# Number theory

Luka Horjak (luka1.horjak@gmail.com)

June 17, 2024

# Contents

# Introduction

These are my lecture notes on the course Number theory in the year 2023/24. The lecturer that year was gost. izr. prof. dr. rer. nat. Daniel Smertnig.

The notes are not perfect. I did not write down most of the examples that help with understanding the course material. I also did not formally prove every theorem and may have labeled some as trivial or only wrote down the main ideas.

I have most likely made some mistakes when writing these notes – feel free to correct them.

# 1 Distribution of prime numbers

*They didn't have internet or Netflix, so it seemed more appealing to compute values of the $\zeta$ function.*
– gost. izr. prof. dr. rer. nat. Daniel Smertnig

February 23, 2024

## 1.1 Riemann zeta function

**Definition 1.1.1.** The *prime counting function* is defined as

$$\pi(x) = \left|\{p \in \mathbb{P} \mid p \leq x\}\right|.$$

**Definition 1.1.2.** Let $(a_n)_n \subseteq \mathbb{C}$ be a sequence. The infinite product

$$\prod_{n=1}^{\infty} a_n$$

converges *absolutely* if it converges normally as a product of constant functions.

**Theorem 1.1.3.** Let $\sigma > 1$ be a real number. For $s \in \mathbb{C}$ with $\operatorname{Re}(s) \geq \sigma$, we have

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1},$$

with both the product and sum converging uniformly and absolutely.[1]

*Proof.* Note that

$$\sum_{n=1}^{\infty} \left|\frac{1}{n^s}\right| = \sum_{n=1}^{\infty} \frac{1}{n^{\operatorname{Re}(s)}} \leq \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}}$$

is convergent, hence the given series converges as well. To prove the convergence of the product, first note that

$$\prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1} = \prod_{p \in \mathbb{P}} \left(\sum_{k=0}^{\infty} p^{-sk}\right).$$

As

$$\sum_{p \in \mathbb{P}} \left|\sum_{k=1}^{\infty} p^{-sk}\right| \leq \sum_{p \in \mathbb{P}} \left(\sum_{k=1}^{\infty} (p^k)^{-\sigma}\right) \leq \sum_{n=1}^{\infty} n^{-\sigma}$$

converges normally, so does the product. To prove equality, we can bound

$$\left|\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{1 - p^{-s}} - \sum_{n=1}^{x} \frac{1}{n^s}\right| \leq \sum_{n=x+1}^{\infty} \left|\frac{1}{n^s}\right| \leq \sum_{n=x+1}^{\infty} \frac{1}{n^{\sigma}},$$

which converges to 0 as $x \to \infty$. ∎

[1] See Complex analysis, section 3 for definition and properties of convergence for products.

**Definition 1.1.4.** The *Riemann zeta function* is defined as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for $\mathrm{Re}(s) > 1$.

**Lemma 1.1.5.** If $\mathrm{Re}(s) > 1$, then $\zeta(s) \neq 0$.

*Proof.* No term in the infinite product is equal to 0. $\square$

**Proposition 1.1.6.** The function $\zeta(s) - \frac{1}{s-1}$ has a holomorphic continuation to $\mathrm{Re}(s) > 0$.

*Proof.* We can write

$$\begin{aligned}
\zeta(s) - \frac{1}{s-1} &= \sum_{n=1}^{\infty} n^{-s} - \int_1^{\infty} x^{-s}\, dx \\
&= \sum_{n=1}^{\infty} \left( n^{-s} - \int_n^{n+1} x^{-s}\, dx \right) \\
&= \sum_{n=1}^{\infty} \int_n^{n+1} \left( n^{-s} - x^{-s} \right) dx
\end{aligned}$$

as long as $\mathrm{Re}(s) > 1$. Now, for $n \le x \le n+1$, we can bound

$$\left| n^{-s} - x^{-s} \right| = \left| \int_n^x s u^{-s-1}\, du \right| \le \frac{|s|}{n^{\mathrm{Re}(s)+1}}.$$

Let $L \subseteq \{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$ be a compact set. As

$$\left| \sum_{n=1}^{\infty} \int_n^{n+1} \left( n^{-s} - x^{-s} \right) dx \right| \le \sum_{n=1}^{\infty} \frac{|s|}{n^{\mathrm{Re}(s)+1}} \le \|\mathrm{id}\|_L \cdot \sum_{n=1}^{\infty} \frac{1}{n^{\sigma+1}}$$

for all $s \in L$, where $\sigma = \min_L |z|$, the series converges uniformly on compact sets. $\square$

**Remark 1.1.6.1.** The $\zeta$ function can be analytically extended to $\mathbb{C} \setminus \{1\}$ by

$$\zeta(1-s) = 2 \cdot (2\pi)^{-s} \cos\left(\frac{\pi}{2} s\right) \Gamma(s) \zeta(s).$$

It has a simple pole with residue 1 at 1.

**Lemma 1.1.7.** The equation $\overline{\zeta(\overline{s})} = \zeta(s)$ holds for all $s \in \mathbb{C} \setminus \{1\}$.

*Proof.* The function $\overline{\zeta(\overline{s})}$ is holomorphic. As it coincides with $\zeta(s)$ for $s \ge 1$, the functions are equal. $\square$

## 1.2 Prime number theorem

**Proposition 1.2.1.** The series
$$\sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s}$$
converges uniformly and absolutely for $\mathrm{Re}(s) \geq \sigma > 1$.

*Proof.* We can bound
$$\sum_{p\in\mathbb{P}} \left|\frac{\log(p)}{p^s}\right| \leq \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^\sigma} \leq \sum_{n=1}^{\infty} \frac{\log(p)}{n^\varepsilon} \cdot \frac{1}{n^{\sigma-\varepsilon}},$$
which clearly converges for $0 < \varepsilon < \sigma - 1$. □

**Definition 1.2.2.** We define functions
$$\theta(x) = \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \log(p)$$
and
$$\phi(s) = \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s}.$$

**Remark 1.2.2.1.** The function $\phi$ is holomorphic for $\mathrm{Re}(s) > 1$.

**Proposition 1.2.3.** The function $\phi$ has a meromorphic continuation to $\mathrm{Re}(s) > \frac{1}{2}$. It has simple poles at points $s = 1$ and zeros of $\zeta(s)$.

*Proof.* Calculate the logarithmic derivative of $\zeta$ as
$$\begin{aligned}
-\frac{\zeta'(s)}{\zeta(s)} &= -\sum_{p\in\mathbb{P}} \frac{\left((1-p^{-s})^{-1}\right)'}{(1-p^{-s})^{-1}} \\
&= -\sum_{p\in\mathbb{P}} \frac{-(1-p^{-s})^{-2}\cdot p^{-s}\log(p)}{(1-p^{-s})^{-1}} \\
&= \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s-1} \\
&= \phi(s) + \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s(p^s-1)}.
\end{aligned}$$
Similarly as in the proof of proposition 1.2.1, we can show that the above series converges locally uniformly and absolutely for $\mathrm{Re}(s) > \frac{1}{2}$. □

**Theorem 1.2.4.** If $\mathrm{Re}(s) = 1$, then $\zeta(s) \neq 0$.

*Proof.* Let $\mu = \mathrm{ord}_{1+ib}\,\zeta \geq 0$. As $\zeta(\overline{z}) = \overline{\zeta(z)}$, we also have $\mu = \mathrm{ord}_{1-ib}\,\zeta$. Now denote $\theta = \mathrm{ord}_{1+2ib}\,\zeta = \mathrm{ord}_{1-2ib}\,\zeta$. As $\phi$ has a simple pole at 1, we have
$$\lim_{\varepsilon\to 0} \varepsilon\phi(1+\varepsilon) = 1.$$

Similarly,

$$\lim_{\varepsilon \to 0} \varepsilon \phi(1+\varepsilon \pm ib) = -\mu,$$

as the logarithmic derivative of $\zeta$ at $b$ has residue $-\mu$, and

$$\lim_{\varepsilon \to 0} \varepsilon \phi(1+\varepsilon \pm 2ib) = -\theta.$$

Now compute

$$f(\varepsilon) = \sum_{r=-2}^{2} \binom{4}{2+r} \phi(1+\varepsilon+rib) = \sum_{p \in \mathbb{P}} \frac{\log(p)}{p^{1+\varepsilon}} \cdot \left(p^{\frac{ib}{2}} - p^{-\frac{ib}{2}}\right)^4 = \sum_{p \in \mathbb{P}} \frac{\log(p)}{p^{1+\varepsilon}} \cdot \left(2 \operatorname{Re}\left(p^{\frac{ib}{2}}\right)\right)^4.$$

It follows that

$$0 \leq \lim_{\varepsilon \to 0} \varepsilon \cdot f(\varepsilon) = 6 - 8\mu - 2\theta.$$

As $\theta \geq 0$, we have $\mu = 0$. □

**Corollary 1.2.4.1.** The function $\phi$ is holomorphic for $\operatorname{Re}(s) = 1$, except for a simple pole with residue 1 at 1. In particular, the function

$$g(z) = \frac{\phi(z+1)}{z+1} - \frac{1}{z}$$

is holomorphic for $\operatorname{Re}(z) \geq 0$.

*Proof.* The proof is obvious and need not be mentioned. □

**Lemma 1.2.5.** Let $x \geq 0$. Then $\theta(x) \leq 4x$.

*Proof.* First let $n \in \mathbb{N}$ be an integer. Then

$$e^{\theta(2n)-\theta(n)} = \prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq 2^{2n},$$

therefore $\theta(2n) - \theta(n) \leq 2n\log(2)$. Now let $n = \left\lceil \frac{x}{2} \right\rceil$. Then

$$\theta(x) - \theta\left(\frac{x}{2}\right) \leq \theta(2n) - \theta(n-1) \leq \log(n) + 2n\log(2) \leq 3n \leq 2x$$

for all $x \geq 6$, but we can manually check that it holds for $x < 6$ as well. But then

$$\theta(x) = \sum_{n=0}^{\infty} \left(\theta\left(\frac{x}{2^n}\right) - \theta\left(\frac{x}{2^{n+1}}\right)\right) \leq \sum_{n=0}^{\infty} \frac{2x}{2^n} = 4x.$$ □

**Lemma 1.2.6.** Let $h \colon \mathbb{R}_{\geq 0} \to \mathbb{C}$ be bounded and locally integrable. Then the following statements are true:

i) The Laplace transform

$$H(z) = \int_0^\infty h(t)e^{-zt}\, dt$$

of $h$ is holomorphic for $\operatorname{Re}(z) > 0$.

March 1, 2024

ii) The function
$$\int_0^T h(t)e^{-zt}\,dt$$
is holomorphic for all $z \in \mathbb{C}$.

*Proof.*

i) Analysis 2b, proposition 4.1.4.

ii) Evident. □

**Theorem 1.2.7.** Let $h\colon \mathbb{R}_{\geq 0} \to \mathbb{C}$ be bounded and locally integrable. Suppose that its Laplace transform
$$H(z) = \int_0^\infty h(t)e^{-zt}\,dt$$
extends to a holomorphic function on $\operatorname{Re}(z) \geq 0$. Then
$$H(0) = \int_0^\infty h(t)\,dt.$$

*Proof.* Define
$$H_T(z) = \int_0^T h(t)e^{-zt}\,dt$$
for $T > 0$. Fix some $R > 0$ and consider the region
$$\Omega = \{z \in \mathbb{\Delta}(R) \mid \operatorname{Re}(z) \geq -\delta\}.$$
By compactness of $i[-R, R]$, we can pick a $\delta$ such that $H$ is holomorphic on $\Omega$. Now partition $\partial\Omega$ into sets $C_1 = \{z \in \partial\Omega \mid \operatorname{Re}(z) \geq 0\}$, $C_2 = \{z \in \partial\Omega \mid -\delta < \operatorname{Re}(z) < 0\}$ and $C_3 = \{z \in \partial\Omega \mid \operatorname{Re}(z) = -\delta\}$. Taking
$$I(z) = \frac{H(z) - H_T(z)}{z} e^{zT}\left(1 + \frac{z^2}{R^2}\right),$$
we can write
$$H(0) - H_T(0) = \frac{1}{2\pi i}\oint\limits_{\partial\Omega} I(z)\,dz$$
using the Cauchy integral formula. Setting $B = \max\{|h(t)| \mid t \in \mathbb{R}_{\geq 0}\}$, we can bound
$$|H(z) - H_T(z)| \leq \int_T^\infty |h(t)| \cdot \left|e^{-zt}\right|\,dt \leq B\frac{e^{-\operatorname{Re}(z)T}}{\operatorname{Re}(z)},$$
hence
$$|I(z)| \leq \frac{B}{\operatorname{Re}(z)} \cdot \left|1 + \frac{z^2}{R^2}\right| \cdot \left|\frac{1}{z}\right| = \frac{B}{R\operatorname{Re}(z)} \cdot \left|\frac{z}{R} + \frac{R}{z}\right| = \frac{B}{R\operatorname{Re}(z)} \cdot 2\operatorname{Re}\left(\frac{z}{R}\right) = \frac{2B}{R^2}$$
for $z \in C_1$. Integrating, we find that
$$\frac{1}{2\pi} \cdot \int\limits_{C_1} |I(z)|\,dz \leq \frac{B}{R}.$$

Next, we bound the integral of $H_T$ over $C_2 \cup C_3$. As $H_T$ is holomorphic, we can write

$$\int_{C_2 \cup C_3} H_T(z)\, dz = \int_{-C_1} H_T(z)\, dz,$$

but as

$$|H_T(z)| \le \int_0^T \left| h(z) e^{-zt} \right| dt \le B \int_0^T e^{-\operatorname{Re}(z)t}\, dt = \frac{B}{\operatorname{Re}(z)} \cdot \left(1 - e^{-\operatorname{Re}(z)T}\right) \le B \frac{e^{-\operatorname{Re}(z)T}}{|\operatorname{Re}(z)|},$$

which is the same bound as above. As

$$\left| H(z) \cdot \left(1 + \frac{z^2}{R^2}\right) \cdot \frac{1}{z} \right| \le M$$

on $C_2 \cup C_3$ for some $M > 0$, we see that

$$\left| H(z) \cdot \left(1 + \frac{z^2}{R^2}\right) \cdot \frac{1}{z} \right| \cdot \left| e^{zT} \right|$$

converges to 0 as $T \to \infty$. By the dominated convergence theorem, the integral

$$\frac{1}{2\pi} \cdot \int_{C_2 \cup C_3} \left| H(z) \left(1 + \frac{z^2}{R^2}\right) \cdot \frac{1}{z} \right| \cdot \left| e^{zT} \right| dz$$

converges to 0 as well. Then

$$\limsup_{T \to \infty} |H(0) - H_T(0)| \le \frac{2B}{R},$$

which, by taking $R \to \infty$, implies

$$\lim_{T \to \infty} H_T(0) = H(0). \qquad \square$$

**Lemma 1.2.8.** For $\operatorname{Re}(z) > 0$, we have

$$g(z) = \int_0^\infty \left( \theta\left(e^t\right) e^{-t} - 1 \right) e^{-zt}\, dt,$$

where $g$ is defined as in corollary 1.2.4.1.

*Proof.* Note that $\theta\left(e^t\right) e^{-t} - 1$ is bounded, hence the given Laplace transform exists. Let $(p_n)_n$ be the ascending sequence of prime numbers. Setting $p_0 = 1$, we have

$$\phi(s) = \sum_{p \in \mathbb{P}} \frac{\log(p)}{p^s} = \sum_{j=1}^\infty \frac{\theta(p_j) - \theta(p_{j-1})}{p_j^s} = \sum_{j=0}^\infty \theta(p_j) \cdot \left( \frac{1}{p_j^s} - \frac{1}{p_{j+1}^s} \right).$$

Using the definite integral of $\frac{1}{x^{s+1}}$, we can rewrite

$$\phi(s) = \sum_{j=0}^\infty \theta(p_j) s \int_{p_j}^{p_{j+1}} \frac{1}{x^{s+1}}\, dx = \sum_{j=0}^\infty s \int_{p_j}^{p_{j+1}} \frac{\theta(x)}{x^{s+1}}\, dx = s \int_1^\infty \frac{\theta(x)}{x^{s+1}}\, dx = s \int_0^\infty \theta(e^t) e^{-st}\, dt$$

for all $\operatorname{Re}(s) > 1$. Hence

$$g(z) = \int_0^\infty \theta(e^t) e^{-(z+1)t}\, dt - \int_0^\infty e^{-zt}\, dt = \int_0^\infty \left( \theta\left(e^t\right) e^{-t} - 1 \right) e^{-zt}\, dt. \qquad \square$$

**Theorem 1.2.9.** The integral

$$\int_1^\infty \frac{\theta(x)-x}{x^2}\,dx$$

converges.

*Proof.* Using the substitution $x=e^t$, we find that

$$\int_1^{e^T} \frac{\theta(x)-x}{x^2}\,dx = \int_0^T \left(\theta\left(e^t\right)e^{-t}-1\right)\,dt.$$

Applying theorem 1.2.7, the claim follows. □

**Theorem 1.2.10.** We have $\theta(x)\sim x$, that is

$$\lim_{x\to\infty}\frac{\theta(x)}{x}=1.$$

*Proof.* Suppose otherwise. We split two cases:

i) For some $\lambda>1$, there exist arbitrarily large $x$ such that $\theta(x)\geq\lambda x$. We can compute

$$\int_x^{\lambda x}\frac{\theta(t)-t}{t^2}\,dt \geq \int_x^{\lambda x}\frac{\lambda x - t}{t^2}\,dt = \int_1^\lambda \frac{\lambda x - xy}{x^2y^2}x\,dy = \int_1^\lambda \frac{\lambda - y}{y^2}\,dy = c > 0.$$

This contradicts the previous theorem.

ii) For some $\lambda<1$, there exist arbitrarily large $x$ such that $\theta(x)\leq\lambda x$. As above, we can compute

$$\int_{\lambda x}^{x}\frac{\theta(t)-t}{t^2}\,dt \leq \int_{\lambda x}^{x}\frac{\lambda x - t}{t^2}\,dt = \int_\lambda^1 \frac{\lambda - y}{y^2}\,dy = c < 0.$$

This again contradicts the previous theorem. □

**Theorem 1.2.11** (Prime number theorem)**.** The prime counting function is asymptotically equivalent to $\frac{x}{\log(x)}$.

