alpha^i \in \mathbb{F}_p^n$, we can find the coefficients of the minimal polynomial as kernel vectors.
- The multiplication in A is of course inherited from $\mathcal{O}$. In order to multiply in A we simply lift the elements to $\mathcal{O}$, form the product and project down again
- Alternatively, we can compute a multiplication table for A
- In step (4) we use the ordinary factorisation over finite fields to split m_α. Since we have more factors, we may as well split A according to all of them.
- Step (5) is, of course, just the extended gcd over $\mathbb{F}_p$
- There is a variation of this algorithm valid in characteristic 0.

LEMMA 6.30: Let $A/I = C/I \oplus D/I$ for I as above. Then we have two ideals $Q_1 := \langle I, C\rangle$ and $Q_2 = \langle I, D\rangle$ and $CD = I$. In order to compute Q_i we just need an arbitrary lift of any $\mathbb{F}_p$-basis of C to $\mathcal{O}$.

LEMMA 6.31: Let $A = \mathcal{O}/\sqrt{p\mathcal{O}} = \oplus\mathcal{O}/Q_i$ for fields $\mathcal{O}/Q_i$. Then Q_i is a prime ideal and $f_i(Q_i) = \dim_{F_p}(\mathcal{O}/Q_i)$. In particular we can find f_i without computing Q_i

The missing data for the prime ideals are the ramification index e_i. In order to compute this we can "simply" compute the valuation

$$e_i = v_{Q_i}(p)$$

however, this requires a valuation element. We can either compute this using CRT (CRT needs just bases!) requiring a large number of ideal multiplications, or use the 2-element normal presentation, which might be hard to find.

EXAMPLE 6.32: Let $f := t^3 + t^2 - 2t + 8$. We showed before that the maximal order is $\mathbb{Z}_L = \mathbb{Z} + \mathbb{Z}t + \mathbb{Z}(\frac{1}{2}(t + t^2))$. Now we'd like to compute the (alleged) three prime ideals over 2.

To compute the radical, we need the kernel of $x \mapsto x^4 \bmod 2\mathbb{Z}_L$. $1^4 = 1$, $t^4 \bmod f = 3t^2 - 10t + 8 = 6\omega_3 - 13\omega_2 + 8 \equiv \omega_2 \bmod 2$ **CHECK** and $(t + t^2)^4 \bmod f = 40t^2+8t+288$, dividing by 4: $(\frac{1}{2}(t+t^2))^4 = 10t^2+2t+72 = 5\omega_3-2\omega_2+18 \equiv \omega_3 \bmod 2$, hence $\ker = 0$ and $I = \langle 2\rangle$, so $A = \mathbb{F}_2^3$. Next, we need $\ker(x \mapsto x^2)$: $1^2 = 1$, $\omega_2^2 = \omega_2^2$ and $\omega_3^2 = \omega_3 - 2\omega_2 - 2$, looking at this mod2, we see that $V = A$ of dimension 3.

Take $\alpha = \omega_2 = t$, we know the minimal polynomial in $\mathbb{Z}[t]$, $t^3 + t^2 - 2t + 8 \equiv t^2(t + 1) \bmod 2$, hence $m_\alpha = t(t + 1)$. From $1 = 1 \cdot t + 1 \cdot (t + 1)$ we compute $\varepsilon = \alpha = \omega_2$ and $A = \langle\omega_2\rangle/I + \langle\omega_2 + 1\rangle/I$.

By computing representation matrices, we see that the 1st ideal has norm 4, while the second has norm 2, hence is already prime. We now need to recurse the algorithm on $\mathbb{Z}_L/\langle\omega_2, I\rangle$.

We compute a basis for $\langle\omega_2, 2\rangle$ as 2, ω_2 and $2\omega_3$, hence $\alpha \in \mathbb{Z}_K/\langle\omega_2, 2\rangle \setminus \mathbb{F}_2$ can be ω_3. Since $\omega_3^2 = -2 - 2t + \omega_3 \equiv \omega_3 \bmod \langle\omega_2, 2\rangle$, the minimal polynomial is again $t(t + 1)$. Thus the final split is $\langle\omega_3, \omega_2, 2\rangle$, $\langle\omega_3 + 1, \omega_2, 2\rangle$ and $\langle\omega_2 + 1, 2\rangle$.

To summarise:

ALGORITHM 6.33 (Cohen-Lenstra):

Input: Order $\mathcal{O}$ and prime number p

Output: All prime ideals containing p.
1: Compute $I = \sqrt{p\mathcal{O}}$
2: Let $H := \{I\}$
3: while H is non-empty do
4: take B from H and remove it.
5: apply 6.29 to $\mathcal{O}/B$ and either print B (in case $\mathcal{O}/B$ is a field) or include the new B_i in H

4. S-Units

THEOREM 6.34 (Product formula): Let $\alpha \in L^*$ be arbitrary. Then

$$\prod_{i=1}^{n} \alpha^{(i)} \prod_{P \in \mathbb{P}_L} N(P)^{-v_P(\alpha)} = 1$$

PROOF. We know $|N(\alpha)| = N(\alpha\mathbb{Z}_L)$, so the statment follows from the computation of the norm via conjugates, the unique prime decomposition of ideals in Dedekind domains and the multiplicativity of the norm of ideals. □

THEOREM 6.35: Let $S \subseteq \mathbb{P}_L$ be a finite set of prime ideals. Then $T(U_S) = TU(\mathbb{Z}_L)$ and

$$U_S/T(U_S) = \langle \varepsilon_i | 1 \leq i \leq \#S + r_1 + r_2 - 1 \rangle$$

is a free $\mathbb{Z}$-module of rank $r_1 + r_2 - 1 + \#S$.

