## 16.2. Decomposition of prime numbers

[For almost all primes, we can use the following:]

**Thm 16.2.1** ($\approx$ Lemma 12.1) Let $K$ be a number field of degree $n$, $\alpha \in \mathcal{O}_K$ with minimal polynomial $f(x)$ of degree $n$. ~~If $\mathbb{Z}[\alpha]$ is p-maximal,~~ Assume that $\mathbb{Z}[\alpha]$ is $p$-maximal.

Let $f(x) \equiv g_1(x)^{e_1} \cdots g_t(x)^{e_t} \mod p$ be the factorisation of f mo
(with $g_i(x) \in \mathbb{Z}[X]$ monic)

Then,

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$$

with prime ideals $\mathfrak{p}_i = (p, g_i(\alpha)) = p\mathcal{O}_K + g_i(\alpha)\mathcal{O}_K$,

$$[\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}] = \deg(g_i).$$

**Rmk** Any ideal $\mathfrak{a} \subset \mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n$ ($\approx$ a rank $n$ lattice). It can therefore be specified by giving $n$ basis vectors, each of which can be written as a lin. comb. of a fixed basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_K$

$\rightsquigarrow$ We can represent an ideal by an integer $n \times n$-matrix $M$, which we can put in Hermite normal form (HNF) by changing the basis of $\mathfrak{a}$.

We have $Nm(I) = |\det(M)|$.

Using HNF, we can also find a basis of the $\mathbb{Z}$-module spanned by any number of elements $\beta_1, \ldots, \beta_m$ of $\mathcal{O}_K$.

This allows us to add / multiply ideals.

Fractional ideals work the same but with rational coefficients

Dividing two (fractional) ideals is also not hard ("just linear algebra"). (cf. chapters 4.6-4.8 of Cohen)

__Alg__ to find the decomposition $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$ for arbitrary $p$:

Compute $\mathfrak{a} := J_p(\mathcal{O}_K) = \mathrm{rad}(p\mathcal{O}_K) = \mathfrak{p}_1\cdots\mathfrak{p}_t$.

It then suffices to factor the squarefree ideal $\mathfrak{a} \mid p\mathcal{O}_K$ and determine the exponents by trial division.

To factor a squarefree ideal $\mathfrak{a} \overset{\prod_{i=1}^{t}\mathfrak{p}_i}{=} \mid p\mathcal{O}_K$, we can use Berlekamp's algorithm (problem 2 on sheet 5):

Note that $\mathcal{O}_K/\mathfrak{a} \underset{\text{CRT}}{\cong} \prod_{i=1}^{t} \mathcal{O}_K/\mathfrak{p}_i$,

where $\mathcal{O}_K/\mathfrak{p}_i = \mathbb{F}_{p^{f_i}}$ is a fin. ext. of $\mathbb{F}_p$.

The map $\mathcal{O}_K/\mathfrak{a}^{\cong\prod\mathbb{F}_{p^{f_i}}} \to \mathcal{O}_K/\mathfrak{a}^{\cong\prod\mathbb{F}_{p^{f_i}}}$, $x \mapsto x^p$ is $\mathbb{F}_p$-linear.

Compute $V = \{x \in \mathcal{O}_K/\mathfrak{a} \mid x^p = x\}$ using linear algebra over $\mathbb{F}_p$. We have $V \cong \prod_{i=1}^{t} \mathbb{F}_p$, so in part., $\dim_{\mathbb{F}_p}(V) = t$.

If $t > 1$:

Pick a random $x \in V$ and compute $y := v_p(x) \in V$.
($= x^{(p-1)/2} - 1$ if $p$ is odd)

The projections onto the factors $\mathbb{F}_p$ are independent and each $\underbrace{\text{projection (of } y\text{) is } 0}_{\Updownarrow \; y \mid \mathfrak{p}_i}$ with prob. $\approx \frac{1}{2}$.

We obtain a splitting $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ and recursively factor $\mathfrak{a}_1, \mathfrak{a}_2$.

Rmk This is not the fastest alg. to decompose $p$!

Rmk The factorization of $f(x)$ over $\mathbb{Q}_p$ looks like the decomposition of $p\mathcal{O}_K$ in $K = \mathbb{Q}[X]/(f)$.

## 16.3. Ideal class group

**Def** The Riemann zeta function is given by

$$\zeta(s) = \sum_{n\geq 1} n^{-s} \left( = \prod_p \frac{1}{1-p^{-s}} \right) \quad \text{for } s \in \mathbb{C} \text{ with } \mathrm{Re}(s) > 1.$$

**Def** The Dedekind zeta function of a number field $K$ is given by

$$\zeta_K(s) = \sum_{\substack{0 \neq \mathfrak{a} \subset \mathcal{O}_K \\ \text{ideal}}} \mathrm{Nm}(\mathfrak{a})^{-s} = \prod_{\substack{\mathfrak{p} \subset \mathcal{O}_K \\ \text{prime} \\ \text{ideal}}} \frac{1}{1-\mathrm{Nm}(\mathfrak{p})^{-s}}$$

for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$.

**Ex** $\zeta_{\mathbb{Q}} = \zeta$.

**Thm 16.3.1** (Class number formula)

$$\lim_{s \to 1} (s-1)\zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} R_K |Cl_K|}{w_K \cdot \sqrt{|D_K|}}$$

if $K$ has $r_1$ real embeddings,
$r_2$ pairs of complex embeddings,

regulator $R_K$, class group $Cl_K$, roots of unity $w_K \subset \mathcal{O}_K$ (=torsion subgroup),

"how far apart the units are"

discriminant $D_K$.

**Ex** $\lim_{s \to 1} (s-1)\zeta(s) = 1$

**Proof** $LHS = \lim_{s \to 1} \frac{\zeta_K(s)}{\zeta(s)}$.

**Rmk** $R_K$, $|Cl_K|$ often show up together and can be hard to separate!

~~Rmk (Brauer-Sieg~~

**Thm 16.3.2** (Brauer-Siegel Thm)

For fixed $n = [K:\mathbb{Q}]$, and any $\varepsilon > 0$,

$$|D_K|^{\frac{1}{2}-\varepsilon} \ll R_K |Cl_K| \ll |D_K|^{\frac{1}{2}+\varepsilon}.$$

$$\left( \frac{\log(R_K |Cl_K|)}{\log(\sqrt{|D_K|})} \to 1. \right)$$