*Proof.* Note that

$$\theta(x)\leq\log(x)\cdot\pi(x)$$

and

$$\theta(x)\geq\sum_{\substack{p\in\mathbb{P}\\ x^{1-\varepsilon}\leq p\leq x}}\log(p)\geq(1-\varepsilon)\log(x)\cdot\left(\pi(x)-x^{1-\varepsilon}\right),$$

therefore

$$\frac{\theta(x)}{x}\leq\frac{\pi(x)\log(x)}{x}\leq\frac{\theta(x)}{(1-\varepsilon)x}+\frac{\log(x)}{x^\varepsilon}.$$

This implies

$$1\leq\limsup_{x\to\infty}\frac{\pi(x)\log(x)}{x}\leq\frac{1}{1-\varepsilon}$$

and

$$1\leq\liminf_{x\to\infty}\frac{\pi(x)\log(x)}{x}\leq\frac{1}{1-\varepsilon}.$$ □

# 2 Algebraic integers

*This is usually attributed to Fermat, but it's not quite correct.*
– gost. izr. prof. dr. rer. nat. Daniel Smertnig

March 8, 2024

## 2.1 Gaussian integers

**Definition 2.1.1.** A domain $R$ is *Euclidean* if there is a function $\delta\colon R \setminus \{0\} \to \mathbb{N}_0$, such that for all $a \in R$ and $b \in R \setminus \{0\}$ we can write $a = bq + r$ for $q, r \in R$, such that $r = 0$ or $\delta(r) < \delta(b)$.

**Proposition 2.1.2.** The Gaussian integers are an Euclidean domain.

*Proof.* Algebra 2, theorem 6.3.4. □

**Definition 2.1.3.** A domain $R$ is a *unique factorisation domain* if every $\alpha \in R$ is of the form

$$\alpha = \prod_{i=1}^{n} p_i$$

for irreducible elements in a unique way up to permutation and multiplication of factors by a unit element.

**Remark 2.1.3.1.** Principal ideal domains (and therefore $\mathbb{Z}[i]$) are unique factorisation domains.

**Lemma 2.1.4.** The function $N\colon \mathbb{Z}[i] \to \mathbb{N}_0$, given by $N(a+bi) = a^2+b^2$, has the following properties:

i) The equality $N(\alpha) = 0$ is equivalent to $\alpha = 0$.

ii) For all $\alpha, \beta \in \mathbb{Z}[i]$ we have $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$.

iii) An element $\alpha \in \mathbb{Z}[i]$ is invertible if and only if $N(\alpha) = 1$.

*Proof.* The proof is obvious and need not be mentioned. □

**Lemma 2.1.5.** Let $p \in \mathbb{P}$ be a prime. Then $-1$ is a quadratic residue modulo $p$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

*Proof.* If $p \equiv 1 \pmod 4$, we can write $-1 \equiv \left(e^{\frac{p-1}{4}}\right)^2 \pmod p$, where $e$ is a primitive root modulo $p$. If $p \equiv 3 \pmod 4$ and $p \mid c^2 + 1$, then

$$1 \equiv \left(c^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} = -1,$$

a clear contradiction. □

**Theorem 2.1.6** (Fermat)**.** Let $p$ be an odd prime. Then $p$ can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$.

*Proof.* It is clear that primes $p \equiv 3 \pmod 4$ cannot be written in such a way. Now suppose that $p \equiv 1 \pmod 4$ and take $b \in \mathbb{N}$ such that $b^2 \equiv -1 \pmod p$. Now note that $p \mid (b-i)(b+i)$, but $p$ clearly can't divide either factor. It follows that $p$ is not a prime element, hence we can factor it as $p = \alpha\beta$.

Now, note that $p^2 = N(p) = N(\alpha) \cdot N(\beta)$, but as $\alpha$ and $\beta$ are not invertible, we have $N(\alpha) = p$, which gives us a representation of $p$ as a sum of two squares. $\square$

**Proposition 2.1.7.** Up to associativity, the prime elements of $\mathbb{Z}[i]$ are the following:

i) $1+i$,

ii) $a+bi$, where $a^2+b^2 = p \in \mathbb{P}$ with $p \equiv 1 \pmod 4$ and $0 < |b| < a$,

iii) $p \in \mathbb{P}$ with $p \equiv 3 \pmod 4$.

*Proof.* It is clear that $1+i$ is a prime element. Elements of the second form are prime since their norm is a prime number. For the last one, if $p = \alpha\beta$ for non-invertible $\alpha$ and $\beta$, then $N(\alpha) = N(\beta) = p$, which is of course impossible. Clearly, they are not associated.

Suppose now that $p \in \mathbb{Z}[i]$ is a prime element. Then $N(p) = p\overline{p}$, which can be factored in integers. But then $p$ divides some prime number $q \in \mathbb{P}$. It follows that $N(p) \mid q^2$, but as $q^2$ can be factored by the above prime elements, $p$ is of such form. $\square$

**Theorem 2.1.8.** Let $n \in \mathbb{N}$. Then there exist integers $a$ and $b$ such that $n = a^2 + b^2$ if and only if $2 \mid \nu_p(n)$ for all prime numbers $p \equiv 3 \pmod 4$.

*Proof.* It is clear that all such numbers can be written as a sum of two squares, as the property is multiplicative.[2] For the converse, suppose that $n = a^2+b^2$ and take any prime number $p \in \mathbb{P}$ such that $p \equiv 3 \pmod 4$ and $p \mid n$. Then, if $b$ is invertible in $\mathbb{Z}_p$, we can write

$$p \,\Bigg|\, \left(\frac{a}{b}\right)^2 + 1\,,$$

which is impossible. It follows that $p \mid a, b$. The theorem is now proven by infinite descent. $\square$

**Remark 2.1.8.1.** This theorem can also be proven by factoring $\alpha = a + bi$.

**Remark 2.1.8.2.** A positive integer $n$ can be written as a sum of 3 squares if and only if it is not of the form $n = 4^a \cdot (8k+7)$.

**Proposition 2.1.9.** Let $\alpha \in \mathbb{Q}(i)$. Then $\alpha \in \mathbb{Z}[i]$ if and only if there exist some $c, d \in \mathbb{Z}$ such that $\alpha$ is a root of the polynomial $P(x) = x^2 + cx + d$.

*Proof.* We see that $P(\alpha) = 0$ and $\alpha \notin \mathbb{Q}$ is equivalent to $P(x) = (x-\alpha)(x-\overline{\alpha})$. Of course, if $\alpha \in \mathbb{Q}$, we must have $\alpha \in \mathbb{Z}$ by the properties of rational roots of integer polynomials. Otherwise, for $\alpha = a+bi$, the condition is equivalent to $2a \in \mathbb{Z}$ and $a^2+b^2 \in \mathbb{Z}$, which is only possible if both $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$. $\square$

[2] $(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$.

## 2.2 Number fields and their rings of integers



**Definition 2.2.1.** A *number field* is a subfield of $\mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$. Elements of $K$ are called *algebraic numbers*.

**Definition 2.2.2.** A field extension $K/\mathbb{Q}$ is *algebraic* if every element $\alpha \in K$ is a root of a polynomial $f \in \mathbb{Q}[x]$. We denote the minimal polynomial of $\alpha$ by $m_\alpha$. Furthermore, set $\deg(\alpha) = \deg(m_\alpha)$.

**Theorem 2.2.3** (Primitive element theorem)**.** Let $K$ be a number field. Then there exists some element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.[3]

*Proof.* Algebra 3, theorem 1.1.7. □

**Proposition 2.2.4.** Let $K$ be a number field. Then $K/\mathbb{Q}$ is a separable extension.

*Proof.* Suppose otherwise. Then $\gcd(m_\alpha, m_\alpha')$ is a polynomial of lower degree with $\alpha$ as a root. □

**Remark 2.2.4.1.** The roots of $m_\alpha$ are called the *algebraic conjugates* of $\alpha$.

**Corollary 2.2.4.2.** There are exactly $\deg(\alpha)$ embeddings $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$.

**Definition 2.2.5.** A complex number $\alpha$ is an *algebraic integer* if there exists a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

**Lemma 2.2.6.** Let $f \in \mathbb{Z}[x]$ be monic and suppose that $f = gh$ for monic polynomials $g, h \in \mathbb{Q}[x]$. Then $g, h \in \mathbb{Z}[x]$.

*Proof.* Let $d, e \in \mathbb{N}$ be minimal integers such that $dg, eh \in \mathbb{Z}[x]$. Note that the coefficients of $dg$ (and similarly $eh$) are coprime. Suppose that $p \mid de$ for some $p \in \mathbb{P}$. It follows that $p \mid def = dgeh$. In particular, the ring $\mathbb{Z}[x]/p\mathbb{Z}[x]$ has a zero divisor, which is impossible, as $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong Z_p[x]$ is an integral domain. □

**Lemma 2.2.7.** A complex number $\alpha$ is an algebraic integer if and only if $m_\alpha$ has integer coefficients.

*Proof.* The proof is obvious and need not be mentioned. □

**Proposition 2.2.8.** Let $K$ be a number field and $\alpha \in K$. Then the following statements are equivalent:

i) The number $\alpha$ is an algebraic integer.

ii) The group $(\mathbb{Z}[\alpha], +)$ is finitely generated.

iii) There exists a subring $R \subseteq K$ such that $\alpha \in R$ and the group $(R, +)$ is finitely generated.

iv) There exists a finitely generated subgroup $(A, +) \subseteq (K, +)$ such that $A \neq 0$ and $\alpha A \subseteq A$.

[3] In other words, $K/\mathbb{Q}$ is simple.

*Proof.* Note that we only need to prove that the last statement implies the first one. Write $A = \langle \beta_i \mid i \leq n \rangle$. We can therefore write

$$\alpha\beta = C\beta,$$

where

$$\beta = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$$

and $C$ is some matrix with integer coefficients. In particular, $\alpha$ is an eigenvalue of $C$, which means it is a root of $\det(C - I\alpha)$, which is a polynomial with integer coefficients. $\square$

**Corollary 2.2.8.1.** Let $K$ be a number field. Then

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ is an algebraic integer}\}$$

is a subring of $K$.

*Proof.* Suppose that $\alpha, \beta \in \mathcal{O}_K$, that is, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated. Then $\mathbb{Z}[\alpha, \beta]$ is finitely generated as well. As both $\alpha + \beta$ and $\alpha \cdot \beta$ are elements of this subring, both are elements of $\mathcal{O}_K$. $\square$

**Definition 2.2.9.** With the notation of the above corollary, we call $\mathcal{O}_K$ the *ring of integers* in $K$.

**Proposition 2.2.10.** Let $K = \mathbb{Q}\left(\sqrt{d}\right)$, where $d \in \mathbb{Z}$ is a square-free integer.

i) If $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{d}\right]$.

ii) If $d \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

*Proof.* Let $\alpha = \frac{a+b\sqrt{d}}{2}$ for $a, b \in \mathbb{Q}$. Clearly, $\mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$. Suppose therefore that $b \neq 0$ and set $\alpha' = \frac{a-b\sqrt{d}}{2}$ and note that

$$m_\alpha = (x - \alpha) \cdot (x + \alpha) = x^2 - ax + \frac{a^2 - db^2}{4}.$$

It follows that $\alpha \in \mathcal{O}_K$ if and only if $a \in \mathbb{Z}$ and $a^2 - db^2 \in 4\mathbb{Z}$. in particular, $db^2 \in \mathbb{Z}$ and hence $b \in \mathbb{Z}$, as $d$ is square-free.

i) Considering $a^2 - db^2 \bmod 4$, we see that both $a$ and $b$ must be even, which gives $\alpha \in \mathbb{Z}\left[\sqrt{d}\right]$.

ii) The same equation modulo 4 now gives us $a \equiv b \pmod 2$. A direct calculation now shows that $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. $\square$

**Remark 2.2.10.1.** All quadratic number fields are of this form.

**Definition 2.2.11.** Let $\omega_n$ be a primitive $n$-th root of unity. The $n$-th *cyclotomic field* is the field $\mathbb{Q}(\omega_n)$. We denote by $\mu_n(\mathbb{C})$ the $n$-th roots of unity and by $\mu_n^*(\mathbb{C})$ the primitive ones.

**Remark 2.2.11.1.** For odd $n$, we have $\mathbb{Q}(\omega_n) = \mathbb{Q}(\omega_{2n})$.

**Proposition 2.2.12.** Let $\omega \in \mu_n^*(\mathbb{C})$. If $k \in \mathbb{N}$ is coprime with $n$, then $\omega$ and $\omega^k$ are algebraic conjugates.

*Proof.* As algebraic conjugation is an equivalence relation, it suffices to prove the proposition for $k = p \in \mathbb{P}$. Let $f = x^n - 1$ and write $f = gm_\omega$. Suppose that $g(\omega^p) = 0$. Then $\omega$ is a root of $g(x^p)$, therefore it is divisible by $m_\omega$ in $\mathbb{Z}[x]$. Let $\overline{g}$ be the projection of $g$ in $\mathbb{Z}[x]\big/p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$. As $\overline{g}(x^p) = \overline{g}(x)^p$, we find that $\overline{m}_\alpha \mid \overline{g}(x)^p$. In particular, $\overline{m}_\alpha$ and $\overline{g}$ share a common factor $\overline{h} \in \mathbb{Z}_p[x]$. But then $\overline{f} = \overline{g} \cdot \overline{m}_\alpha$ is divisible by $\overline{h}^2$, therefore $\overline{f}$ and $\overline{f}'$ share a common factor. As $p \nmid n$, $\overline{f}' = n \cdot X^{n-1} \neq 0$, which is clearly coprime to $\overline{f}$. $\square$

**Definition 2.2.13.** The $n$-th *cyclotomic polynomial* is the polynomial

$$\Phi_n = \prod_{\omega \in \mu_n^*(\mathbb{C})} (x - \omega).$$

**Remark 2.2.13.1.** The polynomial $\Phi_n$ is irreducible by the previous proposition. We have $\deg \Phi_n = \varphi(n)$.

**Proposition 2.2.14.** Let $\omega \in \mu_n^*(\mathbb{C})$. Then $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. Furthermore, the map $(\mathbb{Z}/n\mathbb{Z})^\times \to \operatorname{Gal}\left(\mathbb{Q}(\omega)\big/\mathbb{Q}\right)$ given by $i \mapsto (\omega \mapsto \omega^i)$ is an isomorphism. In particular, $\mathbb{Q}(\omega)\big/\mathbb{Q}$ is Galois.

*Proof.* Note that $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$. The described map is obviously a bijective homomorphism. $\square$

**Corollary 2.2.14.1.** Let $\omega \in \mu_n^*(\mathbb{C})$ Then the roots of unity in $\mathbb{Q}(\omega)$ are precisely $\mu_n(\mathbb{C})$ is $n$ is even and $\mu_{2n}(\mathbb{C})$ if $n$ is odd.

*Proof.* It is enough to consider even $n$. Suppose that $\lambda \in \mathbb{Q}(\omega)$ is a primitive $k$-th root of unity for $k \nmid n$. We can assume that $\gcd(k, n) = 1$ by replacing $\lambda$ with $\lambda^{\gcd(k,n)}$. We now claim that $\lambda\omega$ is a primitive $kn$-th root of unity. Indeed, if $(\lambda\omega)^m = 1$, then $\omega^{km} = 1$ and $\lambda^{nm} = 1$, hence $n \mid km$ and $k \mid nm$. As $k$ and $n$ were chosen to be coprime, we find that $nk \mid m$. It follows that $\mathbb{Q} \subseteq \mathbb{Q}(\omega_{kn}) \subseteq \mathbb{Q}(\omega)$, which is impossible by considering the degrees over $\mathbb{Q}$, as $\varphi(kn) \mid \varphi(n)$ implies $k \in \{1, 2\}$. $\square$

**Corollary 2.2.14.2.** There is a bijection between $2\mathbb{N}$ and cyclotomic fields, given by $m \mapsto \mathbb{Q}\left(e^{\frac{2\pi i}{m}}\right)$.

## 2.3 Trace, norm and discriminant

**Definition 2.3.1.** Let $\mathbb{Q} \subseteq K \subseteq L$ be number fields. We define

$$\operatorname{Hom}_K(L, \mathbb{C}) = \left\{\sigma \colon L \to \mathbb{C} \mid \sigma|_K = \mathrm{id}\right\}.$$

**Remark 2.3.1.1.** Every $\varphi \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ has precisely $[L : K]$ distinct extensions in $\operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C})$.

**Definition 2.3.2.** Let $K \subseteq L$ be number fields, $\operatorname{Hom}_K(L, \mathbb{C}) = \{\sigma_i \mid i \leq n\}$ and $\alpha \in L$. The *relative trace* and *relative norm* of $\alpha$ are defined as

$$T_K^L(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) \quad \text{and} \quad N_K^L(\alpha) = \prod_{i=1}^n \sigma_i(\alpha).$$

If $K = \mathbb{Q}$, we omit the subscript.

**Proposition 2.3.3.** The trace is a linear map and the norm is multiplicative.

*Proof.* The proof is obvious and need not be mentioned. □

**Proposition 2.3.4.** Let $K \subseteq L$ be a number field with $[L : K] = n$. Let $\alpha \in L$ and set

$$f = x^d + \sum_{k=0}^{d-1} a_k x^k$$

to be the minimal polynomial of $\alpha$. Then $T(\alpha) = -\frac{n}{d} a_{d-1}$ and $N(\alpha) = (-1)^n a_0^{\frac{n}{d}}$. In particular, $N(\alpha), T(\alpha) \in K$.

*Proof.* Let $K' = K(\alpha) \subseteq L$. Then $[K' : K] = d$ and $n = d \cdot [L : K']$. We can factor $f$ as

$$f = \prod_{\sigma \in \operatorname{Hom}_K(K', \mathbb{C})} (x - \sigma(a)).$$

As each $\sigma \in \operatorname{Hom}_K(K', \mathbb{C})$ extends to exactly $\frac{n}{d}$ elements of $\operatorname{Hom}_K(L, \mathbb{C})$, the proposition follows from Vieta's formulae. □

**Remark 2.3.4.1.** If $\alpha \in \mathcal{O}_L$, then $N(\alpha), T(\alpha) \in \mathcal{O}_K$.

**Lemma 2.3.5.** Let $K \subseteq L \subseteq M$ be number fields. Then

$$N_K^M = N_K^L \circ N_L^M \quad \text{and} \quad T_K^M = T_K^L \circ T_L^M.$$

*Proof.* Take an element $\alpha \in M$. We now define an equivalence relation on $\operatorname{Hom}_K(M, \mathbb{C})$ as $\sigma \sim \sigma' \iff \sigma|_L = \sigma'|_L$. Note that there are precisely $m = [L : K]$ equivalence classes. Let $\sigma_i \in \operatorname{Hom}_K(M, \mathbb{C})$ be the representatives of the equivalence classes. Now denote $G_i = \operatorname{Hom}_{\sigma_i(L)}(\sigma_i(M), \mathbb{C})$ and compute

$$T_K^M(\alpha) = \sum_{i=1}^m \left(\sum_{\sigma \sim \sigma_i} \sigma(\alpha)\right) = \sum_{i=1}^m \left(\sum_{\sigma \in G_i} \sigma(\sigma_i(\alpha))\right) = \sum_{i=1}^m T_{\sigma_i(L)}^{\sigma_i(M)}\left(\sigma_i(\alpha)\right).$$

March 22, 2024

Now note that $\sigma_i\left(T_L^M(\alpha)\right) = T_{\sigma_i(L)}^{\sigma_i(M)}\left(\sigma_i(\alpha)\right)$, hence

$$T_K^M(\alpha) = \sum_{i=1}^m \sigma_i\left(T_L^M(\alpha)\right) = T_K^L \circ T_L^M(\alpha).$$

The proof for the norm is analogous. □

**Remark 2.3.5.1.** For $K \subseteq L$ and $\alpha \in L$, the map $\varphi_a \colon L \to L$ given by $x \mapsto \alpha x$ is $K$-linear. The norm and trace of $\alpha$ coincide with the determinant and trace of this map.