PROOF. Define a map:

$$\varphi : U_S \to \mathbb{Z}^S : \alpha \mapsto (v_P(\alpha))_{P \in S}$$

then this is well defined and, mostly by definition, $\ker \varphi = U_L$. Let $P \in S$ be arbitrary, then, due to $h_L < \infty$, $P^h = \langle \beta_P \rangle$. Clearly, $\varphi(\beta) = (0, \ldots, 0, h, 0, \ldots, 0)$ showing that $\mathrm{rg}_{\mathbb{Z}}(\operatorname{im} \varphi) = \#S$ □

So the class group algorithm can be viewed as trying to compute a generating system for the S-units. We also note that the map φ used in the proof of the theorem is *constructive*: all we need is to compute valuations $v_P(\alpha)$ for a finite fixed set S.

REMARK 6.36: Let $\alpha \in L^*$ and $S \subseteq \mathbb{P}_L$ a finite set of prime ideals. Then $\alpha \in U_S$ iff $N(\alpha) = \prod_{P \in S} N(P)^{v_P(\alpha)}$ which is easy to test without computing U_S.

However, the problem is using the S-unit theorem is the kernel. We start with the easy observation:

LEMMA 6.37: Let $\alpha_i \in U_S$ $(1 \leq i \leq a)$ and define $V := \langle \alpha_i | i \rangle \leq U_S$. Set $M := (v_P(\alpha_i))_{i,S} \in \mathbb{Z}^{a \times \#S}$ and $k_j \in \mathbb{Z}^a$ a $\mathbb{Z}$-generating system for $\ker M$. Then

$$\ker \varphi|_V = \langle \prod_j \alpha_j^{k_{i,j}} | i \rangle = V \cap U_L$$

PROOF. Since φ is a homomorphism, we note that a linear combination of rows of M correspond to power products of the α_i, thus by the remark above, the $\ker M$ corresponds to units. □

So, we see that this gives a new method for actually computing units! In order to use this, we need to solve the problem of finding dependencies between units. We'd like to use the logarithmic L-maps introduced in the chapter on units, but now need to be more careful about the numerical problems: we are only working in finite precision, hence cannot decide (numerically) if $L(\varepsilon) = 0$ holds or not. To help we have (without proof)

THEOREM 6.38 (Dobrowski): Let $\alpha \in \mathbb{Z}_L$, $\deg L = n > 1$. Then either $\alpha \in TU(\mathbb{Z}_L)$ or there exists a conjugate $\alpha^{(i)}$ such that

$$|\alpha^{(i)}| \geq 1 + \frac{1}{6}\frac{\log n}{n^2}$$

COROLLARY 6.39: Let $\varepsilon \in U_L$ then either $\varepsilon \in TU(\mathbb{Z}_L)$ or $\|L(\varepsilon)\|_2 \geq \frac{21}{128}\frac{\log n}{n^2}$.

PROOF. We have $L(\varepsilon) = (\log|\varepsilon^{(i)}|)_i$. By Dobrowski, either $L(\varepsilon) = 0$ or $|\varepsilon^{(i)} \geq 1 + \frac{1}{6}\frac{\log n}{n^2}$, so we assume the latter. Noting that for $1 > x > 0$ we have $\log(1+x) > x - 1/2x^2 = x(1-1/2x)$, (since $x \to x - 1/2x^2$ is increasing on $[0,1]$), so

$$\begin{aligned}
\log 1 + \frac{1}{6}\frac{\log n}{n^2} &\geq \frac{1}{6}\frac{\log n}{n^2} - \frac{1}{2}\frac{1}{36}\frac{\log^2 n}{n^4} \\
&= \frac{1}{6}\frac{\log n}{n^2}(1 - \frac{1}{2}\frac{1}{6}\frac{\log n}{n^2}) \\
&\geq \frac{1}{6}\frac{\log n}{n^2}(1 - \frac{1}{2}\frac{1}{6}\frac{3/4}{4}) \\
&= \frac{1}{6}\frac{63}{64}\frac{\log n}{n^2}
\end{aligned}$$

This works since $n \to n^{-2}\log n$ is decreasing for $n \geq 2$ and $\log 2 \leq 3/4$ (numerically). □

LEMMA 6.40: Let ε_i $(1 \leq i \leq a < r_1 + r_2)$ be independent units. Then there exists some $K > 0$ such that if ε is an additional unit and $\varepsilon = \prod \varepsilon_i^{n_i}$ then $n_i \leq K\|L(\varepsilon)\|_2$.

PROOF. If $\varepsilon = \prod \varepsilon_i^{n_i}$, then clearly $L(\varepsilon) = \sum n_i L(\varepsilon_i)$ as well. Let $X := (L(\varepsilon_1), \ldots, L(\varepsilon_i))$, then we get $L(\varepsilon) = X(n_i)_i$. We now multiply by X^t from the left: $X^t L(\varepsilon) = (X^t X)(n_i)_i$ where $X^t X \in \mathrm{Gl}(a, \mathbb{R})$.