**Lemma 2.3.6.** Let $\alpha \in \mathcal{O}_K$. Then $\alpha$ is invertible if and only if $N_{\mathbb{Q}}^K(\alpha) = \pm 1$.

*Proof.* If $\alpha$ is invertible, then clearly $N_{\mathbb{Q}}^K(\alpha) = \pm 1$, as the norm is multiplicative. Now suppose that $N_{\mathbb{Q}}^K(\alpha) = \pm 1$ and let $d = \deg m_\alpha$ be the degree of the minimal polynomial

$$m_\alpha = x^d + \sum_{k=0}^{d-1} a_k x^k$$

of $\alpha$. By our assumption, $a_0 = \pm 1$, therefore

$$1 = \pm\alpha \cdot \sum_{k=1}^{d} a_k x^{k-1}.$$ □

**Remark 2.3.6.1.** If $N_{\mathbb{Q}}^K(\alpha) \in \mathbb{P}$, then $\alpha$ is irreducible.

**Definition 2.3.7.** Let $K$ be a number field. Suppose that $[K : \mathbb{Q}] = n$ and denote $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_i \mid i \leq n\}$. The *discriminant* of $(\alpha_1, \dots, \alpha_n)$ is defined as

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det\left[\sigma_i(\alpha_j)\right]_{i,j \leq n}^2.$$

**Proposition 2.3.8.** The following statements hold:

i) For any $\alpha_i \in K$ we have $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det\left[T_{\mathbb{Q}}^K(\alpha_i\alpha_j)\right]_{i,j}$.

ii) For any $\alpha_i \in K$ we have $\operatorname{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$. If $\alpha_i \in \mathcal{O}_K$, then the discriminant is an integer.

iii) If $\beta = A\alpha$ for some matrix $A \in M_n(\mathbb{Q})$, then

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

*Proof.*

i) Let $C = \left[\sigma_i(\alpha_j)\right]_{i,j}$. Then

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(C)^2 = \det(C^\top C).$$

Now note that

$$(C^\top C)_{i,j} = \sum_{k=1}^n \sigma_k(\alpha_i)\sigma_k(\alpha_j) = T_{\mathbb{Q}}^K(\alpha_i\alpha_j).$$

ii) Follows from the previous statement.

iii) Let $A = \left[a_{i,j}\right]_{i,j}$. Then

$$\sigma_i(\beta_j) = \sum_{k=1}^{n} a_{j,k}\sigma_i(a_k),$$

hence

$$\left[\sigma_i(\beta_j)\right]_{i,j} = \left[\sigma_i(\alpha_j)\right]_{i,j} \cdot A^\top. \qquad \square$$

**Proposition 2.3.9.** Let $K = \mathbb{Q}(\alpha)$ and $n = [K : \mathbb{Q}]$. Denote by $\alpha_1, \ldots, \alpha_n$ the algebraic conjugates of $\alpha$. Then

$$\operatorname{disc}\left(1, \alpha, \ldots, \alpha^{n-1}\right) = \prod_{i \neq j}(\alpha_j - \alpha_i)^2 = (-1)^{\frac{n(n-1)}{2}} \cdot N_{\mathbb{Q}}^{K}(f'(\alpha)),$$

where $f$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$.

*Proof.* Order $\alpha_i$ such that $\alpha = \alpha_1$ and $\sigma_i(\alpha) = \alpha_i$. The first equality is now clear from the Vandermonde determinant. Now note that

$$f' = \sum_{i=1}^{n} \prod_{j \neq i}(x - \alpha_j),$$

therefore

$$f'(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j).$$

A straightforward calculation now shows that

$$N_{\mathbb{Q}}^{K}(f'(\alpha)) = \prod_{i=1}^{n} \sigma_i(f'(\alpha)) = \prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n} \prod_{j \neq i}(\alpha_i - \alpha_j) = (-1)^{\frac{n(n-1)}{2}} \cdot \prod_{i \neq j}(\alpha_j - \alpha_i)^2. \qquad \square$$

**Theorem 2.3.10.** Let $K$ be a number field with $n = [K : \mathbb{Q}]$. Elements $\alpha_1, \ldots, \alpha_n \in K$ form a $\mathbb{Q}$-basis of $K$ if and only if

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \neq 0.$$

*Proof.* Let $K = \mathbb{Q}(\beta)$. Then $(1, \beta, \ldots, \beta^{n-1})$ form a basis of $K$, so we can write $\alpha = A\beta$ for some matrix $A \in M_n(\mathbb{Q})$. As we have

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

and $\operatorname{disc}(\beta_1, \ldots, \beta_n) \neq 0$, the conclusion follows. $\square$

## 2.4 Integral bases

**Proposition 2.4.1.** Let $K$ be a number field. Then

$$K = \left\{ \frac{\alpha}{d} \;\middle|\; d \in \mathbb{N} \land \alpha \in \mathcal{O}_K \right\}.$$

*Proof.* Take $\beta \in K$ and let

$$f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$$

be a polynomial with $f(\beta) = 0$. Then, multiplying by $a_n^{n-1}$, we find a monic polynomial with $a_n\beta$ as a root, hence $a_n\beta \in \mathcal{O}_K$. $\square$

**Definition 2.4.2.** Let $K$ be a number field. An *integral basis* of $\mathcal{O}_K$ is a $\mathbb{Z}$-module basis of $\mathcal{O}_K$.

**Theorem 2.4.3** (Structure)**.**

i) If $M$ is a finitely generated $\mathbb{Z}$-module, then $M = F \oplus T$ where $F$ is a finitely generated free $\mathbb{Z}$-module and $T$ is finite.

ii) Let $F$ be a finitely generated free $\mathbb{Z}$-module of rank $n$. If $G \subseteq F$ is a submodule, then $G$ is also finitely generated and free as a $\mathbb{Z}$-module with rank at most $n$. Furthermore, there exists a basis $(b_1, \dots, b_n)$ of $F$ and $d_1, \dots, d_m \in \mathbb{N}$ with $d_i \mid d_{i+1}$ such that $(d_1b_1, \dots, d_mb_m)$ is a basis of $G$.

iii) Let $T$ be a finite abelian group. Then

$$T = \bigoplus_{i=1}^{r} \mathbb{Z}_{n_i}.$$

Furthermore, we can choose $n_i$ such that $n_i \mid n_{i+1}$ – such choice of $n_i$ is unique.

**Lemma 2.4.4.** Suppose that $(\alpha_1, \dots, \alpha_n)$ is a $\mathbb{Q}$-basis of $K$, contained in $\mathcal{O}_K$, and denote $d = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$. Then

$$\mathcal{O}_K \subseteq \frac{1}{d} \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i.$$

*Proof.* Let $\beta \in \mathcal{O}_K$ and write

$$\beta = \sum_{i=1}^{n} x_i \alpha_i.$$

Now compute

$$T_{\mathbb{Q}}^K(\alpha_i\beta) = T_{\mathbb{Q}}^K\left(\sum_{j=1}^{n} x_j\alpha_i\alpha_j\right) = \sum_{j=1}^{n} x_j T_{\mathbb{Q}}^K(\alpha_i\alpha_j),$$

hence

$$b = \begin{bmatrix} T(\alpha_1\beta) \\ \vdots \\ T(\alpha_n\beta) \end{bmatrix} = \underbrace{\Big[T_{\mathbb{Q}}^K(\alpha_i\alpha_j)\Big]_{i,j}}_{C} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

As $\det C = d \neq 0$, we can write $x = C^{-1}b$. As $\det C \cdot C^{-1} \in M_n(\mathbb{Z})$, the conclusion follows. $\square$

**Theorem 2.4.5.** The set $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$. If $I \triangleleft \mathcal{O}_K$ is a non-zero ideal, then $I$ is a finitely generated free $\mathbb{Z}$-module of rank $n$. In particular, $\mathcal{O}_K$ is a noetherian ring.

*Proof.* Let $(\alpha_1, \ldots, \alpha_n)$ be a $\mathbb{Q}$-basis of $K$ contained in $\mathcal{O}_K$ and set $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$. Then

$$\bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i \subseteq \mathcal{O}_K \subseteq \bigoplus_{i=1}^{n} \mathbb{Z}\frac{\alpha_i}{d}.$$

By the structure theorem, $\mathcal{O}$ is finitely generated. As it contains a submodule of rank $n$, it itself has rank $n$.

Let $I \triangleleft \mathcal{O}_K$ be a non-zero ideal and $\gamma \in I \setminus \{0\}$. As $\gamma\mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K$, we can apply the same argument as above. $\square$

**Remark 2.4.5.1.** If $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$ are two $\mathbb{Z}$-basis of $I$, then clearly $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \operatorname{disc}(\beta_1, \ldots, \beta_n)$. We can therefore define $\operatorname{disc}(I) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$.

**Remark 2.4.5.2.** If $J \subseteq I$ are both finitely generated free $\mathbb{Z}$-modules, each containing a $\mathbb{Q}$-basis of $K$, then

$$\operatorname{disc}(J) = \left| {}^{I}\!\big/_{J} \right|^2 \cdot \operatorname{disc}(I)$$

by the structure theorem.

**Theorem 2.4.6.** Let $K$ be a number field and let $I \subseteq \mathcal{O}_K$ be a finitely generated free $\mathbb{Z}$-module containing a $\mathbb{Q}$-basis $(\alpha_1, \ldots, \alpha_n)$ of $K$. Set $d = |\operatorname{disc}(\alpha_1, \ldots, \alpha_n)|$ and write $d = d_0^2 d_1$ with $d_1$ being square-free. For $1 \le i \le n$, choose $c_{i,j} \in \mathbb{Z}$ and $c_{i,i} \in \mathbb{N}$ such that

$$\beta_i = \frac{1}{d_0} \sum_{j=1}^{i} c_{i,j}\alpha_j \in I$$

and $c_{i,i}$ are minimal. Then $(\beta_1, \ldots, \beta_n)$ is a $\mathbb{Z}$-basis of $I$.

*Proof.* Write

$$J = \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i \subseteq I \subseteq \mathcal{O}_K.$$

Note that $\operatorname{disc}(I)$ and $\operatorname{disc}(J)$ are both integers and

$$d_0^2 \cdot d_1 = d = \operatorname{disc}(J) = [I : J]^2 \cdot \operatorname{disc}(I),$$

and as $d_1$ is square-free, it follows that $[I : J] \mid d_0$, therefore $d_0 I \subseteq J$. Note that $(\beta_1, \ldots, \beta_n)$ are $\mathbb{Q}$-linearly independent and $\langle \beta_i \mid i \le n \rangle_{\mathbb{Z}} \subseteq I$. It therefore suffices to show that $I \subseteq \langle \beta_i \mid i \le n \rangle_{\mathbb{Z}}$. Suppose otherwise, and let $\gamma \in I \setminus \langle \beta_i \mid i \le n \rangle_{\mathbb{Z}}$. As $\gamma \in \frac{1}{d_0} J$, we can write

$$\gamma = \frac{1}{d_0} \sum_{i=1}^{s} x_i\alpha_i$$

with $x_i \in \mathbb{Z}$ and $x_s \neq 0$. Choose $\gamma$ such that $s$ is minimal, and among those, the one with minimal $|x_s|$. Assume further that $x_s > 0$. But then, as $x_s \ge c_{s,s}$ by choice of $\beta_s$, we find that $x_s - \beta_s \in \langle \beta_i \mid i \le n \rangle_{\mathbb{Z}}$ by minimality, which is a contradiction. $\square$

**Corollary 2.4.6.1.** The ring $\mathcal{O}_K$ has an integral basis of the form $\{\alpha_i \mid i \le n\}$ with $\alpha_1 = 1$.

March 29, 2024

*Proof.* Apply the previous theorem to a $\mathbb{Q}$-basis of $\mathcal{O}_K$ of the form $(1, \alpha_2', \ldots, \alpha_n')$. $\square$

**Remark 2.4.6.2.** If $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ are elements such that $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ is square-free, they form an integral basis.

**Definition 2.4.7.** Let $K$ be a number field and $(\alpha_1, \ldots, \alpha_n)$ an integral basis of $\mathcal{O}_K$. We then define

$$\operatorname{disc}(K) = \operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}.$$

**Remark 2.4.7.1.** If $d$ is square-free and $K = \mathbb{Q}\left(\sqrt{d}\right)$, then

$$\operatorname{disc}(K) = \begin{cases} d, & d \equiv 1 \pmod 4, \\ 4d, & d \equiv 2, 3 \pmod 4. \end{cases}$$

## 2.5 Integral bases of Cyclotomic fields

**Lemma 2.5.1.** Suppose that $n = p^e$ with $p \in \mathbb{P}$ and $e \geq 1$. Choose $\zeta \in \mu_n^*(\mathbb{C})$ and set $K = \mathbb{Q}(\zeta)$.

i) We have
$$N^K(1-\zeta) = \prod_{p \nmid j}(1-\zeta^j) = p.$$
If $n \neq 2$, then $N^K(1-\zeta) = N^K(\zeta - 1)$.

ii) We have
$$(1-\zeta)^{\varphi(n)} \;\Big|\; p$$
in $\mathbb{Z}[\zeta]$.

*Proof.*

i) Recall that
$$\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \left\{\zeta \mapsto \zeta^j \;\middle|\; p \nmid j\right\}.$$
It follows that
$$N^K(1-\zeta) = \prod_{\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} (1 - \sigma(\zeta)) = \prod_{p \nmid j}(1-\zeta^j).$$
If $n \neq 2$, then $\varphi(n)$ is even and $N^K(1-\zeta) = N^K(\zeta - 1)$ follows. Now note that
$$\Phi_{p^e}(x) = \frac{x^{p^e} - 1}{x^{p^{e-1}} - 1} = \sum_{j=0}^{p-1} x^{jp^{e-1}} = \prod_{p \nmid j}(x - \zeta^j).$$
Evaluating the expression at $x = 1$, we get $N^K(1-\zeta) = p$.

ii) Note first that $1 - \zeta \mid 1 - \zeta^j$ for all $j \in \mathbb{N}$. But then
$$(1-\zeta)^{\varphi(n)} \;\Bigg|\; \prod_{p \nmid j}(1-\zeta^j) = p.$$
□

**Lemma 2.5.2.** If $\zeta \in \mu_p^*(\mathbb{C})$ for $p \in \mathbb{P}$, then
$$\mathrm{disc}(1, \zeta, \dots, \zeta^{p-2}) = \begin{cases} p^{p-2}, & p \equiv 1, 2 \pmod 4, \\ -p^{p-2}, & p \equiv 3 \pmod 4. \end{cases}$$

*Proof.* Without loss of generality assume $p \neq 2$. Then
$$m_\zeta = \Phi_p = \frac{x^p - 1}{x - 1} = \sum_{j=0}^{p-1} x^j.$$
By proposition 2.3.9, it holds that
$$\mathrm{disc}(1, \zeta, \dots, \zeta^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} \cdot N^K(\Phi_p'(\zeta)).$$

As
$$\Phi_p + (x-1)\Phi_p' = p \cdot x^{p-1},$$
we get
$$\Phi_p'(\zeta) = \frac{p \cdot \zeta^{p-1}}{\zeta - 1},$$
therefore
$$N(\Phi_p'(\zeta)) = \frac{N(p) \cdot N(\zeta^{-1})}{N(\zeta - 1)} = \frac{p^{p-1} \cdot 1}{p} = p^{p-2}. \qquad \square$$

**Lemma 2.5.3.** Let $n \in \mathbb{N}$ and $\zeta \in \mu_n^*(\mathbb{C})$. Then
$$\operatorname{disc}\left(1, \zeta, \ldots, \zeta^{\varphi(n)-1}\right) \;\Big|\; n^{\varphi(n)}.$$

*Proof.* Write
$$x^n - 1 = \Phi_n(x) \cdot g(x)$$
for $g \in \mathbb{Z}[x]$. Then $nx^{n-1} = \Phi_n'(x) \cdot g(x) + \Phi_n(x) \cdot g'(x)$, therefore
$$n\zeta^{n-1} = \Phi_n'(\zeta) \cdot g(\zeta).$$
Taking the norm, we get
$$n^{\varphi(n)} \cdot N(\zeta^{n-1}) = N(\Phi_n'(\zeta)) \cdot N(g(\zeta)),$$
but as $N(g(\zeta)) \in \mathbb{Z}$ and $N(\zeta^{n-1}) = \pm 1$, the conclusion follows. $\square$

**Theorem 2.5.4.** Let $n = p^e$ for $p \in \mathbb{P}$ and $e \geq 1$. Choose $\zeta \in \mu_n^*(\mathbb{C})$ and set $K = \mathbb{Q}(\zeta)$. Then
$$\mathcal{O}_K = \mathbb{Z}[\zeta] = \bigoplus_{j=0}^{\varphi(n)-1} \mathbb{Z}\zeta^j.$$

*Proof.* Let $m = [K : \mathbb{Q}] = \varphi(n)$. By the previous lemma, we have
$$\operatorname{disc}(1, \zeta, \ldots, \zeta^{m-1}) = \pm p^t$$
for some $t \geq 0$. By lemma 2.4.4, we see that
$$\mathcal{O}_K \subseteq \frac{1}{p^t} \cdot \left\langle (1-\zeta)^j \;\middle|\; j \leq m-1 \right\rangle_{\mathbb{Z}},$$
as $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$. Suppose that $\mathbb{Z}[1-\zeta] \subset \mathcal{O}_K$. Then there exists some
$$\alpha = \frac{1}{p} \cdot \sum_{j=i}^{m-1} a_j (1-\zeta)^j \in \mathcal{O}_K \setminus \mathbb{Z}[1-\zeta]$$
with $0 \leq i \leq m-1$ and $a_j \in \mathbb{Z}$ with $p \nmid a_i$. By lemma 2.5.1, we get $(1-\zeta)^{i+1} \mid p$, therefore
$$\frac{p\alpha}{(1-\zeta)^{i+1}} = \frac{a_i}{1-\zeta} + \sum_{j=i+1}^{m-1} a_j (1-\zeta)^{j-i-1},$$
and so $1 - \zeta \mid a_i$. But then $\pm p = N(1-\zeta) \mid N(a_i)$, which is impossible as we have $N(a_i) = a_i^m$. $\square$

**Lemma 2.5.5.** Let $K$ and $L$ be number fields with $m = [K : \mathbb{Q}]$ and $n = [L : \mathbb{Q}]$. Assume that $[KL : \mathbb{Q}] = mn$. Then for every pair $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ and $\varphi \in \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C})$ there exists a unique $\psi \in \mathrm{Hom}_{\mathbb{Q}}(KL, \mathbb{C})$ such that $\psi|_K = \sigma$ and $\psi|_L = \varphi$.