Consider $\mathcal{L} := \sum \mathbb{Z}L(\varepsilon_i)$ the lattice spanned by $L(\varepsilon_i)$. Then Minkowski's theorem shows

$$M_1^a \leq \gamma_a^a d(\mathcal{L})$$

By construction $\det X^t X = d^2(\mathcal{L})$ and, by Dobrowski, $M_1 \geq \frac{21}{128}\frac{\log n}{n^2} =: K_0$, so $\det X^t X \geq K_0^a \gamma_a^{-a} =: K_1$ By Cramer's rule

$$n_i = \det(X^t L(\varepsilon_1, \ldots, L(\varepsilon), \ldots, L(\varepsilon_a)))/\det(X^t X)$$

Hadamat shows

$$\det(X^t(L(\varepsilon_1), \ldots, L(\varepsilon), \ldots, L(\varepsilon_a))) \leq \|L(\varepsilon)\|_2 K_2, \text{ so} n_i \leq K_2/K_1\|L(\varepsilon)\|_2$$

as required. □

We note that the "denominator" estimate from Dobrowski's theorem is very pessimistic. In important cases (eg. if the unit group has already full rank), we can frequently use better lower bounds.

The lemma is instrumental in deciding how much precision needs to be used for the real-linear algebra:

$$L(\varepsilon) = \sum n_i L(\varepsilon_i)$$

iff

$$\|L(\varepsilon) - \sum n_i L(\varepsilon_i)\|_2 \leq \frac{21}{128}\frac{\log n}{n^2}$$

Note however, that $L(\varepsilon) = \sum n_i L(\varepsilon_i)$ does not give the dependency: $\ker L = TU(\mathbb{Z}_L)$, so we sill need to account for the torsion.

An additional complication comes from the rounding-errors during the linear algebra, however those are either well known (to numerical people) or can be avoided by using integral operations only: Instead of solving $L(\varepsilon) = \ldots$, we define $L_\lambda(\varepsilon) := (\lfloor \lambda \log |\varepsilon^{(i)}| \rceil)_i$ and search for short elements in

$$\mathbb{Z}L_\lambda + \sum \mathbb{Z}L_\lambda(\varepsilon_i)$$

We know the shortest element in here (provided λ is large enough), as the non-zero minimum should larger than $\lambda\frac{21}{128}\frac{\log n}{n^2}$. Hence any short combination has to come from an exact zero.

The goal now is to combine all this into an algorithm to compute the class group and, if possible, the unit group as well. By the S-unit theorem we know that the relation matrix wil have full rank, eventually. The proof of the Dirichlet unit theorem shows furthermore, that eventually, the kernel of the relation matrix will generate the full unit group. Thus, eventually, if the relation matrix is "complete" we have both the units and the class group.

The problem is in deciding when we are "complete": it is "easy" to check that both image and kernel have the correct rank, but this only shows that we have a subgroup of the S-unit group of finite index. We'd like the index to be 1.

5. ζ-Function

DEFINITION 6.41: Let

$$\zeta_L(s) := \sum_{A \leq \mathbb{Z}_L} N(A)^{-s}$$

for $\Re(s) > 1$ the ζ-function of L.

LEMMA 6.42: The ζ-function has many important properties:

(1) The series convereges uniformely for $\Re(s) > 1$, thus defines a holomorphic function there.
(2) The function has a meromorphic extension to the entire complex plane $\mathbb{C}$
(3) The function has a simple pole at $s = 1$ and is holomorphic elsewhere
(4) There is a functional equation linking $\zeta_L(s)$ to $\zeta_L(1 - s)$

PROOF. Unfortunately, most of this is too hard for now - it requires a dedicated lecture. □

LEMMA 6.43 (GRH- Generalised Riemannian Hypothesis): It is conjectured that
$$\{s \in \mathbb{C} | \zeta_L(s) = 0\} \subseteq \{s \in \mathbb{C} | \Re(s) = 1/2\}$$
apart from "trivial zeroes".

The importance of the ζ-function for us stems from some consequences:

THEOREM 6.44: For the residue of the ζ-function we have:
$$\operatorname{Res}_{s=1} \zeta_L = 2^{r_1}(2\pi)^{r_2} \frac{h_L R_L}{\omega\sqrt{|d_L|}}$$
where h_L is the class number, R_L the regulator, ω the size of the torsio group and d_L the discriminant of the maximal order.

So, if we could compute the residue, we'd have a link between the regulator and the class number! The next theorem implies a means to compute it (well approximate it)

THEOREM 6.45 (Euler product): The ζ-function admits an *Euler product*
$$\zeta_L(s) = \prod \frac{1}{1 - N(P)^{-s}}$$
where the product converges uniformely on $\Re(s) > 1$

LEMMA 6.46:
$$\operatorname{Res}_{s=1} \zeta_L = \prod_{p \in \mathbb{P}_{\mathbb{Z}}} \prod_{Q|p} \frac{1 - 1/p}{1 - 1/N(Q)}$$

This gives a means to approximate the residue, the factors of the above product are easily computed (also explaining why in the index divisor factorisation it was important to easily get the inertia degrees, hence the norms).

Of course, the lemma does not mention at all the rate of convergence. Here we have:

THEOREM 6.47 (Bach, GHR): There exists an explicit constant $D > 0$ such that the residue can be approximated within an error of $\sqrt{2}$ using primes of norm $\leq D \log^2(|d_L|)$ only. Moreover, there is an polynomial algorithm computing this approximation.

This means, we have an algorithm, running on $O(\log^2 |d_L|)$ computing some number E satisfying $1/\sqrt{2} \leq E/\operatorname{Res} \leq \sqrt{2}$.

This implies a stopping condition of the relation search in the class group algorithm: if the relation matrix has full rank, we have a tentative class group, more precisely, we found a finite group C such that $\mathrm{Cl}_L = C/U$, hence $h_L | \#C$, we have a multiple of the class number. Similarly, if the kernel is large enough, we have a subgroup U of the unit group of finite index, hence we also have a multiple R of the regulator. Combining everything: iff $1/2 < \#CR/E < 2$ then $C = \mathrm{Cl}$ and $R = R_L$ and we're done.

Using the GRH, we get another benefit:

THEOREM 6.48 (Bach, GRH): Let

$$B := \{Q \in \mathbb{P}_L | N(Q) \leq 12 \log^2 |d_L|\}$$

then $\mathrm{Cl}_L = \langle B \rangle$

Since $\log^2 |d_L| \ll \sqrt{|d_L|}$, this is much better than the use of the Minkowski-bound. However

- This is conditional under the GRH only
- In contrast to the Minkowski bound, giving a representative for any ideal class bounded by the constant, this bounds a generating set only.

It should be noted that, experimentally, even the Bach-bound is too large.

THEOREM 6.49 (Brauer-Siegel): Let L_n be a sequence of number fields of fixed degree N over $\mathbb{Q}$. Then

$$\log h_n R_n \sim \log \sqrt{|d_n|}$$

In partiular to imaginary quadratic fields (where the regulator is trivial), that $h_n \to \infty$. In this case, this was made constructive: there are explicit lists of all imaginary quadratic fields with class number 1, 2, ..., 100 by now (Watkins, 2004).

Experimentally, in general, the class number is small, hence the regulator is large. However, it is unknown if there is an infinite number of fields with class number one. Heuristically and experimentally, 75% of real quadratic fields have class number 1. This is part of the Cohen-Lenstra (and Malle, Martinet) conjectures about class groups. As a consequence, for real-quadratic fields, we have $\mathrm{reg} = \pm \log |\varepsilon^{(1)}| \sim \sqrt{d}$ for any fundamental units. This shows, that we cannot expect to be able to write any fundamental unit in time polynomial in the input - at least not this way, using coordinates. Also, since the real-precision necessary to obtain the logarithm from the coordinate is also at least as large as the number of digits, we need a *huge* precision.

A partial solution to this problem is to use the *product representation*: in the algorithm, units are always obtained as power products: $\varepsilon = \prod \alpha_i^{n_i}$. Assuming α_i and n_i are "small" this reduces the precision.

We'll refine the class group algorithm based on the ideas accumulated so far. We assume that we somehow have fixed a factor base

$$B := \{Q \in \mathbb{P}_L | N(Q) \leq X\}$$

and an approximation E to the Euler product as above.

ALGORITHM 6.50 (Relation processing):

Input: α, a possible relation
Output: Either `false` if α is no relation or the complete factorisation.

1: Compute $N := |N(\alpha)|$
2: If N is not X-smooth, return `false`
3: For $Q \in B$ do
4: if $N(Q)|N$, then
5: $e_Q := v_Q(\alpha)$
6: $N := N/N(Q)^{e_Q}$. If $N = 1$, return $(e_Q)_Q$

ALGORITHM 6.51 (Relation matrix processing):

Input: a set of (possible) relations S
Output: `false` if we need more relations, h_L and reg_L otherwise
1: Compute the relation matrix $M = (M_{\alpha,Q})_{\alpha,Q}$ using the above algorithm.
2: Compute the Smith-form of M. If M has not full rank, i. e. some elementary divsors are 0, return `false`, else let h be the product of the elementary divsors.
3: Compute a basis k_i for the kernel of M.
4: Compute $U := \langle \prod \alpha^{k_i,\alpha} | i \rangle$.
5: If $\operatorname{rg} U < r$, return `false`, else $R := \operatorname{reg}(U)$
6: If $1/\sqrt{2} < Rh < \sqrt{2}$, return (h, R), else `false`

There are many practical optimisations to both algorithms to be done:

(1) In general, we do not compute the norm exactly, but use a probabilistic algorithm only. If the norm is wrong, we "loose" a few relations, but might gain speed.
(2) Also, in general, $\alpha \in A$ for some explicitly known ideal A, hence $N(A)|N(\alpha)$ which is also used
(3) Instead of computing the Smith-form, we usually start by computing the rank modulo some medium sized prime.
(4) If the rank is not full, we also study the missing pivot elements to find the ideals that need more relations. This allows for a more targeted search
(5) Directly computing the entire kernel of M is very expensive (time and memory), hence one computes only a few kernel elements coming from suitable submatrices. If those are sufficient, we're done.
(6) Also, the process is incremental: if we need more relations, we keep as much information as possible: a partial echelon form modulo p, a Smith-form, some units. We simply append and process the new relations.
(7) If, in step (6) we have $1/m < RH < m$ we can apply the saturation techniques from 4.27 noting that (almost) nothing in there is unit specific. It is sometimes much faster to saturate than to hunt the missing relation.