*Proof.* Note that every $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ extends to $\psi \in \mathrm{Hom}_{\mathbb{Q}}(KL, \mathbb{C})$ in $[KL : K] = n$ distinct ways. The $n$ maps $\psi|_L$ are then clearly distinct, hence one of them is equal to $\varphi$. Uniqueness is obvious. □

**Theorem 2.5.6.** Let $K$ and $L$ be number fields with $m = [K : \mathbb{Q}]$ and $n = [L : \mathbb{Q}]$. Suppose that $(\alpha_1, \ldots, \alpha_m)$ and $(\beta_1, \ldots, \beta_n)$ are integral basis of $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively. If $[KL : \mathbb{Q}] = mn$ and $\gcd(\mathrm{disc}(K), \mathrm{disc}(L)) = 1$, then

$$(\alpha_i\beta_j \mid i \leq m \wedge j \leq n)$$

is an integral basis for $\mathcal{O}_{KL}$. Furthermore,

$$\mathrm{disc}(KL) = \mathrm{disc}(K)^n \cdot \mathrm{disc}(L)^m.$$

*Proof.* Let $\gamma \in \mathcal{O}_{KL}$ and write

$$\gamma = \sum_{i,j} c_{i,j}\alpha_i\beta_j$$

with $c_{i,j} \in \mathbb{Q}$. This representation is unique, as $\{\alpha_i\beta_j \mid i \leq m \wedge j \leq n\}$ is a $\mathbb{Q}$-basis of $\mathcal{O}_{KL}$. Now write

$$\xi_j = \sum_{i=1}^{m} c_{i,j}\alpha_i \in K.$$

That gives us

$$\gamma = \sum_{j=1}^{n} \beta_j\xi_j.$$

Let $\mathrm{Hom}_K(KL, \mathbb{C}) = \{\varphi_i \mid i \leq n\}$. Applying $\varphi_i$ to the above equation, we get

$$b = \begin{bmatrix} \varphi_1(\gamma) \\ \varphi_2(\gamma) \\ \vdots \\ \varphi_n(\gamma) \end{bmatrix} = \underbrace{\begin{bmatrix} \varphi_1(\beta_1) & \varphi_1(\beta_2) & \ldots & \varphi_1(\beta_n) \\ \varphi_2(\beta_1) & \varphi_2(\beta_2) & \ldots & \varphi_2(\beta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_n(\beta_1) & \varphi_n(\beta_2) & \ldots & \varphi_n(\beta_n) \end{bmatrix}}_{B} \cdot \begin{bmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{bmatrix}.$$

Let $d = \mathrm{disc}(L) = \det(B)^2$. Then

$$d\xi = dB^{-1}b = d \cdot \frac{\mathrm{adj}(B)}{\det(B)} \cdot b = \det(B) \cdot \mathrm{adj}(B) \cdot b.$$

It follows that $d\xi_j$ are algebraic integers, therefore $d \cdot c_{i,j} \in \mathbb{Z}$ for all $i$ and $j$. By symmetry, the same holds for $d' = \mathrm{disc}(K)$. As $\gcd(d, d') = 1$, we get $c_{i,j} \in \mathbb{Z}$.

Let now $\mathrm{Hom}_L(KL, \mathbb{C}) = \{\sigma_j \mid j \leq m\}$ and denote by $\psi_{i,j}$ the element of $\mathrm{Hom}_Q(KL, \mathbb{C})$ with $\psi_{i,j}|_K = \sigma_i$ and $\psi_{i,j}|_L = \varphi_j$. Denote by $A$ the $(mn) \times (mn)$ matrix with

$$A = \left[\psi_{i,j}(\alpha_s\beta_t)\right]_{\substack{i,s\leq m\\ j,t\leq n}} = \begin{bmatrix} B & 0 & \dots & 0 \\ 0 & B & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & B \end{bmatrix} \cdot \begin{bmatrix} \sigma_1(\alpha_1)I_n & \sigma_1(\alpha_2)I_n & \dots & \sigma_1(\alpha_m)I_n \\ \sigma_2(\alpha_1)I_n & \sigma_2(\alpha_2)I_n & \dots & \sigma_2(\alpha_m)I_n \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_m(\alpha_1)I_n & \sigma_m(\alpha_2)I_n & \dots & \sigma_m(\alpha_m)I_n \end{bmatrix}.$$

Reindexing, we find that

$$\det \begin{bmatrix} \sigma_1(\alpha_1)I_n & \sigma_1(\alpha_2)I_n & \dots & \sigma_1(\alpha_m)I_n \\ \sigma_2(\alpha_1)I_n & \sigma_2(\alpha_2)I_n & \dots & \sigma_2(\alpha_m)I_n \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_m(\alpha_1)I_n & \sigma_m(\alpha_2)I_n & \dots & \sigma_m(\alpha_m)I_n \end{bmatrix} = \det \begin{bmatrix} C & 0 & \dots & 0 \\ 0 & C & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & C \end{bmatrix},$$

where

$$C = \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_m) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \dots & \sigma_2(\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_m) \end{bmatrix}.$$

It follows that

$$\mathrm{disc}(KL) = \det(A)^2 = \left(\det(B)^m \cdot \det(C)^n\right)^2 = \mathrm{disc}(L)^m \cdot \mathrm{disc}(K)^n. \qquad \square$$

**Theorem 2.5.7.** Let $n \geq 1$ and $\zeta \in \mu_n^*(\mathbb{C})$. Denote $K = \mathbb{Q}(\zeta)$. Then $(1, \zeta, \dots, \zeta^{\varphi(n)-1})$ is an integral basis of $\mathcal{O}_K$.

*Proof.* We prove the theorem by induction on the number of distinct prime factors of $n$. The claim clearly holds for $n = 1$ and prime powers by theorem 2.5.4. Now write $n = st$ for $s, t < n$ with $\gcd(s, t) = 1$. Choose $\zeta_s \in \mu_s^*(\mathbb{C})$ and $\zeta_t \in \mu_t^*(\mathbb{C})$. By the proof of corollary 2.2.14.1, $\zeta_s \cdot \zeta_t$ is a primitive $st$-th root of unity, therefore $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_s)\mathbb{Q}(\zeta_t)$. We therefore get

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \varphi(s) \cdot \varphi(t) = [\mathbb{Q}(\zeta_s) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_t) : \mathbb{Q}].$$

By the induction hypothesis,

$$\mathrm{disc}(\mathbb{Q}(\zeta_s)) = \mathrm{disc}(\mathbb{Z}[\zeta_s]) \mid s^{\varphi(s)}$$

and similarly for $t$. In particular, $\gcd(\mathrm{disc}(\mathbb{Q}(\zeta_s), \mathbb{Q}(\zeta_t)) = 1$, therefore

$$\mathcal{O}_K = \mathbb{Z}[\zeta_s, \zeta_t] = \mathbb{Z}[\zeta_n]$$

by the previous theorem. $\square$

**Remark 2.5.7.1.** We can in fact show that

$$\operatorname{disc}(K) = (-1)^{\frac{\varphi(n)}{2}} \cdot n^{\varphi(n)} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} p^{-\frac{\varphi(n)}{p-1}}.$$

**Theorem 2.5.8** (Stickelberger)**.** Let $K$ be a number field. Then $\operatorname{disc}(K) \equiv 0, 1 \pmod 4$.

*Proof.* Let $L$ be the Galois closure of $K$, that is the smallest field $L$ containing $K$ such that $\operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C}) = \operatorname{Gal}\left({}^{L}/_{\mathbb{Q}}\right)$. Denote $n = [K : \mathbb{Q}]$ and choose $\{\sigma_i \mid i \le n\} \subseteq \operatorname{Gal}\left({}^{L}/_{\mathbb{Q}}\right)$ to be extensions of elements of $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. Furthermore, let $(\alpha_1, \dots, \alpha_n)$ be an integral basis of $\mathcal{O}_K$. Denote

$$C = \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \dots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{bmatrix}.$$

Then $\operatorname{disc}(K) = \det(C)^2$. Write

$$P = \sum_{\substack{\pi \in S_n \\ \operatorname{sgn}(\pi)=1}} \prod_{i=1}^{n} \sigma_{\pi(i)}(\alpha_i) \quad \text{and} \quad N = \sum_{\substack{\pi \in S_n \\ \operatorname{sgn}(\pi)=-1}} \prod_{i=1}^{n} \sigma_{\pi(i)}(\alpha_i).$$

As $\det(C) = P - N$, we get

$$\operatorname{disc}(K) = (P - N)^2 = (P + N)^2 - 4PN.$$

It is clear that both $P + N$ and $PN$ are elements of $\mathcal{O}_L$. For all $\varphi \in \operatorname{Gal}\left({}^{L}/_{\mathbb{Q}}\right)$ we have $\varphi \circ \sigma_i|_K \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, therefore there exists a permutation $\tau \in S_n$ such that $\varphi \circ \sigma_i|_K = \sigma_{\tau(i)}\big|_K$ for all $i$. As $\operatorname{sgn}(\tau \circ \pi) = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\pi)$, we get

$$\varphi(P) = \sum_{\substack{\pi \in S_n \\ \operatorname{sgn}(\pi)=1}} \prod_{i=1}^{n} \varphi(\sigma_{\pi(i)}(\alpha_i)) = \sum_{\substack{\pi \in S_n \\ \operatorname{sgn}(\pi)=\operatorname{sgn}(\tau)}} \prod_{i=1}^{n} \sigma_{\pi(i)}(\alpha_i) = \begin{cases} P, & \operatorname{sgn}(\tau) = 1, \\ N, & \operatorname{sgn}(\tau) = -1. \end{cases}$$

We get a similar condition on $\varphi(N)$. It follows that $\varphi(P+N) = P+N$ and $\varphi(P \cdot N) = P \cdot N$. Therefore $P + N$ and $P \cdot N$ are both integers and hence

$$\operatorname{disc}(K) \equiv (P + N)^2 \equiv 0, 1 \pmod 4.$$

□

**Remark 2.5.8.1.** The Galois closure $L$ of $K$ if given by

$$L = \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})} \sigma(K).$$

# 3 Dedekind domains

*Sorry if you're TEXing this now.*
– gost. izr. prof. dr. rer. nat. Daniel Smertnig

April 5, 2024

## 3.1 Prime ideal factorisation

**Definition 3.1.1.** Let $D$ and $D'$ be domains with $D \subseteq D'$ and let $K$ be the quotient field of $D$. An element $\alpha' \in D'$ is *integral* over $D$ if there exists a monic polynomial $f \in D[x]$ such that $f(\alpha) = 0$. The domain $D$ is *integrally closed* if

$$D = \{\alpha \in K \mid \alpha \text{ is integral over } D\}.$$

**Lemma 3.1.2.** Let $K$ be a number field and $\mathfrak{a} \lhd \mathcal{O}_K$ a non-zero ideal. Then $|\mathcal{O}_K/\mathfrak{a}| < \infty$. Furthermore, if $\mathfrak{p} \lhd \mathcal{O}_K$ is a non-zero prime ideal, then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number $p$. The ring $\mathcal{O}_K/\mathfrak{p}$ is a finite field extension of $\mathbb{Z}_p$.

*Proof.* Let $\alpha \in \mathfrak{a}$ be a non-zero element. As $\alpha$ is an algebraic integer, we can write

$$\alpha^m + \sum_{j=0}^{m-1} a_j \alpha^j = 0$$

for integers $a_j$, where we assume $a_0 \neq 0$. But then we must have $a_0 \in \mathfrak{a}$, therefore $a_0\mathcal{O}_K \subseteq \mathfrak{a}$. Hence $\mathcal{O}_K/\mathfrak{a}$ is a quotient of $\mathcal{O}_K/a_0\mathcal{O}_K$. By the structure theorem the quotient is finite, as the above free abelian groups both have the same rank.

Now let $\mathfrak{p}$ be a prime ideal. Note that $\mathcal{O}_K/\mathfrak{p}$ is a finite domain and therefore a field. Note that $a_0 \in \mathfrak{p} \cap \mathbb{Z} \setminus \{0\}$, therefore the intersection $\mathfrak{p} \cap \mathbb{Z}$ is non-trivial. In particular, it is a prime ideal of $\mathbb{Z}$ and hence $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number $p$. As the kernel of the map $\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$ is $p\mathbb{Z}$, it induces an injective map $\mathbb{Z}_p \to \mathcal{O}_K/\mathfrak{p}$. □

**Theorem 3.1.3.** Let $K$ be a number field. Then $\mathcal{O}_K$ is a noetherian integrally closed domain and every non-zero prime ideal of $\mathcal{O}_K$ is maximal.

*Proof.* We already know that $\mathcal{O}_K$ is noetherian. Let $\alpha \in K$ be integral over $\mathcal{O}_K$. It follows that $\mathcal{O}_K[\alpha]$ is a finitely-generated $\mathcal{O}_K$-module and hence a finitely-generated $\mathbb{Z}$-module. This implies that $\alpha$ is an algebraic integer.

If $\mathfrak{p}$ is a non-zero prime ideal, then $\mathcal{O}_K/\mathfrak{p}$ is a field and hence $\mathfrak{p}$ is maximal. □

**Definition 3.1.4.** A *Dedekind domain* is a noetherian integrally closed domain in which every non-zero prime ideal is maximal.

**Definition 3.1.5.** Let $D$ be a domain and $K$ its quotient field.

i) A *fractional ideal* of $D$ is a $D$-submodule of $K$ that is of the form $c^{-1}I$ for some $c \in D \setminus \{0\}$ and $0 \neq I \lhd D$.

ii) A fractional ideal $I$ is *invertible* if there exists a fractional ideal $J$ such that $IJ = D$.

**Remark 3.1.5.1.** For a fractional ideal $I$, we write

$$I^{-1} = \{x \in K \mid xI \subseteq D\}.$$

If $I$ is invertible, then $I^{-1}$ is its unique inverse.

**Lemma 3.1.6.** Let $D$ be a Dedekind domain that is not a field. For every non-zero ideal $I \lhd D$ there exists an integer $r \geq 0$ and non-zero prime ideals $P_i \lhd D$ such that

$$\prod_{i=1}^{r} P_i \subseteq I.$$

*Proof.* Let $\Omega$ be the set of ideals $I$ for which the above does not hold. Suppose that $\Omega \neq \emptyset$. As $D$ is noetherian, there exists a maximal ideal $I \in \Omega$, which clearly cannot be a prime ideal. Also note that $I \neq D$. It follows that there exist $a, b \in D \setminus I$ such that $ab \in I$. But then both $aD + I$ and $bD + I$ are not in $\Omega$ by maximality of $I$. Now we can just take the product of their respective prime ideals, which gives a contradiction. $\square$

**Lemma 3.1.7.** Let $D$ be a Dedekind domain that is not a field and $P \lhd D$ be a non-zero prime ideal. For every non-zero ideal $I \lhd D$ we have $I \subset IP^{-1}$.

*Proof.* Consider first the case $I = D$. Let $a \in P \setminus \{0\}$ and write

$$\prod_{i=1}^{r} P_i \subseteq aD \subseteq P,$$

where $r$ is minimal. As $P$ is a prime ideal, we must have $P_i \subseteq P$ for some $i$ – without loss of generality let this be $P_1$. As prime ideals are maximal, we must hence have $P_1 = P$. By minimality of $r$, we must have

$$\prod_{i=2}^{r} P_i \not\subseteq aD,$$

hence it has an element $b$ such that $b \notin aD$ but $bP \subseteq aD$. But then $\frac{b}{a} \in P^{-1} \setminus D$, as required.

Now consider the general case. Note that, as $D$ is noetherian, the ideal $I$ is finitely generated – write $I = \langle a_i \mid i \leq m \rangle_D$. Suppose that $I = IP^{-1}$ and let $x \in P^{-1}$.

Choose $c_{i,j}$ such that

$$xa = x \cdot \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} = \underbrace{\begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,m} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m,1} & c_{m,2} & \cdots & c_{m,m} \end{bmatrix}}_{C} \cdot \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix}.$$

But then $xa = Ca$, therefore $\det(xI_m - C) = 0$. Expanding the determinant, we get a monic polynomial with $x$ as a root, therefore $x$ is integral over $D$ and hence $x \in D$. It follows that $P^{-1} \subseteq D$, which we have already shown cannot happen. $\square$

**Theorem 3.1.8.** If $D$ is a Dedekind domain, then every non-zero ideal is a product of prime ideals. Such a representation is unique up to the order of factors.

*Proof.* If $D$ is a field, its only ideals are 0 and $D$ itself, which clearly factors.

Let $\Omega$ be the set of all non-zero ideals of $D$ that cannot be factored as a product of prime ideals. As $D$ is noetherian, there exists a maximal element $I \in \Omega$. Note that $I \neq D$. Let $P$ be a maximal ideal of $D$ containing $I$. Then $I \subset IP^{-1}$ and $P \subset PP^{-1} subseteq D$, but as $P$ is maximal, we actually have $PP^{-1} = D$. By maximality of $P$, we can factor

$$IP^{-1} = \prod_{r=2}^{m} P_i,$$

but then

$$I = IPP^{-1} = P \cdot \prod_{r=2}^{m} P_i.$$

Next, we show that this factorisation is unique. Suppose otherwise that

$$\prod_{i=1}^{r} P_i = \prod_{i=1}^{s} Q_i$$

for prime ideals $P_i$ and $Q_i$. But this implies that $Q_i \subseteq P_1$ for some $i$, as $P_1$ is prime. Without loss of generality let $Q_1 \subseteq P_1$. As $Q_1$ is maximal, we must have $Q_1 = P_1$. Multiplying by $P_1^{-1}$ and using the fact that $P_1P_1^{-1} = D$, we get uniqueness by induction. □

**Corollary 3.1.8.1.** If $D$ is a Dedekind domain, then every fractional ideal is invertible.

*Proof.* Let $I$ be a fractional ideal. Let $c \in D^*$ be an element such that $cI \triangleleft D$. We can therefore factor $cI$ as a product of prime ideals $P_i$. But all of there are invertible and so

$$I \cdot c \prod_{i=1}^{r} P_i^{-1} = D.$$ □

## 3.2 Fractional ideals and the class group

**Definition 3.2.1.** Let $D$ be a Dedekind domain and $P \triangleleft D$ be a non-zero prime ideal. The *$P$-adic valuation* $\nu_P(I)$ of a non-zero ideal $I \triangleleft D$ is the exponent of $P$ in the factorization of $I$.

**Remark 3.2.1.1.** We denote the prime ideals of $D$ by $\mathcal{P}(D)$. The monoid of of all non-zero ideals is denoted by $\mathcal{I}(D)^\bullet$, while the monoid of fractional ideals is denoted by $\mathcal{F}(D)$.

**Theorem 3.2.2.** There is a group isomorphism $\mathcal{F}(D) \to \mathbb{Z}^{\mathcal{P}(D)}$, $I \mapsto (\nu_P(I))_{P\in\mathcal{P}(D)}$, that restricts to a monoid isomorphism $\mathcal{I}(D)^\bullet \to \mathbb{N}_0^{\mathcal{P}(D)}$.

**Definition 3.2.3.** Let $D$ be a Dedekind domain. Let $\mathcal{H}(D)$ be all the non-zero principal ideals of $D$. The abelian group $\mathcal{C}(D) = \mathcal{F}(D)\big/\mathcal{H}(D)$ is the *class group* of $D$.

**Remark 3.2.3.1.** The sequence

$$1 \longrightarrow D^* \longrightarrow K^* \longrightarrow \mathcal{F}(D) \longrightarrow \mathcal{C}(D) \longrightarrow 1$$

is exact.

**Theorem 3.2.4.** Let $D$ be a Dedekind domain. The following statements are equivalent.

i) The domain $D$ is a unique factorisation domain.

ii) The class group $\mathcal{C}(D)$ is trivial.

iii) The domain $D$ is a principal ideal domain.

*Proof.* Note that we only need to prove that the class group of a unique factorisation domain is trivial. It therefore suffices to show that every prime ideal $P \subseteq D$ is principal. Let $a \in P \setminus \{0\}$ and write

$$a = \prod_{i=1}^r p_i$$

for prime elements $p_i$ of $D$. It follows that $p_i \in P$ for some $i$. But then $p_iD \subseteq P$ is also a prime ideal, which must be equal to $P$ by maximality. □

**Proposition 3.2.5.** Every principal ideal domain is a Dedekind domain.

*Proof.* As every ideal of $D$ is generated by one element, it is a noetherian ring.

Let $K$ be the quotient field of $D$. Suppose that $f\left(\frac{a}{b}\right) = 0$ for a monic polynomial $f$ and $\frac{a}{b} \in K$. Since $D$ is a unique factorisation domain, we can further assume that $a$ and $b$ have no non-trivial common factor. As

$$0 = b^m f\left(\frac{a}{b}\right),$$

we can deduce that $b \mid a^m$ in $D$. This immediately shows that $b$ is a unit and therefore $\frac{a}{b} \in D$, which means that $D$ is integrally closed.

Now let $P \triangleleft D$ be a non-zero prime ideal, contained in a maximal ideal $M$. It is clear that $P = (p)$ and $M = (q)$ for some prime elements $p, q \in D$. But this implies $q \mid p$ and hence $(p) = (q)$, therefore $P = M$ is maximal. □



April 12, 2024

### 3.3 Chinese remainder theorem

**Theorem 3.3.1** (Chinese remainder theorem)**.** Let $R$ be a ring and let $I_1, \dots, I_m \triangleleft R$ be ideals that are pairwise comaximal.[4] Then the map

$$R \big/ \textstyle\bigcap_{i=1}^m I_i \to \displaystyle\prod_{i=1}^m R \big/ I_i \,,$$

given by

$$r + \bigcap_{i=1}^m I_i \mapsto (r + I_1, \dots, r + I_m)\,,$$

is an isomorphism of $R$-algebras.

*Proof.* It suffices to show that the above homomorphism is surjective. Let $a_1, \dots, a_m \in R$. For all $i, j$ there exist elements $x_{i,j} \in I_i$ and $y_{i,j} \in I_j$ such that $x_{i,j} + y_{i,j} = 1$. Setting

$$z_i = \prod_{j \neq i} y_{i,j},$$

it is clear that $z_i \equiv \delta_{i,j} \pmod{I_j}$. But then

$$\varphi\left(\sum_{i=1}^m z_i a_i\right) = (a_1 + I_1, \dots, a_m + I_m)\,. \qquad \square$$

**Corollary 3.3.1.1.** Let $D$ be a Dedekind domain, $P_1, \dots, P_m \triangleleft D$ be pairwise distinct prime ideals, and $e_1, \dots, e_m \in \mathbb{N}_0$. If $a_1, \dots, a_m \in D$, then there exists an element $a \in D$ such that for all $i \leq m$ we have

$$a \equiv a_i \pmod{P_i^{e_i}}.$$

*Proof.* The proof is obvious and need not be mentioned. $\square$

**Corollary 3.3.1.2.** Let $D$ be a Dedekind domain, $P_1, \dots, P_m \triangleleft D$ be pairwise distinct prime ideals, and $e_1, \dots, e_m \in \mathbb{Z}$. Then there exists an element $x \in K^*$ with $v_{P_i}(x) = e_i$ for all $i \leq m$ and $v_P(x) \geq 0$ for all non-zero primes $P \neq P_i$.

*Proof.* The case where $e_i \geq 0$ for all $i$ follows from the previous corollary. Construct an element $b \in D$ such that $\nu_{P_i}(b) = \max(0, -e_i)$ for all $i$. Then, construct an element $a \in D$ such that $\nu_{P_i}(a) = \max(0, e_i)$ for all $i$ and $\nu_Q(a) \geq \nu_Q(b)$ for all other prime ideals $Q$. Then $\frac{a}{b}$ is one such element. $\square$

**Theorem 3.3.2.** Let $D$ be a Dedekind domain and let $I \triangleleft D$ be a non-zero ideal. If $a \in I$ is a non-zero element, then there exists some $b \in I$ such that $I = (a, b)$.

*Proof.* Consider all prime ideals $P_i$ with $\nu_{P_i}(aD) > 0$. Note that $\nu_{P_i}(aD) \geq \nu_{P_i}(I)$. Choose an element $b$ such that $\nu_{P_i}(b) = \nu_{P_i}(I)$ for all $I$. It is clear that

$$\nu_P(I) = \min(\nu_P(aD), \nu_P(bD)) = \nu_P(aD + bD)$$

holds, hence $I = (a, b)$. $\square$

[4] That is, $I_i + I_j = R$ for all $i \neq j$.

# 4 Minkowski theory

*We'll skip this so we don't have to do any actual integrals, so if you're bored …*
– gost. izr. prof. dr. rer. nat. Daniel Smertnig

## 4.1 Lattices

**Definition 4.1.1.** Let $V$ be an $\mathbb{R}$-vector space of dimension $n$. A *lattice* is a subgroup

$$\Gamma = \sum_{i=1}^{m} \mathbb{Z}v_i \subseteq V,$$

where $v_i$ are $\mathbb{R}$-linearly independent vectors. The tuple $(v_1, \dots, v_m)$ is called the *basis* of the lattice. The lattice is *complete* if $m = n$. The set

$$F = \left\{ \sum_{i=1}^{m} x_i v_i \;\middle|\; \forall i \leq m \colon x_i \in [0,1) \right\}$$

is the *fundamental domain* of the basis $(v_1, \dots, v_m)$.

**Proposition 4.1.2.** Let $V$ be an $n$-dimensional $\mathbb{R}$-vector space and $\Gamma \subseteq V$ be a subgroup. Then the following statements are equivalent:

i) The set $\Gamma$ is a lattice.

ii) The point 0 is not an accumulation point of $\Gamma$.

iii) The set $\Gamma$ is discrete.

*Proof.* Suppose that $\Gamma$ is a lattice. Extend its basis $(v_1, \dots, v_m)$ to a basis of $\mathbb{R}^n$. Then

$$\left\{ \sum_{i=1}^{n} x_i v_i \;\middle|\; \forall i \colon x_i \in (-1,1) \right\}$$

contains no points of $\Gamma$ other than 0.

If 0 is not an accumulation point of $\Gamma$, the set is clearly discrete, as accumulation points are translation invariant.

Now suppose that $\Gamma$ is discrete and let $W = \mathbb{R}\Gamma$. Choose a basis $(w_1, \dots, w_m) \subseteq \Gamma$ for $W$. The set

$$\Gamma_0 = \bigoplus_{i=1}^{m} w_i \mathbb{Z} \subseteq \Gamma$$

is therefore a complete lattice in $W$. The fundamental domain $F_0$ of $\Gamma_0$ is a set of representatives for $W/\Gamma_0$. But then there exists a set $R \subseteq F_0$ of representatives of $\Gamma/\Gamma_0$, which is both bounded and discrete, and therefore finite. For $d = [\Gamma : \Gamma_0]$ we then have $\Gamma \subseteq \frac{1}{d}\Gamma_0$, which must then be a free abelian group of rank $m$ by the structure theorem. Since it spans $W$, its generators must be $\mathbb{R}$-linearly independent. $\square$

**Lemma 4.1.3.** A lattice $\Gamma \subseteq V$ is complete if and only if $V/\Gamma$ has a bounded system of representatives.

*Proof.* If $\Gamma$ is complete, then any fundamental domain gives us a bounded system of representatives.

Suppose now that $\Gamma \subseteq V$ is a lattice and $B$ a bounded set with

$$V = \bigcup_{\gamma \in \Gamma} (\gamma + B).$$

Let $W = \operatorname{Lin}(\Gamma)$. As it is a finite-dimensional subspace in $V$, it is a closed subspace. Take an arbitrary $v \in V$. We can write $n \cdot v = \gamma_n + \beta_n$ for some $\gamma_n \in \Gamma$ and $\beta_n \in B$. It follows that

$$v = \lim_{n \to \infty} \frac{1}{n} \cdot (\gamma_n + \beta_n) = \lim_{n \to \infty} \frac{1}{n} \cdot \gamma_n \in W. \qquad \square$$

**Definition 4.1.4.** Let $\Gamma \subseteq \mathbb{R}^n$ be a complete lattice with fundamental domain $F$. We define its *volume* as

$$\operatorname{vol}(\Gamma) = \operatorname{vol}(F).$$

April 19, 2024

**Theorem 4.1.5** (Minkowski)**.** Let $\Gamma \subseteq \mathbb{R}^n$ be a complete lattice and $X \subseteq \mathbb{R}^n$ a set with the following properties:

i) It is symmetric around 0.

ii) It is convex.

iii) We have $\operatorname{vol}(X) > 2^n \operatorname{vol}(\Gamma)$.

Then $X$ contains a non-zero point of $\Gamma$.

*Proof.* Suppose that the family $\left\{\frac{1}{2}X + \gamma\right\}_{\gamma \in \Gamma}$ is pairwise disjoint. We can write

$$\mathbb{R}^n = \bigcup_{\gamma \in \Gamma} (\gamma + F),$$

where $F$ is the fundamental domain of $\Gamma$. It follows that

$$\frac{1}{2}X = \bigcup_{\gamma \in \Gamma} \left(\frac{1}{2}X \cap (\gamma + F)\right),$$

therefore

$$\frac{1}{2^n} \operatorname{vol}(X) = \sum_{\gamma \in \Gamma} \operatorname{vol}\left(\frac{1}{2}X \cap (\gamma + F)\right) = \sum_{\gamma \in \Gamma} \operatorname{vol}\left(\left(\frac{1}{2}X - \gamma\right) \cap F\right) \leq \operatorname{vol}(F),$$

which is a contradiction.

We can now write

$$\gamma_1 + \frac{1}{2}x_1 = \gamma_2 + \frac{1}{2}x_2$$

for some distinct $\gamma_i \in \Gamma$ and $x_i \in X$. It is clear that the point $\frac{1}{2}(x_1 - x_2) \neq 0$ is in both $X$ and $\Gamma$. $\square$

## 4.2 From ideals to lattices

**Definition 4.2.1.** Let $K$ be a number field of degree $n$. An embedding $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ is called a *real embedding* if $\sigma(K) \subseteq \mathbb{R}$. Otherwise, it is called a *complex embedding.*

**Remark 4.2.1.1.** A conjugate of a complex embedding is again a complex embedding. We denote by $r$ the number of real embeddings and by $s = \frac{n-r}{2}$ the number of pairs of conjugated complex embeddings.

**Remark 4.2.1.2.** Henceforth we assume the notation that $\sigma_1, \dots, \sigma_r$ are real embeddings and $\sigma_{r+i} = \overline{\sigma}_{r+i+s}$.

**Remark 4.2.1.3.** We can embed $j \colon K \to \mathbb{R}^n$ as

$$j(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \operatorname{Re} \sigma_{r+1}(\alpha), \dots, \operatorname{Re} \sigma_{r+s}(\alpha), \operatorname{Im} \sigma_{r+1}(\alpha), \dots, \operatorname{Im} \sigma_{r+s}(\alpha)).$$

**Proposition 4.2.2.** Let $\mathfrak{a} \subseteq K$ be a fractional ideal. Then $j(\mathfrak{a})$ is a complete lattice with

$$\mathrm{vol}(j(\mathfrak{a})) = 2^{-s} \sqrt{|\mathrm{disc}(\mathfrak{a})|}.$$

*Proof.* Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Then

$$\mathrm{disc}(\mathfrak{a}) = \det \begin{bmatrix} \sigma_k(\alpha_\ell) \end{bmatrix}_{k,\ell \le n}^2 .$$

Note that

$$\begin{bmatrix} \operatorname{Re} \sigma_{r+\ell}(\alpha) \\ \operatorname{Im} \sigma_{r+\ell}(\alpha) \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2i} & -\frac{1}{2i} \end{bmatrix} \cdot \begin{bmatrix} \sigma_{r+\ell}(\alpha) \\ \sigma_{r+\ell+s}(\alpha) \end{bmatrix}.$$

It follows that

$$j(\alpha) = \underbrace{\begin{bmatrix} I_r & 0 & 0 \\ 0 & \frac{1}{2} I_s & \frac{1}{2} I_s \\ 0 & \frac{1}{2i} I_s & -\frac{1}{2i} I_s \end{bmatrix}}_{C} \cdot \begin{bmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix}.$$

As $\det(C) = \frac{1}{2^s} \cdot \left(-\frac{1}{i}\right)^s$, we get $|\det(C)| = \frac{1}{2^s}$. Finally, we get

$$\mathrm{vol}(j(\mathfrak{a})) = |\det (j(\alpha_1), j(\alpha_2), \dots, j(\alpha_n))| = |\det C| \cdot \left| \det \begin{bmatrix} \sigma_k(\alpha_\ell) \end{bmatrix}_{k,\ell \le n} \right| = 2^{-s} \cdot \sqrt{|\mathrm{disc}(\mathfrak{a})|}.$$

□

**Theorem 4.2.3.** Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. For $i \le r+s$ let $c_i > 0$ be real numbers such that

$$\prod_{i=1}^r c_i \prod_{i=1}^s c_{i+r}^2 > \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}(\mathfrak{a})|}.$$

Then there exists a non-zero $\alpha \in \mathfrak{a}$ such that $|\sigma_i(\alpha)| < c_i$ for all $i \le n$.

*Proof.* Let

$$X = \left\{x \in \mathbb{R}^n \;\middle|\; \forall i \le r\colon\ |x_i| < c_i \wedge \forall i \le s\colon x_{r+i}^2 + x_{r+s+i}^2 < c_{r+i}^2\right\}.$$

We can then calculate

$$\operatorname{vol}(X) = \prod_{i=1}^{r}(2c_i) \cdot \prod_{i=1}^{s}\left(c_{r+i}^2 \cdot \pi\right) = 2^r \cdot \pi^s \cdot \prod_{i=1}^{r} c_i \prod_{i=1}^{s} c_{i+r}^2 > 2^{r+s} \cdot \sqrt{|\operatorname{disc}(\mathfrak{a})|} = 2^n \cdot \operatorname{vol}(j(\mathfrak{a})).$$

The set $j(\mathfrak{a}) \cap X$ therefore contains a non-zero element. Its preimage is the sought element. $\square$

**Theorem 4.2.4** (Minkowski)**.** Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. Then there exists a non-zero $\alpha \in \mathfrak{a}$ such that

$$\left|N^K(\alpha)\right| \le \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathfrak{a})|}.$$

*Proof.* Choose a real $c > 0$ such that

$$c^n > n! \cdot \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathfrak{a})|}$$

and let

$$Y = \left\{x \in \mathbb{R}^n \;\middle|\; \sum_{i=1}^{r}|x_i| + 2\sum_{i=1}^{s}\sqrt{x_{r+i}^2 + x_{r+s+i}^2} < c\right\}.$$

Someone who actually knows how to integrate can show that

$$\operatorname{vol}(Y) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{c^n}{n!} = 2r + s \cdot \left(\frac{\pi}{4}\right)^s \cdot \frac{c^n}{n!} > 2^{r+s} \cdot \sqrt{|\operatorname{disc}(\mathfrak{a})|} = 2^n \operatorname{vol}(j(\mathfrak{a})).$$

It follows that $Y \cap j(\mathfrak{a})$ contains a non-zero element. Equivalently, there exists some non-zero $\alpha \in \mathfrak{a}$ such that $j(\alpha) \in Y$.

Now note that

$$\begin{aligned}
\sqrt[n]{N^K(\alpha)} &= \prod_{i=1}^{r}|\sigma_i(\alpha)|^{\frac{1}{n}} \cdot \prod_{i=1}^{s}\sqrt{(\operatorname{Re}\sigma_{r+i}(\alpha))^2 + (\operatorname{Im}\sigma_{r+i}(\alpha))^2}^{\frac{2}{n}} \\
&\le \frac{1}{n} \cdot \left(\sum_{i=1}^{r}|\sigma_i(\alpha)| + 2\sum_{i=1}^{s}\sqrt{(\operatorname{Re}\sigma_{r+i}(\alpha))^2 + (\operatorname{Im}\sigma_{r+i}(\alpha))^2}\right) \\
&< \frac{c}{n}.
\end{aligned}$$

But then

$$\left|N^K(\alpha)\right| < \frac{c^n}{n^n} \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathfrak{a})|} + \varepsilon$$

for some $\varepsilon > 0$. Note that the set $\left|N^K(\mathfrak{a})\right|$ is discrete – taking $c$ small enough we therefore get

$$\left|N^K(\alpha)\right| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathfrak{a})|}. \qquad \square$$

## 4.3 Finiteness of the class group

**Definition 4.3.1.** Let $\mathfrak{a} \triangleleft \mathcal{O}_K$ be a non-zero ideal. We define the *norm* of $\mathfrak{a}$ as

$$N(\mathfrak{a}) = \left| {\mathcal{O}_K}/{\mathfrak{a}} \right|.$$

**Proposition 4.3.2.** Let $K$ be a number field.

i) If $\mathfrak{a}, \mathfrak{b} \triangleleft \mathcal{O}_K$ are non-zero ideals, then $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$.

ii) If $\mathfrak{a} = (\alpha)$ for a non-zero $\alpha \in \mathcal{O}_K$, then $N(\mathfrak{a}) = \left| N^K(\alpha) \right|$.