Still missing are, of course

(1) Relation search
(2) p-th roots for the saturation (compact representation)
(3) Overall analysis

6. Class Group

ALGORITHM 6.52 (Ideal-Class Reduction):

Input: Ideal $A \leq \mathbb{Z}_L$, weights $\lambda \in \mathbb{R}^r$ such that both $N(A)$ and $\exp \lambda_i = O(d_L)$
Output: α such that $A\alpha \leq \mathbb{Z}_L$, $N(\alpha A) \leq C\sqrt{|d_L|}$ for some explicit C independent of A and λ, $T_{2,\lambda}(\alpha)$ small.
1: $v := (1/n) \sum c_i \lambda_i$, $\mu := \exp(\lambda_i - v)$
2: α the 1st LLL-basis element of A^{-1} in $T_{2,\mu}$

PROOF. By construction, $\prod \mu_i = 1$, hence the algebraic-geometric means shows

$$|N(\alpha)|^{2n} \leq \frac{1}{n} T_{2,\mu}(\alpha)$$

LLL implies

$$T_{2,\mu}^n(\alpha) \leq C|d_L|N(A)^{-2}$$

hence $N(\alpha A) \leq C'\sqrt{|d_L|}$ and the rest follows. □

ALGORITHM 6.53 (Ideal Product Reduction):

Input: $\prod A_i^{n_i}$ for $n_i \geq 0$ and $A_i \leq Z_L$
Output: $\prod \alpha_i^{r_i}$, $B \leq \mathbb{Z}_L$ such that

$$\prod A_i^{n_i} = B \prod \alpha_i^{r_i}$$

and $N(B)$, $T_2(\alpha_i)$ "small".

1: $B := \mathbb{Z}_L$
2: repeat
3: Find a sub-product $C = B \prod A_j^{k_j}$ such that $N(C) \geq |d_L|$ is minimal.
4: Use 6.52 to write $C = \alpha B$ for some small α and a new ideal B and replace the product.

For any integral ideal $A = \prod Q^{v_Q(A)}$ we define $\lfloor \sqrt[r]{A} \rfloor := \prod Q^{\lfloor v_Q(A)/r \rfloor}$. While in general, we cannot compute this without a full factorisation, in the context of class group algorithms, the factorisation is genrally known.

ALGORITHM 6.54:

Input: $\prod \alpha_i^{k_i}$ with α_i small, $l > 0$ and B the corresponding principal ideal (of small norm).
Output: β_i such that $\prod \alpha_i^{k_i} = \prod_{i=0}^{k} \beta_i^{l^i}$ where $k = O(\log(T_2(\prod \alpha_i^{k_i})))$

1: Compute $(v_i)_i := (\prod \alpha_j^{k_j})^{(i)}$, the conjugates
2: Set $I := \mathbb{Z}_L$
3: for $k := \log \|v\|_\infty$ to 0 do
4: $\lambda_i := \sqrt[l^k]{|v_i|}$
5: Call 6.52 for $I^l \lfloor \sqrt[l^k]{B} \rfloor$ and λ to find β_k and and new (small) ideal I
6: $(v_i) := (v_i/(\beta_k^{(i)})^{l^k})_i$

PROOF. In each iteration, $\|v\|_\infty$ is reduced by a factor of $\sqrt{|d_L|}$ roughly and $N(\sqrt[l^k]{B})$ stays bounded. □

The algorithm 6.54 is important for 2 unreleated reasons:

(1) It allows the reduction modulo l-th powers, hence, in particular, the "easier" computation of l-th roots of huge power products for the saturation
(2) The resulting power product has a total size that is polynomial in the logarithm of the conjugates, hence allows to compute a representation of units that is polynomial in the regulator!

However, in order to apply those techniques we still need a real precision that depends on the size of the input, thus can be much too large. A second, more subtle problem is that, on input we have a power product of relations, while on output we generally don't.

It should be mentioned that the algorithm outlined above is a crucial part in modern integer factorisation methods: the NFS algorithm produces, near the end, a huge list of $> 10^6$ algebraic numbers. At that point of the algorithm it it known that the product is a square. One needs a root to finish.

To find relations we have several possibilities and this is on-going research. Fundamentally, one tries to find suitable T_2-small elements, since then they will have a "small" norm, hence should be composed from "small" prime ideals.

ALGORITHM 6.55 (Relations 1):

Input: Integral ideal A and weights v
Output: Relation(s) involving A
1: find $T_{2,v}$ small elements as LLL-basis elements

ALGORITHM 6.56 (Relations 2):

Input: Integral ideal A and weights v
Output: Relation(s) involving A
1: find $T_{2,v}$ small elements via lattice enumeration

ALGORITHM 6.57 (Relations 3):

Input: Integral ideal A
Output: Relation(s) involving A
1: find a random power product C of elements in the factor basis B until the norm is larger than d_L
2: Use 6.52 to find α such that αC is small and hope that α is a relation

ALGORITHM 6.58 (Relations 4):

Input: Integral ideal A
Output: Relation(s) involving A
1: Find two T_2 small elements α and $\beta \in A$
2: Compute $f(x,y) = N(x\alpha + y\beta)/N(A) \in \mathbb{Z}[x,y]$
3: Use sieve-methods to find lots of pairs (x,y) such that $f(x,y)$ is B-smooth, i. e. involves only primes in B
4: return $x\alpha + y\beta$

The 3rd method is the one that allowed Buchmann to analyse the overall algorithm. His result is based on

THEOREM 6.59: Let

$$\psi_L(x,y) := \#\{A \leq \mathbb{Z}_L | N(A) \leq x \text{ and } P|A \Rightarrow N(P) \leq y\}$$

be the number of y-smooth ideals of norm bounded by x. Then $\forall n \in \mathbb{N}$, $\varepsilon > 0 \exists x_0(\varepsilon, n) \forall x > x_0 \forall y, L$ such that $\max(\log^{1+\varepsilon}(x), \log^{2+\varepsilon}|d_L|) \leq \exp(\log^{1-\varepsilon}(x))$ we have

$$\psi_L(x,y) \geq x \exp(-u(\log(u + \log\log u + O(\frac{1}{\varepsilon} + \log \tilde{n}))))$$

for $u := \log x / \log y$ and $\tilde{n}$ the degree of the normal closure of L

This theorem is applied to $y := C \log^2 |d_L|$ (which is not quite correct) to show that in this case there exist sufficiently many "smooth" ideals of bounded norm. Since the only (practical) reduction, using LLL, results in ideals of norm $O(\sqrt{|d_L|})$, we're going to have $x = \tilde{C}\sqrt{|d_L|}$ (where $\tilde{C}$ is explicit!) and have to choose C (thus y) to make the above estimate yield enough relations. Obviously, we need at least one relation for each element of the factor base, so, while a larger factor base makes the search for individual relations easier it also requires more relations to be found.

Buchmann analysed this dependency and came up with an asymptotically optimal choice resulting in a sub-exponential total run-time.

ALGORITHM 6.60 (Complete Classgroup):

Input: A number field L
Output: A factor basis B, a set of relations $\alpha_i \in U_B$ and a relation matrix giving the strutcture of the class group.
1: Compute $\mathbb{Z}_L$ (or better: a LLL-reduced basis for $\mathbb{Z}_L$)
2: Compute a factor base $B := \{Q \in \mathbb{P}_L | N(Q) \leq C_1\}$
3: Compute an approximation to the Euler product (with error bounded by $\sqrt{2}$)
4: Find enough relations so that the relation matrix has full rank and approximates the Euler product by a small error
5: For all small primes (bounded by the error) and all elementary divisors of the relation matrix, saturate the relations.
6: For all prime $Q \in \mathbb{P}_L \setminus B$ and $N(Q) \leq C_2$ find some $\alpha \in Q \setminus Q^2$ such that $\alpha \in U_{B \cup \{Q\}}$

Typically, $C_1 = c_1 \log^2 |d_L|$ for $c_1 < 1$ and C_2 is either $12 \log^2 |d_L|$ for GRH results or $c_2\sqrt{|d_L|}$ for unconditional results. Step (4) is inserted since saturation is frequently faster in finding the "last" missing relation. Step (5) finds the missing relations, while (6) proves that we did not make a mistake in choosing C_1 too small. Without (6) we could have computed a subgroup of the class group only.

ALGORITHM 6.61 (S-Units):

Input: A finite set $S \subseteq \mathbb{P}_L$ and the output of 6.60
Output: A set of fundamental S-units
1: for all $Q \in S$ find some $\alpha \in Q \setminus Q^2$ such that $\alpha \in U_{B \cup S}$
2: Build an extended relation matrix M for $B \cup S$ and the new relations α
3: $U_S = \{m \in [M]_{\mathbb{Z}} | m_Q = 0 \text{ for } q \notin S\}$

ALGORITHM 6.62 (Principal ideal testing):

Input: An integral ideal $A \leq \mathbb{Z}_L$ and the output of 6.60
Output: `false` or α such that $\langle \alpha \rangle = A$
1: find $\alpha \in A$ such that $N(\alpha)/\prod N(P)^{v_P(\alpha)} = N(A)/\prod N(P)^{v_P(A)}$
2: if $(v_P(\alpha))_{P \in S} \in [M]$ then A is a PID and a generator can be found using linear algebra

For α as above we have $A/\alpha \in \langle B \rangle$, and thus A is PID iff A/α is. The latter can now be decided using the relations already known. On the other hand, since $\langle B, L^* \rangle = I_L$, such an α does exist.

This is the basis for a great deal of further algorithms, e.g one can solve norm equations, study field extensions (class field theory), aid other Diophantine equations (Thue, Unit equations, Indexform equations)

EXAMPLE 6.63: Let $L := K(\sqrt{a})/K$ be a number field of degree 2. Then we can find M/L of degree 2 such that M/K is cyclic iff $a = u^2 + v^2$ for some u, $v \in K$. This is equivalent to $a = N(\gamma)$ for $\gamma \in K(i)$.