*Proof.*

i) If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, the conclusion follows from the Chinese remainder theorem. It therefore suffices to consider the case where $\mathfrak{a}$ and $\mathfrak{b}$ are both powers of the same non-zero prime ideal $\mathfrak{p}$, that is, $N(\mathfrak{p}^{e+1}) = N(\mathfrak{p}^e) \cdot N(\mathfrak{p})$ for $e \geq 0$.

   We will show that ${\mathcal{O}_K}/{\mathfrak{p}} \cong {\mathfrak{p}^e}/{\mathfrak{p}^{e+1}}$. Take $a \in \mathfrak{p}^e \setminus \mathfrak{p}^{e+1}$ and consider the homomorphism $\varphi \colon \mathcal{O}_K \to {\mathfrak{p}^e}/{\mathfrak{p}^{e+1}}$, given by $\varphi(x) = ax + p^{e+1}$. This induces a homomorphism ${\mathcal{O}_K}/{\mathfrak{p}} \to {\mathfrak{p}^e}/{\mathfrak{p}^{e+1}}$, which means that ${\mathfrak{p}^e}/{\mathfrak{p}^{e+1}}$ is a ${\mathcal{O}_K}/{\mathfrak{p}}$-vector space. If the above rings were not isomorphic, its dimension would be at least 2, therefore it would have a non-trivial subspace of the form ${\mathfrak{b}}/{\mathfrak{p}^{e+1}}$ for an ideal $\mathfrak{b} \triangleleft \mathcal{O}_K$. But then $\mathfrak{p}^{e+1} \subset \mathfrak{b} \subset \mathfrak{p}^e$, which implies $\mathfrak{p} \subset \mathfrak{p}^{-e}\mathfrak{b} \subset \mathcal{O}_K$, which contradicts $\mathfrak{p}$ being a maximal ideal.

ii) Let $\beta_1, \dots, \beta_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then $\alpha\beta_1, \dots, \alpha\beta_n$ is a $\mathbb{Z}$-basis of $(\alpha)$. We therefore have

$$\operatorname{disc}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]^2 \cdot \operatorname{disc}(\mathcal{O}_K).$$

   It therefore suffices to show that

$$\operatorname{disc}(\mathfrak{a}) = N^K(\alpha)^2 \cdot \operatorname{disc}(\mathcal{O}_K).$$

   Indeed, we have

$$\begin{aligned}
\operatorname{disc}(\mathfrak{a}) &= \det \Big[\sigma_k(\alpha\beta_\ell)\Big]_{k,\ell \leq n}^2 \\
&= \det \Big[\sigma_k(\alpha)\sigma_k(\beta_\ell)\Big]_{k,\ell \leq n}^2 \\
&= \prod_{k=1}^n \sigma_k(\alpha) \cdot \det \Big[\sigma_k(\beta_\ell)\Big]_{k,\ell \leq n}^2 \\
&= N^K(\alpha)^2 \cdot \operatorname{disc}(\mathcal{O}_K).
\end{aligned}$$

□

**Remark 4.3.2.1.** The norm multiplicatively extends to a map $\mathcal{F}(\mathcal{O}_K) \to \mathbb{Q}^*$.

**Theorem 4.3.3.** The class group of $\mathcal{O}_K$ is finite. Furthermore, every ideal class contains a representative $\mathfrak{a}$ with

$$N(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}.$$

*Proof.* We claim that for every $M > 0$ there exist only finitely many non-zero ideals $\mathfrak{a} \lhd \mathcal{O}_K$ with $N(\mathfrak{a}) \leq M$. Indeed, suppose that $|\mathcal{O}_K/\mathfrak{a}| \leq M$. Then $M! \cdot \mathcal{O}_K/\mathfrak{a} = 0$, therefore

$$M! \cdot \mathcal{O}_K \subseteq \mathfrak{a} \subseteq \mathcal{O}_K.$$

But as $\mathcal{O}_K/M!\mathcal{O}_K$ is finite, there are only finitely many possible $\mathfrak{a}$ satisfying the above condition.

It now suffices to show the above bound. Let $\mathfrak{a}_0 \lhd \mathcal{O}_K$ be a representative of an ideal class and let $\mathfrak{b} = \alpha\mathfrak{a}_0^{-1}$ be an ideal. By Minkowski's theorem, there exists an element $\beta \in \mathfrak{b}$ with

$$\left|N^K(\beta)\right| \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\mathrm{disc}(\mathfrak{b})|}.$$

As $\mathrm{disc}(\mathfrak{b}) = \mathrm{disc}(K) \cdot N(\mathfrak{b})^2$, we get

$$N\left(\beta\mathfrak{b}^{-1}\right) = \left|N^K(\beta)\right| \cdot N(\mathfrak{b})^{-1} \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^2 \cdot \sqrt{|\mathrm{disc}(K)|}.$$

But since $[\beta\mathfrak{b}^{-1}] = [\mathfrak{a}_0]$, this ideal satisfies our conditions. □

**Definition 4.3.4.** The *class number* of $\mathcal{O}_K$ is defined as the size of its class group, that is $h_K = |\mathcal{C}(\mathcal{O}_K)|$.

**Theorem 4.3.5** (Minkowski)**.** If $n = [K : \mathbb{Q}] \geq 2$, then

$$|\mathrm{disc}(K)| \geq \left(\frac{\pi^s n^n}{4^s n!}\right)^2 > 1.$$

Furthermore, the lower bound diverges as $n \to \infty$.

*Proof.* By Minkowski's theorem, there exists an element $\alpha \in \mathcal{O}_K$ with

$$\left|N^K(\alpha)\right| \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\mathrm{disc}(K)|}.$$

Since $\left|N^K(\alpha)\right| \geq 1$, we get

$$|\mathrm{disc}(K)| \geq \left(\frac{n^n}{n!}\right)^2 \cdot \left(\frac{\pi}{4}\right)^{2s} \geq \left(\frac{n^n}{n!}\right)^2 \cdot \left(\frac{\pi}{4}\right)^n = f(n).$$

Since $f(2) = \frac{\pi^2}{4} > 2$ and

$$\frac{f(n+1)}{f(n)} = \frac{\pi}{4} \cdot \left(\frac{n+1}{n}\right)^{2n} \geq \frac{3\pi}{4} > 1$$

by Bernoulli's inequality, the lower bound indeed diverges and is greater than 1. □

**Theorem 4.3.6** (Hermite)**.** For all $D \geq 0$ there exist only finitely many number fields $K$ with $|\mathrm{disc}(K)| \leq D$.

April 26, 2024

*Proof.* By Minkowski's theorem, it suffices to show that there exist only finitely many number fields $K$ with $\operatorname{disc}(K) = d$ and $[K : \mathbb{Q}] = n$. This is clear for $n = 1$, hence assume $n > 1$.

First note that there exists some $\alpha \in \mathcal{O}_K \setminus \{0\}$ such that $|\sigma_1(\alpha)| < \sqrt{d}+1$ and $|\sigma_i(\alpha)| < 1$ for $i \geq 2$ by theorem 4.2.3. But then all conjugates of $\alpha$ are bounded in terms of $d$, hence so are the coefficients of its minimal polynomial. Therefore there are only finitely many such $\alpha$ for fixed $n$.

Next, we show that $K = \mathbb{Q}(\alpha)$, which shows that there are only finitely many such number fields. We split two cases.

i) Suppose that $r > 0$. Then

$$|\sigma_1(\alpha)| = \left|N^K(\alpha)\right| \cdot \prod_{i=2}^{n} |\sigma_i(\alpha)|^{-1} > \left|N^K(\alpha)\right| \geq 1.$$

Now consider $\sigma_1|_{\mathbb{Q}(\alpha)} \in \operatorname{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \mathbb{C})$. It has exactly $[K : \mathbb{Q}(\alpha)]$ extensions to an element of $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. Since $|\tilde{\sigma}_1(\alpha)| = |\sigma_1(\alpha)| > 1$, we must have $\tilde{\sigma}_1 = \sigma_1$ and so $[K : \mathbb{Q}(\alpha)] = 1$.

ii) Now suppose that $r = 0$. Modifying the proof of theorem 4.2.3, we can further take $|\operatorname{Re}\sigma_1(\alpha)| < 1$ and $|\operatorname{Im}\sigma_1(\alpha)| < C\sqrt{d}$ for some constant $C$. Then

$$|\sigma_1(\alpha)|^2 = \left|N^K(\alpha)\right| \cdot \prod_{i=2}^{n} |\sigma_i(\alpha)|^{-2} > \left|N^K(\alpha)\right| \geq 1.$$

Again consider $\sigma_1|_{\mathbb{Q}(\alpha)} \in \operatorname{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \mathbb{C})$. As above, we see that every extension satisfies $|\tilde{\sigma}_1(\alpha)| = |\sigma_1(\alpha)| > 1$, therefore $\tilde{\sigma}_1 \in \{\sigma_1, \overline{\sigma}_1\}$. Since they differ in $\alpha$ by our modified assumptions, only one extends $\sigma_1|_{\mathbb{Q}(\alpha)}$ and so $[K : \mathbb{Q}(\alpha)] = 1$. □

**Remark 4.3.6.1.** A *Pisot number* is a real algebraic integer $\alpha > 1$ whose all conjugates have absolute value less than 1.

## 4.4 Dirichlet's unit theorem

**Definition 4.4.1.** Let $K$ be a number field. We denote the set of all roots of unity in $K$ by $\mu(K)$.

**Definition 4.4.2.** We define a map $\lambda\colon \mathcal{O}_K^* \to \mathbb{R}^{r+s}$ as

$$\lambda(\alpha) = \left(\log\left|\sigma_1(\alpha)\right|, \dots, \log\left|\sigma_r(\alpha)\right|, 2\log\left|\sigma_{r+1}(\alpha)\right|, \dots, 2\log\left|\sigma_{r+s}(\alpha)\right|\right).$$

**Remark 4.4.2.1.** Note that $\lambda\colon (\mathcal{O}_K^*, \cdot) \to (\mathbb{R}, +)$ is a group homomorphism.

**Lemma 4.4.3.** The set $\lambda\left(\mathcal{O}_K^*\right)$ is a lattice in the hyperplane

$$H = \left\{x \in \mathbb{R}^{r+s} \;\middle|\; \sum_{i=1}^{r+s} x_i = 0\right\}.$$

*Proof.* It clearly suffices to show that $\lambda\left(\mathcal{O}_K^*\right)$ is discrete. That is, there exists a neighbourhood of 0 containing only finitely many points in this set.

Let $B = [-C, C]^{r+s}$. Clearly, $j\left(\lambda^{-1}(B)\right)$ is bounded. Since $j(\mathcal{O}_K)$ is a lattice, $\lambda^{-1}(B)$ is finite and hence so is $B \cap \lambda(\mathcal{O}_K^*)$. $\square$

**Lemma 4.4.4.** We have $\ker\lambda = \mu(K)$, which is a finite cyclic group.

*Proof.* First note that if $\zeta \in \mu(K)$, then clearly $|\sigma_i(\zeta)| = 1$ and so $\lambda(\zeta) = 0$. As $\lambda(\ker(\lambda))$ is trivially bounded, the proof of the previous lemma shows that $\ker\lambda$ is finite. This means that every element of $\ker\lambda$ has finite order and is therefore a root of unity. As every finite multiplicative subgroup of a field is cyclic, the conclusion follows. $\square$

**Proposition 4.4.5.** We have $\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^t$ for some $t \le r + s - 1$.

*Proof.* The short exact sequence

$$1 \longrightarrow \mu(K) \hookrightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \mathbb{Z}^t \longrightarrow 0$$

is exact and therefore splits. $\square$

**Lemma 4.4.6.** Let $M \ge 0$. Up to associativity, there exist only finitely many elements $\alpha \in \mathcal{O}_K$ with $\left|N^K(\alpha)\right| < M$.

*Proof.* The condition is equivalent to $N((\alpha)) < M$, but there are only finitely many such ideals. $\square$

**Theorem 4.4.7** (Dirichlet's unit theorem)**.** Let $K$ be a number field. Then $\mu(K)$ is a finite cyclic group and $\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^{r+s-1}$.

*Proof.* We already know that $\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^t$ and that $\mu(K)$ is cyclic. It is therefore enough to show that $t = r + s - 1$. To do so, we will show that $\lambda\left(\mathcal{O}_K^*\right) \subseteq H$ is a complete lattice. Equivalently, we need to show that $H/\lambda\left(\mathcal{O}_K^*\right)$ has a bounded system of representatives.

Set $g(x) = (|\sigma_1(x)|, \dots, |\sigma_{r+s}(x)|)$ and $l(x) = (\log x_1, \dots, \log x_r, 2\log x_{r+1}, \dots, 2\log x_{r+s})$, so that $\lambda = l \circ g$. Furthermore, let

$$\|x\| = \prod_{i=1}^{r} x_i \cdot \prod_{i=1}^{s} x_{r+i}^2.$$

Then $\|g(x)\| = 1$ for all $x \in \mathcal{O}_K^*$. Finally, set $S = l^{-1}(H)$.

We claim that there exists a bounded set $T \subseteq S$ such that

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} g(\varepsilon)T.$$

To see this, choose $c \in (\mathbb{R}^+)^{r+s}$ such that

$$\|c\| > \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|\mathrm{disc}(K)|}$$

and set

$$X = \left\{ x \in \left(\mathbb{R}^+\right)^{r+s} \;\middle|\; \forall i \colon x_i < c_i \right\}.$$

Note that, for any $y \in S$, we have $\|cy^{-1}\| = \|c\|$. By theorem 4.2.3 there exists a non-zero element $\alpha \in \mathcal{O}_K$ with $g(\alpha) \in yX$. This element also satisfies $\left|N^K(\alpha)\right| \le \|c\|$. There are only finitely many such elements up to associativity – denote them by $\alpha_1, \dots, \alpha_m$.

We claim that

$$T = S \cap \bigcup_{i=1}^{m} g(\alpha_i)^{-1} X$$

satisfies the conditions. Indeed, it is clearly bounded. For any $y \in S$, and set $g(\alpha) = y^{-1}x$ for some $\alpha \in \mathcal{O}_K$ and $x \in X$, where $\left|N^K(\alpha)\right| \le \|c\|$. This means that $\varepsilon = \alpha^{-1} \cdot \alpha_i \in \mathcal{O}_K^*$ for some $i \le m$. Hence

$$y = g(\alpha)^{-1}x = g\left(\alpha_i \cdot \varepsilon^{-1}\right)^{-1} x = g(\varepsilon) \cdot g(\alpha_i)^{-1} x \in g(\varepsilon)T,$$

as required.

For each $x \in T$, we now have that $x_i$ are bounded from above. But as $\|x\| = 1$, they are also bounded from below. The set $l(T)$ is therefore bounded, but as

$$H = l(S) = \bigcup_{\varepsilon \in \mathcal{O}_K^*} l(g(\varepsilon)T) = \bigcup_{\varepsilon \in \mathcal{O}_K^*} \left(\lambda(\varepsilon) + l(T)\right),$$

the set $l(T)$ is a bounded set of representatives for $H / \lambda(\mathcal{O}_K^*)$. □

# 5 Decomposition of primes in extensions

*The even case is a bit more odd.*
– gost. izr. prof. dr. rer. nat. Daniel Smertnig

## 5.1 Prime ideals in extensions

**Lemma 5.1.1.** Let $K \subseteq L$ be number fields, $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ and $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$. Then

$$\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L \iff \mathfrak{p} \subseteq \mathfrak{P} \iff \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}.$$

*Proof.* Suppose first that $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$. Then we have $\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}$.

Now suppose that $\mathfrak{p} \subseteq \mathfrak{P}$. Then as $\mathfrak{p} \subseteq \mathfrak{P} \cap \mathcal{O}_K$ is a maximal ideal, it must be equal to this intersection.

Finally, suppose that the last condition holds. Then

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P} \cap \mathcal{O}_K)\,\mathcal{O}_L \subseteq \mathfrak{P}\mathcal{O}_L = \mathfrak{P}.$$ □

**Definition 5.1.2.** If any of the above conditions hold, we say that $\mathfrak{P}$ *lies over* $\mathfrak{p}$. Similarly, $\mathfrak{p}$ *lies under* $\mathfrak{P}$.

**Lemma 5.1.3.** Every $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ lies over a unique $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$.

*Proof.* Uniqueness follows from the previous lemma, therefore we only need to show that $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ is a prime ideal. To see that it is non-empty, apply lemma 3.1.2. Now it is clear that it is a prime ideal by definition. □

**Remark 5.1.3.1.** By lemma 3.1.2, the quotient ${}^{\mathcal{O}_L}/_{\mathfrak{p}\mathcal{O}_L}$ is finite, therefore each prime ideals lies under at most finitely many prime ideals.

**Remark 5.1.3.2.** The ring homomorphism $\mathcal{O}_K \hookrightarrow \mathcal{O}_L \to {}^{\mathcal{O}_L}/_{\mathfrak{P}}$ induces a field embedding ${}^{\mathcal{O}_K}/_{\mathfrak{p}} \to {}^{\mathcal{O}_L}/_{\mathfrak{P}}$.

**Definition 5.1.4.** Let $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.

i) The quotient ${}^{\mathcal{O}_L}/_{\mathfrak{P}}$ is the *residue field* of $\mathfrak{P}$.

ii) The number $[{}^{\mathcal{O}_L}/_{\mathfrak{P}} : {}^{\mathcal{O}_K}/_{\mathfrak{p}}]$ is the *inertia degree*, which we denote by $f = f(\mathfrak{P} \mid \mathfrak{p})$.

iii) The multiplicity $\nu_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_L)$ of $\mathfrak{P}$ in $\mathfrak{p}\mathcal{O}_L$ is the *ramification index* of $\mathfrak{P}$, which we denote by $e = e(\mathfrak{P} \mid \mathfrak{p})$.