PROOF. We note that $K(\sqrt{a}) = K(\sqrt{b})$ iff $a/b \in (K)^2$ and, since the characteristic is different from 2, and M/L is quadratic, $M = L(\sqrt{\alpha})$ for some $\alpha \in L$. Hence $\alpha = s + t\sqrt{a}$. Since M/K should be cyclic, we see $t \neq 0$ since otherwise $\mathrm{Aut}(M/K) = V_4$. Thus we see $(x^2 - (s + t\sqrt{a}))(x^2 - (s - t\sqrt{a})) \in K[x]$ is irreducible with a root $\sqrt{\alpha} \in M$. Galois immediately show that $x^2 - (s - t\sqrt{a})$ needs to have a root $\sqrt{\beta}$ as well, $\alpha/\beta \in (L)^2$ hence $\alpha\beta \in (L)^2$ also. We conclude $\alpha\beta = s^2 - t^2 a = (u + v\sqrt{a})^2 = u^2 + v^2 a + 2uv\sqrt{a}$ and u, v, s, $t \in K$, hence $uv = 0$. If $v = 0$ then one can see that the Galois group is wrong again by studying

$$\sqrt{s + t\sqrt{a}} \mapsto \alpha/\beta\sqrt{s - t\sqrt{a}}$$

which has only order 2 then. So $u = 0$ and

$$s^2 - t^2 a = v^2 a$$

thus

$$a = \frac{a^2}{t^2 + v^2} = (\frac{sv}{v^2 + t^2})^2 + (\frac{st}{v^2 + t^2})^2$$

as claimed. □

To solve norm equations, like in the last example, we can use S-units. But before we start, we need a lemma:

LEMMA 6.64: Let $L/\mathbb{Q}$ be quadratic and $A \in I_L$ be an ideal of norm 1. Then

$$A = \prod Q^{1-\sigma}$$

for suitable prime ideals $Q \in \mathbb{P}_L$ and $\sigma : L \to L$ the non-trivial automorphism.

PROOF. Let $p \in \mathbb{P}_\mathbb{Z}$ and Q_i the prime ideals above p. Then since $N(A) = 1$, we also have $\prod_{Q|p} N(Q)^{v_Q(A)} = 1$. Now, we either have $p\mathbb{Z}_L = Q$ or $= Q^2$, in which case $v_Q(A) = 0$ or $p\mathbb{Z}_L = Q_1 Q_2 = Q^{1+\sigma}$ and $v_Q(A) = -v_{\sigma(Q)}(A)$. So $v_Q(AQ^{v_Q(A)(1+\sigma)}) = 0$ and $N(AQ^{v_Q(A)(1+\sigma)}) = 1$. By induction, A can be seen to be of the desired form. □

THEOREM 6.65: Let $L/\mathbb{Q}$ be quadratic, $k \in \mathbb{Z}$ arbitrary. Assume there is some $\theta \in L$ such that $N(\theta) = k$, we can find some $\tau \in U_S$ with $N(\tau) = k$ for S containing $\mathrm{supp}\, k\mathbb{Z}_L$ and large enough to allow $\langle S \rangle = \mathrm{Cl}_L$

PROOF. Let θ the solution, $N(\theta) = k$. Since k is integral, we can find an ideal $\Theta \leq \mathbb{Z}_L$ such that $N(\Theta) = |k|$, $\operatorname{supp}\Theta \subseteq \operatorname{supp} k\mathbb{Z}_L$. Now, by construction, $N(\theta\Theta^{-1}) = 1$, thus by the lemma

$$\theta\Theta^{-1} = \prod Q^{1-\sigma}.$$

Since S generates the class group, we can find $\alpha_Q \in L$ and $B_Q \in \langle S \rangle$ such that $Q = \alpha_Q B_Q$. Now

$$\theta\Theta^{-1} = \prod Q^{1-\sigma} = \prod \alpha_Q^{1-\sigma} \prod B_Q^{1-\sigma}$$

thus

$$\theta \prod \alpha_Q^{1-\sigma} = \Theta \prod B_Q^{1-\sigma}$$

Now $N(\prod \alpha_Q^{1-\sigma}) = 1$ and clearly $\operatorname{supp}\theta \prod \alpha_Q^{1-\sigma} = \operatorname{supp}\Theta \prod B_Q^{1-\sigma} \subseteq S$, so we have a solution in U_S. □

Note: it is really neccessary for S to be larger than $\operatorname{supp} k$: take for example $L := \mathbb{Q}[\sqrt{34}]$. This field has class number 2 and fundamental unit $\varepsilon = 35 + 6\sqrt{34}$ or norm $+1$. On the other hand, we have $3\mathbb{Z}_L = P_1P_2$, hence $P_1P_2^{-1}$ is a principal ideal of norm 1. As it turns out the generator $\alpha = 1/3(-5 - \sqrt{34})$ has in fact norm -1.