**Theorem 5.1.5.** Let $n = [L : K]$, where $K \subseteq L$ are number fields. Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ and $\mathfrak{P}_1, \dots, \mathfrak{P}_r \in \mathcal{P}(\mathcal{O}_L)$ be the distinct prime ideals over $\mathfrak{p}$. Denote by $e_i = e(\mathfrak{P}_i \mid \mathfrak{p})$ and $f_i = f(\mathfrak{P}_i \mid \mathfrak{p})$. Then

$$\sum_{i=1}^{r} e_i f_i = n.$$

*Proof.* Let $\kappa = {}^{\mathcal{O}_K}/_{\mathfrak{p}}$. Let $\alpha_1, \dots, \alpha_m \in \mathcal{O}_L$ be such that $\overline{\alpha}_1, \dots, \overline{\alpha}_m \in {}^{\mathcal{O}_L}/_{\mathfrak{p}\mathcal{O}_L}$ is a $\kappa$-basis.

Suppose that
$$\sum_{i=1}^{m} c_i\alpha_i = 0$$
where $c_i \in K$ are not all equal to 0. By clearing denominators, we can take $c_i \in \mathcal{O}_K$. Denote
$$0 \neq \mathfrak{c} = \langle c_1, \dots, c_m \rangle_{\mathcal{O}_K} \triangleleft \mathcal{O}_K$$
and let $d \in \mathfrak{c}^{-1} \setminus \mathfrak{c}^{-1}\mathfrak{p}$. Then
$$\sum_{i=1}^{m} dc_i\alpha_i = 0$$
and all $dc_i$ are elements of $\mathcal{O}_K$, but $dc_i \notin \mathfrak{p}$ for some index $i$. It follows that
$$\sum_{i=1}^{r} \overline{dc_i}\overline{\alpha}_i = 0,$$
which is a contradiction.

Now let $M = \langle \alpha_1, \dots, \alpha_m \rangle_{\mathcal{O}_K}$ and write $N = \mathcal{O}_L/M$ as a $\mathcal{O}_K$-module. Note that, by the choice of $\alpha_i$, $\mathcal{O}_L = M + \mathfrak{p}\mathcal{O}_L$ holds. We can check that $N = \mathfrak{p}N$.

As $\mathcal{O}_L$ is a finitely generated $\mathbb{Z}$-module, it is finitely generated as a $\mathcal{O}_K$-module. Denote $N = \langle \beta_1, \dots, \beta_s \rangle_{\mathcal{O}_K}$. Note that we can write
$$\beta_i = \sum_{j=1}^{s} c_{i,j}\beta_j$$
for $c_{i,j} \in \mathfrak{p}$. Let $C = \left[c_{i,j}\right]_{i,j}$. It follows that $(C - I)\beta = 0$. By construction we have $d = \det(C - I) = (-1)^s \pmod{\mathfrak{p}}$, hence
$$d\beta = \operatorname{adj}(C - I) \cdot (C - I)\beta = 0$$
and so $d\beta_i = 0$ for all $i$. By definition, it follows that $dN = 0$, therefore $d\mathcal{O}_L \subseteq M$. But then
$$L = dL = d\,\langle \mathcal{O}_L \rangle_K \subseteq \langle M \rangle_K = \langle \alpha_1, \dots, \alpha_m \rangle_K\,,$$
therefore $\{\alpha_i \mid i \leq m\}$ is a $K$-basis of $L$.

In particular, $\dim_\kappa \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \dim_K L = n$. But then
$$N(\mathfrak{p}\mathcal{O}_L) = \left|\mathcal{O}_L\big/\mathfrak{p}\mathcal{O}_L\right| = |\kappa|^n = N(\mathfrak{p})^n,$$
and
$$N(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^{r} N(\mathfrak{P}_i)^{e_i} = \prod_{i=1}^{r} N(\mathfrak{p})^{e_if_i}.$$ □

**Definition 5.1.6.** The *conductor* of $\mathcal{O}_K[\alpha]$ in $\mathcal{O}_L$ is the set
$$\mathfrak{f} = \{\beta \in \mathcal{O}_L \mid \beta\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]\}\,.$$

**Remark 5.1.6.1.** The conductor is the largest common ideal of $\mathcal{O}_L$ and $\mathcal{O}_K[\alpha]$.

**Lemma 5.1.7.** If $\alpha \in \mathcal{O}_L$, then the minimal polynomial $g$ of $\alpha$ over $K$ has coefficients in $\mathcal{O}_K$.

*Proof.* Denote $n = [K(\alpha) : K]$ and let $\operatorname{Hom}_K(K(\alpha), \mathbb{C}) = \{\sigma_i \mid i \leq n\}$. Then $\sigma_i(\alpha)$ are algebraic conjugates of $\alpha$ and therefore algebraic integers. It follows that the coefficients of $g$ are algebraic integers as well by Vieta's formulae. As they are contained in $K$ by definition, the coefficients are elements of $\mathcal{O}_K$. □

**Theorem 5.1.8** (Dedekind-Kummer)**.** Let $\alpha \in \mathcal{O}_L$ be an element such that $L = K(\alpha)$ and let $\mathfrak{f}$ be the conductor of $\mathcal{O} = \mathcal{O}_K[\alpha]$ in $\mathcal{O}_L$. Let $g \in \mathcal{O}_K[x]$ be the minimal polynomial of $\alpha$ over $K$ and let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ be coprime to $\mathfrak{f} \cap \mathcal{O}_K$. Suppose that monic polynomials $g_1, \dots, g_r \in \mathcal{O}_K[x]$ and integers $e_1, \dots, e_r \in \mathbb{N}$ are such that

$$\overline{g} = \prod_{i=1}^{r} \overline{g}_i^{e_i}$$

is the prime factorisation of $\overline{g}$ in $\mathcal{O}_K/\mathfrak{p}\,[x]$. Finally, for $i \leq r$, let $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$. Then $\mathfrak{P}_i$ are the prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$, $e_i = e(\mathfrak{P}_i \mid \mathfrak{p})$ and $\deg g_i = f(\mathfrak{P}_i \mid \mathfrak{p})$.

*Proof.* Denote $\kappa = \mathcal{O}_K/\mathfrak{p}$. Consider the homomorphism $\varphi\colon \mathcal{O} \hookrightarrow \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. By assumption, we have $\mathfrak{p} + (\mathfrak{f} \cap \mathcal{O}_K) = \mathcal{O}_K$, therefore $\mathfrak{p}\mathcal{O}_L + \mathfrak{f} = \mathcal{O}_L$. Since $\mathfrak{f} \subseteq \mathcal{O}$, $\varphi$ is surjective. Note that $\ker \varphi = \mathcal{O} \cap \mathfrak{p}\mathcal{O}_L$. As $\mathfrak{p}\mathcal{O} + \mathfrak{f} = \mathcal{O}$, we have

$$\ker \varphi = \mathfrak{p}\mathcal{O}_L \cap \mathcal{O} = (\mathfrak{p}\mathcal{O} + \mathfrak{f})\,(\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}) \subseteq \mathfrak{p}\mathcal{O},$$

therefore $\ker \varphi = \mathfrak{p}\mathcal{O}$ and so

$$\mathcal{O}_L \big/ \mathfrak{p}\mathcal{O}_L \cong \mathcal{O} \big/ \mathfrak{p}\mathcal{O}\,.$$

But as

$$\mathcal{O} \big/ \mathfrak{p}\mathcal{O} \cong \mathcal{O}_K[x] \big/ (\mathfrak{p}, g) \cong \mathcal{O}_K/\mathfrak{p}\,[x] \big/ (g)\,,$$

we in fact have

$$\mathcal{O}_L \big/ \mathfrak{p}\mathcal{O}_L \cong \kappa[x] \big/ (\overline{g})\,.$$

By the Chinese remainder theorem, we can further write

$$R = \kappa[x] \big/ (\overline{g}) \cong \prod_{i=1}^{r} \kappa[x] \big/ (\overline{g}_i^{e_i})$$

The ideals of each component are precisely $\left(\overline{g}_i^j\right)$ for some $j \leq e_i$, therefore $R$ has precisely $r$ maximal ideals. Denote them by $\mathfrak{m}_i$. Note that

$$\dim_\kappa R \big/ \mathfrak{m}_i = \dim_\kappa \kappa[x] \big/ (\overline{g}_i) = \deg(g_i)$$

and

$$\bigcap_{i=1}^{r} \mathfrak{m}_i^{e_i} = \{0\}\,.$$

Let now $\overline{\mathfrak{P}}_i$ be the preimages of $\mathfrak{m}_i$ under the above ring isomorphism – it therefore has the same properties as described above. Furthermore, $\mathfrak{P}_i$ are precisely the preimages of $\overline{\mathfrak{P}}_i$ under the homomorphism $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. They are the maximal ideals containing $\mathfrak{p}\mathcal{O}_L$ and

$$f(\mathfrak{P}_i \mid \mathfrak{p}) = \left[\mathcal{O}_L \big/ \mathfrak{P}_i : \kappa\right] = \deg\left(\overline{g}_i\right) = f_i.$$

We can easily check that $\mathfrak{P}_i^{e_i}$ are the preimages of $\overline{\mathfrak{P}}_i$, therefore

$$\prod_{i=1}^r \mathfrak{P}_i^{e_i} = \cap_{i=1}^r \mathfrak{P}_i^{e_i} \subseteq \mathfrak{p}\mathcal{O}_L.$$

We can therefore write

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{P}_i^{m_i},$$

but as

$$n = \sum_{i=1}^r m_i f_i \le \sum_{i=1}^r e_i f_i = \deg g = n,$$

we in fact have $m_i = e_i$. □

**Definition 5.1.9.** Let $K \subseteq L$ be number fields with $n = [L : K]$. Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ be such that

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{P}^{e_i}$$

is a factorisation in $\mathcal{O}_L$. Denote $f_i = f(\mathfrak{P} \mid \mathfrak{p})$ and $e_i = e(\mathfrak{P}_i \mid \mathfrak{p})$.

i) The ideal $\mathfrak{p}$ is *completely split*[5] if $r = n$.

ii) The ideal $\mathfrak{p}$ is *non-split* if $r = 1$.

iii) The ideal $\mathfrak{p}$ is *inert* if $\mathfrak{p}\mathcal{O}_L$ is a prime ideal (equivalently, $r = e_1 = 1$ and $f_1 = n$).

iv) The ideal $\mathfrak{P}_i$ is *unramified* over $K$ if $e_i = 1$ and *ramified* if $e_i > 1$.

v) The ideal $\mathfrak{P}_i$ is *totally ramified* over $K$ if $e_i > 1$ and $f_i = 1$.

vi) The ideal $\mathfrak{p}$ is *unramified* in $L$ if all $\mathfrak{P}_i$ are unramified and *ramified* otherwise.

**Remark 5.1.9.1.** The elements of $\operatorname{Gal}(L/K)$ permute prime ideals lying over $\mathfrak{p}$.

**Theorem 5.1.10.** Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ and let $p \in \mathbb{P}$ be such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. If $\mathfrak{p}$ is ramified in $L$, then $p \mid \operatorname{disc}(L)$. In particular, only finitely many primes of $\mathcal{O}_K$ ramify in $L$.

*Proof.* Note that if $\mathfrak{p}$ is ramified in $L$, then $p\mathbb{Z}$ is also ramified in $L$. Since the set $\{\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K) \mid \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}\}$ is finite for a fixed prime $p$, it suffices to consider $K = \mathbb{Q}$.

Let now $p \in \mathbb{P}$ be a prime number and $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_L)$ be a prime ideal with $p\mathbb{Z} \subseteq \mathfrak{p}$. Set $e = e(\mathfrak{p} \mid p\mathbb{Z}) > 1$. Write $p\mathcal{O}_L = \mathfrak{p}\mathfrak{a}$ for an ideal $\mathfrak{a} \triangleleft \mathcal{O}_L$ and let $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathcal{P}(\mathcal{O}_L)$ be the prime ideals lying over $p\mathcal{O}_L$. Since $e > 1$, we have

$$\mathfrak{a} \subseteq \bigcap_{i=1}^r \mathfrak{p}_i.$$

Let $\alpha_1, \dots, \alpha_n$ be an integral basis of $\mathcal{O}_L$ and choose an element $\alpha \in \mathfrak{a} \setminus p\mathcal{O}_L$. We can write

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

[5] Also *totally split*.

where $p \nmid c_i$ for some $i$. Without loss of generality let $i = 1$. Consider now

$$A = \langle \alpha, \alpha_2, \ldots, \alpha_n \rangle_{\mathbb{Z}} = \langle c_1\alpha_1, \alpha_2, \ldots, \alpha_n \rangle_{\mathbb{Z}} \subseteq \mathcal{O}_L.$$

As

$$\operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n) = |\mathcal{O}_L : A|^2 \cdot \operatorname{disc}(\mathcal{O}_L) = c_1^2 \cdot \operatorname{disc}(\mathcal{O}_L),$$

it suffices to show that $p \mid d = \operatorname{disc}(\alpha, \alpha_2, \ldots, \alpha_n)$.

Let $N/L$ be a finite extension such that $N/\mathbb{Q}$ is Galois. Now we can extend the $n = [L : \mathbb{Q}]$ embeddings of $L$ into $\mathbb{C}$ to automorphisms $\sigma_i \in \operatorname{Gal}(N/\mathbb{Q})$. For any $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_N)$ lying over $p\mathbb{Z}$, the ideal $\mathfrak{P} \cap \mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$ lying over $p\mathbb{Z}$, hence $\alpha \in \mathfrak{P} \cap \mathcal{O}_L$. In particular, $\alpha$ is contained in every prime ideal of $\mathcal{O}_N$ lying over $p\mathbb{Z}$.

Fix a prime ideal $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_N)$ lying over $p\mathbb{Z}$. For any $\sigma \in \operatorname{Gal}(N/\mathbb{Q})$, the set $\sigma^{-1}(\mathfrak{P})$ is another such prime ideal, meaning $\alpha \in \sigma(\mathfrak{P})$. By the definition of the discriminant, we get $d \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$, hence $p \mid d$. $\square$

## 5.2 Quadratic fields, quadratic reciprocity and cyclotomic fields

**Theorem 5.2.1.** Let $K = \mathbb{Q}\left(\sqrt{d}\right)$, where $d \neq 1$ is a square-free integer.

i) Let $p$ be an odd prime. The prime factorisation of $p\mathcal{O}_K$ is of the following form:

(a) If $p \nmid d$ and $d \equiv b^2 \pmod{p}$, then $p\mathcal{O}_K = \left(p, \sqrt{d}+b\right)\left(p, \sqrt{d}-b\right)$.

(b) If $d$ is a non-square modulo $p$, then $p\mathcal{O}_K$ is a prime ideal.

(c) If $p \mid d$, then $p\mathcal{O}_K = \left(p, \sqrt{d}\right)^2$.

ii) The prime factorisation of $2\mathcal{O}_K$ is of the following form:

(a) If $2 \mid d$, then $2\mathcal{O}_K = \left(2, \sqrt{d}\right)^2$.

(b) If $d \equiv 3 \pmod{4}$, then $2\mathcal{O}_K = \left(2, 1+\sqrt{d}\right)^2$.

(c) If $d \equiv 1 \pmod{8}$, then $2\mathcal{O}_K = \left(2, \frac{1+\sqrt{d}}{2}\right)\left(2, \frac{1-\sqrt{d}}{2}\right)$.

(d) If $d \equiv 5 \pmod{8}$, then $2\mathcal{O}_K$ is a prime ideal.

*Proof.*

i) Note that $\mathfrak{f} \cap \mathbb{Z} \in \{\mathbb{Z}, 2\mathbb{Z}\}$, which is coprime to $p\mathbb{Z}$.

(a) We can factor
$$x^2 - \overline{d} = \left(x - \overline{b}\right)\left(x + \overline{b}\right) \in \mathbb{F}_p[x].$$
As $p$ is odd, the factors are distinct. The conclusion follows from theorem 5.1.8.

(b) Note that $x^2 - \overline{d}$ is irreducible in $\mathbb{F}_p[x]$ and apply theorem 5.1.8.

(c) The polynomial $x^2$ factors trivially, so we can again apply theorem 5.1.8.

ii)

(a) Note that $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{d}\right]$ and $\mathfrak{f} = \mathcal{O}_K$. We can therefore again apply theorem 5.1.8 with the trivial factorisation.

(b) Same as the previous case.

(c) Now $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. The minimal polynomial is therefore given by
$$g(x) = x^2 - x + \frac{1-d}{4}.$$
Since $d \equiv 1 \pmod{8}$, we have $\overline{g}(x) = x(x-1) \in \mathbb{F}_2[x]$. Now apply theorem 5.1.8.

(d) Same as the previous case, but now $\overline{g}(x) = x^2 + x + \overline{1}$ is irreducible. $\square$

**Definition 5.2.2.** Let $p$ be a prime number. An integer $a$ is a *quadratic residue* modulo $p$ if $a \equiv b^2 \pmod{p}$ for some integer $b$. We define the *Legendre symbol* as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1, & p \nmid a \text{ and } a \text{ is a quadratic non-residue modulo } p, \\ 0, & p \mid a. \end{cases}$$

**Remark 5.2.2.1.** For $p \neq 2$, then $\left(\mathbb{F}_p^*\right)^2$ is the unique subgroup of index 2 of $\mathbb{F}_p^*$. From this we deduce that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

In particular, $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^* \to S^0$ is a group homomorphism with kernel $\left(\mathbb{F}_p^*\right)^2$.

**Lemma 5.2.3.** Let $p$ be an odd prime and $a \in \mathbb{Z}$. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

*Proof.* The group $\mathbb{F}_p^*$ is cyclic with order $p-1$, and the generator maps to $-1$ under both homomorphisms. □

**Theorem 5.2.4** (Quadratic reciprocity law)**.** Let $p$ and $q$ be distinct odd primes. Then

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

*Proof.* Let $\zeta \in \mu_p^*(\mathbb{C})$. The following calculations are all done in $\mathbb{Z}[\zeta]$.