In order to solve norm equations in $\mathbb{Z}_L$ rather than L we have a couple of options:

(1) Find all integral ideals of the correct norm and then do PID testing
(2) Use the S-unit approach to parametrise all field elements with the correct norm and intersect with $\mathbb{Z}_L$
(3) Use a direct, geometric approach (nice algorithm, but *slow*)

Norm equations in arbitrary orders $\mathcal{O}$ can then either be reduced to norm equations in $\mathbb{Z}_L$ by observing that $\mathbb{Z}_L/\mathcal{O}^*$ is finite - or one can use the geometric approach. Norm equations are important as a building block for more general Diophantine equations:

- Thue equations: Let $F \in \mathbb{Z}[x, y]$ be homogenous and irreducible. Then $F[x, y] = k$ is a Thue-equation. Such an equation has only finitely many solutions and each of them solves $N(x + y\theta) = k$ for θ a root of $F[1, y]$ in the corresponding number field. So Thue equations need norm equations as the first step
- S-unit equations: Solve $a\varepsilon_1 + b\varepsilon_2 = c$ for S-units ε_i and arbitrary a, b, c. Again, this has only finitely many solutions, and is reduced to Thue equations.
- Indexform equations: Try to find (all) $\alpha \in \mathbb{Z}_L$ such that $(\mathbb{Z}_L : \mathbb{Z}[\alpha]) = k$. This is reduced to S-unit equations
- Searching for points on $y^2 = x^3 + k$, so called Mordell-curve is reduced, among other things, to indexform equations.

7. The Number Field Sieve

We want to factorise N a *huge* number (say 120 or more decimal digits). We used the primality provers to see that N is neither a power nor a prime. We also established easily, that N is not divisible by any prime $< 10^{10}$. What's next?

Recall that most modern factorisation methods try to find X, $Y \in \mathbb{Z}$ such that $X^2 \equiv Y^2 \bmod N$ and then hopefully split N via $\gcd(X \pm Y, N)$. The number field sieve is trying to find such numbers by means of number fields.

Let $f \in \mathbb{Z}[t]$ be irreducible such that we have for some $r \in \mathbb{Z}$

$$f(r) \equiv 0 \bmod N$$

i. e. f needs to have a root modulo N. (Finding such polynomials is not easy, one way is to write $N = \sum n_i r^i$ in base r and turn this into a polynomial. Note however that r and n_i won't be small and f won't be monic). So far we have $R := \mathbb{Z}[\zeta] = \mathbb{Z}[t]/f$ and $\varphi : R \to \mathbb{Z}/n\mathbb{Z} : \theta \mapsto r$. Strictly, R is not that well defined (as f is not monic), so maybe think of the number field defined by f and a partial homomorphism. (Alternatively, we can use θ and the minimal polynomial to define an order: $\mathbb{Z} + \sum_{j=2}^{n} \mathbb{Z}(\sum_{i=1}^{j} f_{n-i-1}\theta^i)$ is an order. We will just assume that (unknown) the index to maximal order is coprime to N. If we ever find s.th. not coprime, we have a factorisation)

Assume that we have some $g \in \mathbb{Z}[\theta]$ that is a square. Then $\varphi(g)$ is a square in $\mathbb{Z}/N\mathbb{Z}$ as well and we might be able to use the above idea. Slightly better:

We will be looking at elements $\alpha_i = a_i + b_i\theta$ such that $\prod \alpha_i$ is a square in $\mathbb{Q}[\theta]$ and such that $\prod a_i + rb_i$ is a square in $\mathbb{Z}$.

In NFS, we fix an algebraic factor base B of prime ideals in $\mathbb{Q}[\theta]$, more specific, we only take unramified (easy) degree 1 prime ideals, also know as roots of f modulo p. We also fix a rational factor base C of prime numbers. To find suitable pairs a, b such that $a + b\theta$ is B-smooth, we apply sieving. Starting with the observation that if $a + b\theta \in Q$ for some $Q \in B$, we also have $(a + kp) + (b + lp)\theta \in Q$ for $p = \min \mathbb{N} \cap Q$. This is used systematically to mark pairs (a, b) such that the resulting algebraic number has many prime divisors in B (and similarly in C). To make the method more successful we keep track of the norm of the elements $|N(a+b\theta)| = |b^n N(a/b+\theta)| = |b^n f(a/b)|$: We know that $N(c+\theta)$ is (up to sign) the constant term of the monic characteristic polynomial. However for $g(t) := f(t - c)$ we have $g(\theta + c) = f(\theta + c - c) = f(\theta) = 0$, so g is the characteristic polynomial of $\theta + c$. For the constant term $g(0)$ we have $g(0) = f(-c)$ as claimed. The sieving algorithm keeps track of the norms of the elements and the norms of the prime ideals Q to find elements that hopefully are B-smooth.

The next problem is that, even if we find β such that $\beta \in U_B$ and $v_Q(\beta) \equiv 0 \bmod 2$ for all Q, we don't neccessarily have that β is a square (in $\mathbb{Q}$ the sign might be wrong, here we have problems with general units). To aid here, we check that β is a square modulo a few unrelated prime ideals P.

As a result, we have $\prod a_i + b_i\alpha = \beta^2$ (probably) for some $\beta \in \mathbb{Q}[\theta]$ and $\prod a_i + rb_i = \gamma^2$ for some $\gamma \in \mathbb{Z}$. Next, we need to compute the roots. Here we need the algorithms of the previous section. Typically, we have $> 10^6$ pairs and a huge product that cannot be evaluated directly.