Define the Gauss sum

$$\tau = \sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) \zeta^a = \sum_{j=1}^{n-1} \left(\frac{j}{p}\right) \zeta^j.$$

Let $c$ be a quadratic non-residue modulo $p$. Then

$$-\sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) = \left(\frac{c}{p}\right) \cdot \sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) = \sum_{a \in \mathbb{F}_p^*} \left(\frac{ac}{p}\right) = \sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right),$$

therefore

$$\sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) = 0.$$

Also, recall that

$$\sum_{a \in \mathbb{F}_p^*} \zeta^{ab} = -1$$

for all $b \in \mathbb{F}_p^*$, as $\zeta^b$ is also a primitive root of unity. As $\left(\frac{a}{p}\right) = \left(\frac{a^{-1}}{p}\right)$, we find that

$$\begin{aligned}
\tau^2 &= \sum_{a,b \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \zeta^{a+b} \\
&= \left(\frac{-1}{p}\right) \cdot \sum_{a,b \in \mathbb{F}_p^*} \left(\frac{ab^{-1}}{p}\right) \zeta^{a-b} \\
&= \left(\frac{-1}{p}\right) \cdot \sum_{b,c \in \mathbb{F}_p^*} \left(\frac{c}{p}\right) \zeta^{cb-b} \\
&= \left(\frac{-1}{p}\right) \cdot \left( \sum_{b \in \mathbb{F}_p^*} 1 + \sum_{\substack{c \in \mathbb{F}_p^* \\ c \neq 1}} \left(\frac{c}{p}\right) \cdot \sum_{b \in \mathbb{F}_p^*} \zeta^{b(c-1)} \right)
\end{aligned}$$

As $c - 1 \neq 0$ in the innermost sum, we can further compute

$$\begin{aligned} \tau^2 &= \left(\frac{-1}{p}\right) \cdot \left(p - 1 - \sum_{\substack{c \in \mathbb{F}_p^* \\ c \neq 1}} \left(\frac{c}{p}\right)\right) \\ &= p \cdot \left(\frac{-1}{p}\right). \end{aligned}$$

In $\mathbb{Z}_q[\zeta]$ we can now compute

$$\tau^q = \tau \cdot \left((-1)^{\frac{p-1}{2}} \cdot p\right)^{\frac{q-1}{2}} = \tau \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right)$$

and

$$\tau^q = \sum_{a \in \mathbb{F}_p^*} \left(\frac{a}{p}\right) \zeta^{aq} = \left(\frac{q}{p}\right) \cdot \sum_{a \in \mathbb{F}_p^*} \left(\frac{aq}{p}\right) \zeta^{aq} = \left(\frac{q}{p}\right) \tau.$$

Equating and multiplying by $\tau$, we get

$$\left(\frac{-1}{p}\right) p \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right) = \tau^2 \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right) = \tau^2 \cdot \left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right) \cdot p \cdot \left(\frac{q}{p}\right).$$

As $p$ is invertible in $\mathbb{Z}_q[\zeta]$, we get the sought equality. $\square$

**Proposition 5.2.5.** If $p$ is an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

*Proof.* Note that, in $\mathbb{Z}_p[i]$, we have

$$1 + i \cdot (-1)^{\frac{p-1}{2}} = 1 + i^p = (1+i)^p = (1+i) \cdot 2^{\frac{p-1}{2}} \cdot i^{\frac{p-1}{2}} = \left(\frac{2}{p}\right) \cdot (1+i) \cdot i^{\frac{p-1}{2}}.$$

If $p \equiv 1 \pmod 4$, we multiply the above equation by $\frac{1-i}{2}$ to get

$$1 = \left(\frac{2}{p}\right) \cdot (-1)^{\frac{p-1}{4}}$$

in $\mathbb{Z}_p[i]$. Similarly, if $p \equiv 3 \pmod 4$, multiply the equation by $\frac{1+i}{2}$ instead to get

$$1 = \left(\frac{2}{p}\right) \cdot i \cdot i^{\frac{p-1}{2}} = \left(\frac{2}{p}\right) \cdot (-1)^{\frac{p+1}{4}}.$$ $\square$

**Proposition 5.2.6.** Let $p$ be a prime number and $k, m \in \mathbb{N}$ be integers such that $p \nmid m$. Let

$$f = \operatorname{ord}_{\mathbb{Z}_m^*}(\overline{p}) = \min\left\{\ell \in \mathbb{N} \;\middle|\; p^\ell \equiv 1 \pmod m\right\}.$$

i) If $\zeta \in \mathbb{F}_{p^k}$ is a primitive $m$-th root of unity and $g \in \mathbb{F}_p[x]$ is the minimal polynomial of $\zeta$, then

$$\mathbb{F}_p(\zeta) \cong \mathbb{F}_p[x]/(g) \cong \mathbb{F}_{p^f}.$$

In particular, $\deg g = f$.

ii) If $\Phi_m \in \mathbb{Z}[x]$ is the $m$-th cyclotomic polynomial, then

$$\overline{\Phi} = \prod_{i=1}^{r} \overline{g}_i \in \mathbb{F}_p[x]$$

for pairwise distinct monic irreducible polynomials $\overline{g}_i \in \mathbb{F}_p[x]$ with $\deg(\overline{g}_i) = f$ for all $i$.

*Proof.*

i) Note that

$$\mathbb{F}_p(\zeta) \cong \mathbb{F}_p[x]\big/(g)$$

is a finite field, therefore $\mathbb{F}_p(\zeta) \cong \mathbb{F}_{p^k}$ for some $k \geq 1$. Note that $\mathbb{F}_{p^k}^*$ contains a primitive $m$-th root of unity if and only if $p^k \equiv 1 \pmod{m}$. By choice of $f$, we have $f \mid k$ and therefore

$$\mathbb{F}_{p^f} = \left\{x \in \mathbb{F}_{p^k} \;\middle|\; x^{p^f} = x\right\}.$$

By definition of $f$, it contains all $m$-th roots of unity of $\mathbb{F}_{p^k}$, hence $\mathbb{F}_p(\zeta) \subseteq \mathbb{F}_{p^f}$. It follows that $k = f$.

ii) Recall that

$$x^m - 1 = \prod_{\ell \mid m} \Phi_\ell.$$

In particular, every $m$-th root of unity of $\mathbb{F}_{p^f}$ is a root of some cyclotomic polynomial $\overline{\Phi}_\ell \in \mathbb{F}_p[x]$ with $\ell \mid m$. As $\mathbb{F}_{p^f}$ contains precisely $\varphi(\ell)$ primitive $\ell$-th roots of unity, they are exactly the roots of $\overline{\Phi}_\ell$. In particular, $\overline{\Phi}_m$ has no repeated roots in $\mathbb{F}_{p^f}$. We can therefore factor

$$\overline{\Phi}_m = \prod_{i=1}^{r} \overline{g}_i,$$

where each $\overline{g}_i$ is a minimal polynomial of some primitive $m$-th root of unity. In particular, $\deg(\overline{g}_i) = f$. □

**Theorem 5.2.7.** Let $n$ be a natural number and $\zeta \in \mu_n^*(\mathbb{C})$. Denote $K = \mathbb{Q}(\zeta)$ and let $p \in \mathbb{P}$. Let $v = \nu_p(n)$ and denote $m = \frac{n}{p^v}$ and

$$f = \operatorname{ord}_{\mathbb{Z}_m^*}(\overline{p}) = \min\left\{\ell \in \mathbb{N} \;\middle|\; p^\ell \equiv 1 \pmod{m}\right\}.$$

Then $p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p^v)}$ with distinct $\mathfrak{p}_i$ and $f(\mathfrak{p}_i \mid p) = f$.

*Proof.* As the conductor is trivial, we can apply the Dedekind-Kummer theorem to all $p \in \mathbb{P}$. The minimal polynomial of $\zeta$ is of course $\Phi_n$. Recall that

$$\mu_n^*(\mathbb{C}) = \left\{\xi \cdot \omega \;\middle|\; \xi \in \mu_{p^v}^*(\mathbb{C}) \wedge \omega \in \mu_m^*(\mathbb{C})\right\}.$$

For such $\xi$ we have

$$(\xi - 1)^{p^v} \equiv \xi^{p^v} - 1 \equiv 0 \pmod{\mathfrak{p}}$$

for all $\mathfrak{p} \mid p\mathcal{O}_K$, therefore $\xi \equiv 1 \pmod{\mathfrak{p}}$. We can therefore factor

$$\Phi_n = \prod_{\substack{\xi \in \mu_{p^v}^*(\mathbb{C}) \\ \omega \in \mu_m^*(\mathbb{C})}} (x - \xi\omega) \equiv \prod_{\omega \in \mu_m^*(\mathbb{C})} (x - \omega)^{\varphi(p^v)} \equiv \Phi_m^{\varphi(p^v)} \pmod{\mathfrak{p}}.$$

But then $\Phi_n = \Phi_m^{\varphi(p^v)}$ in $\mathbb{F}_p[x]$, hence

$$\overline{\Phi}_n = \prod_{i=1}^{r} \overline{g}_i^{\varphi(p^v)}$$

by the previous proposition. Furthermore, $\overline{g}_i$ are monic, irreducible and distinct with $\deg(\overline{g}_i) = f$. $\square$

**Corollary 5.2.7.1.** A prime $p \neq 2$ is completely split if and only if $p \equiv 1 \pmod{n}$.

**Corollary 5.2.7.2.** A prime number $p \in \mathbb{P}$ is ramified if and only if $p \mid n$, except if $p = 2 = \gcd(n, 4)$.

# 6 Hilbert theory

*The rest of this theorem becomes a sudoku with these numbers.*
– gost. izr. prof. dr. rer. nat. Daniel Smertnig

## 6.1 Decomposition of primes in Galois extensions

**Proposition 6.1.1.** Let $p \in \mathbb{P}$ and $n \geq 1$.

i) The map $\varphi\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, given by $x \mapsto x^p$, is a field automorphism.[6]

ii) The group $\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$ is generated by $\varphi$, which is of order $n$.

iii) We have $m \mid n$ if and only if we can embed $\mathbb{F}_{p^m}$ into $\mathbb{F}_{p^n}$.

iv) Every extension $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is a cyclic Galois group generated by $\varphi^m$.

*Proof.*

i) Note that $(x+y)^p = x^p + y^p$, therefore $\varphi$ is additive and injective.

ii) Recall that $\left|\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)\right| \leq n$, hence we only need to show that $\varphi$ is of order $n$, which is clear by considering the generator of $\mathbb{F}_{p^n}^*$.

iii) By the Galois correspondence, the subfields of $\mathbb{F}_{p^n}$ are precisely $\mathbb{F}_{p^n}^{\langle \varphi^d \rangle}$ for $d \mid n$.

iv) Note that $\mathbb{F}_{p^m} = \mathbb{F}_{p^n}^{\langle \varphi^m \rangle}$, hence $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is Galois with $\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}\right) = \langle \varphi^m \rangle$. □

**Lemma 6.1.2.** Let $K \subseteq L$ be number fields and suppose that $L/K$ is Galois. Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$. Then $G = \mathrm{Gal}\left(L/K\right)$ acts transitively on $\{\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L \mid \mathfrak{P} \mid \mathfrak{p}\}$.

*Proof.* Suppose that $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$ and that $\mathfrak{P}'$ is not in the orbit of $\mathfrak{P}$. In particular, $\mathfrak{P}'$ is comaximal to each $\sigma(\mathfrak{P})$. By the Chinese remainder theorem, there exists some $\alpha \in \mathcal{O}_L$ such that $\alpha \equiv 0 \pmod{\mathfrak{P}'}$ and $\alpha \equiv 1 \pmod{\sigma(\mathfrak{P})}$ for all $\sigma \in G$. But then

$$N_K^L(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$$

and $\sigma(\alpha) \notin \mathfrak{P}$ for all $\sigma$. As $\mathfrak{P}$ is prime, it follows that $N_K^L(\alpha) \notin \mathfrak{P}$, which is a contradiction. □

**Proposition 6.1.3.** Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$. Furthermore, let $\mathfrak{P}$ and $\mathfrak{P}'$ be prime ideals of $\mathcal{O}_L$ with $\mathfrak{P}, \mathfrak{P}' \mid \mathfrak{p}$.

i) We have $e(\mathfrak{P} \mid \mathfrak{p}) = e(\mathfrak{P}' \mid \mathfrak{p})$.

ii) We have $\mathcal{O}_L/\mathfrak{P} \cong \mathcal{O}_L/\mathfrak{P}'$ as $\mathcal{O}_K/\mathfrak{p}$-algebras. In particular, $f(\mathfrak{P} \mid \mathfrak{p}) = f(\mathfrak{P}' \mid \mathfrak{p})$.

[6] This is the Frobenius automorphism.

*Proof.*

i) Let

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

and denote $\mathfrak{P} = \mathfrak{P}_1$. Let $\sigma$ be an automorphism such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Then

$$\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{P}_i^{e_1} \prod_{i=2}^{r} \sigma(\mathfrak{P}_i)^{e_i}.$$

ii) Note that $\sigma$ induces a homomorphism $\mathcal{O}_L \to {\mathcal{O}_L}\big/{\sigma(\mathfrak{P}}$ by $\alpha \mapsto \sigma(\alpha) + \sigma(\mathfrak{P})$. As its kernel is $\mathfrak{P}$, we get $\mathcal{O}_L/\mathfrak{P} \cong \mathcal{O}_L/\mathfrak{P}'$. $\square$

**Definition 6.1.4.** Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ and $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be such that $\mathfrak{P} \mid \mathfrak{p}$. Then

$$D(\mathfrak{P}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

is the *decomposition group* of $\mathfrak{P}$. The fixed field $L^{D(\mathfrak{P})}$ is the *decomposition field* of $\mathfrak{P}$.

**Remark 6.1.4.1.** As $G$ acts transitively, we have $[G : D(\mathfrak{P})] = r = [L^{D(\mathfrak{P})} : K]$. In particular, $\mathfrak{p}$ is non-split if and only if $L^{D(\mathfrak{P})} = K$ and is completely split if and only if $L^{D(\mathfrak{P})} = L$.

**Remark 6.1.4.2.** Every $\sigma \in D(\mathfrak{P})$ induces an automorphism $\overline{\sigma}$ of $\mathcal{O}_L/\mathfrak{P}$ by $\alpha + \mathfrak{P} \mapsto \sigma(\alpha) + \mathfrak{P}$.

**Remark 6.1.4.3.** Denote $\kappa(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$ and $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$. Then $\overline{\sigma} \in \mathrm{Gal}\left({\kappa(\mathfrak{P})}\big/{\kappa(\mathfrak{p})}\right)$. Furthermore, $\sigma \mapsto \overline{\sigma}$ is a group homomorphism.

**Proposition 6.1.5.** Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ and $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be such that $\mathfrak{P} \mid \mathfrak{p}$. Then the monomorphism $D(\mathfrak{P}) \to \mathrm{Gal}\left({\kappa(\mathfrak{P})}\big/{\kappa(\mathfrak{p})}\right)$ is surjective.

*Proof.* Let $\alpha \in \mathcal{O}_L$ be such that $\overline{\alpha} \in \kappa(\mathcal{P})$ is a primitive element of the field extension ${\kappa(\mathfrak{P})}\big/{\kappa(\mathfrak{p})}$. Let $\overline{g} \in \kappa(\mathfrak{p})[x]$ and $h \in \mathcal{O}_K[x]$ be the minimal polynomials of $\overline{\alpha}$. It follows that $\overline{g} \mid \overline{h}$.

As $L/K$ is Galois, the polynomial $h$ splits into linear factors, that is

$$h = \prod_{\tau \in \mathrm{Hom}_K(K(\alpha), \mathbb{C})} (x - \tau(\alpha)),$$

and each $\tau$ extends to some $\sigma_i \in \mathrm{Hom}_K(L, \mathbb{C}) = G$.

Let $\tau \in \mathrm{Gal}\left({\kappa(\mathfrak{P})}\big/{\kappa(\mathfrak{p})}\right)$. Then $\overline{g}\left(\tau r \overline{\alpha}\right) = \tau\left(\overline{g}\left(\overline{\alpha}\right)\right) = 0$, hence $\tau\left(\overline{\alpha}\right)$ is a root of $\overline{g}$ and $\overline{h}$. Hence $\tau\left(\overline{\alpha}\right) = \overline{\sigma_i(\alpha)}$ for some $i$ and therefore $\tau = \overline{\sigma}_i$. $\square$

**Definition 6.1.6.** Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ and $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be such that $\mathfrak{P} \mid \mathfrak{p}$. The group

$$I(\mathfrak{P}) = \ker\left(D(\mathfrak{P}) \to \mathrm{Gal}\left({\kappa(\mathfrak{P})}\big/{\kappa(\mathfrak{p})}\right)\right) = \{\sigma \in G \mid \forall \alpha \in \mathcal{O}_L \colon \sigma(\alpha) - \alpha \in \mathfrak{P}\}$$

is the *inertia group* of $\mathfrak{P}$ and the fixed field $L^{I(\mathfrak{P})}$ is the *inertia field* of $\mathfrak{P}$.

**Theorem 6.1.7.** Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ and $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be such that $\mathfrak{P} \mid \mathfrak{p}$. Denote as usual $f = f(\mathfrak{P} \mid \mathfrak{p})$ and $e = e(\mathfrak{P} \mid \mathfrak{p})$ and let $r = |\{\mathfrak{P}' \in \mathcal{P}(\mathcal{O}_L) \mid \mathfrak{P}' \mid \mathfrak{p}\}|$. Finally, let

$$\mathfrak{P}_I = \mathfrak{P} \cap L^{I(\mathfrak{P})} \quad \text{and} \quad \mathfrak{P}_D = \mathfrak{P} \cap L^{D(\mathfrak{P})}.$$

i) The extension $L^{I(\mathfrak{P})}/L^{D(\mathfrak{P})}$ is Galois with

$$\mathrm{Gal}\left(L^{I(\mathfrak{P})}/L^{D(\mathfrak{P})}\right) \cong \mathrm{Gal}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right).$$

Furthermore,

$$|I(\mathfrak{P})| = \left[L : L^{I(\mathfrak{P})}\right] = e \quad \text{and} \quad |D(\mathfrak{P}) : I(\mathfrak{P})| = \left[L^{I(\mathfrak{P})} : L^{D(\mathfrak{P})}\right] = f.$$

ii) We have $e(\mathfrak{P}_D \mid \mathfrak{p}) = f(\mathfrak{P}_D \mid \mathfrak{p}) = 1$.

iii) We have $e(\mathfrak{P}_I \mid \mathfrak{P}_D) = 1$ and $f(\mathfrak{P}_I \mid \mathfrak{P}_D) = f$.

iv) We have $e(\mathfrak{P} \mid \mathfrak{P}_I) = e$ and $f(\mathfrak{P} \mid \mathfrak{P}_I) = 1$.

*Proof.*

i) By construction, $L/L^{D(\mathfrak{P})}$ is Galois with $\mathrm{Gal}\left(L/L^{D(\mathfrak{P})}\right) = D(\mathfrak{P})$. As $I(\mathfrak{P}) \triangleleft D(\mathfrak{P})$, the extension in question is indeed Galois and

$$\mathrm{Gal}\left(L^{I(\mathfrak{P})}/L^{D(\mathfrak{P})}\right) \cong D(\mathfrak{P})/I(\mathfrak{P}) \cong \mathrm{Gal}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right).$$

Recall that $[L : K] = n = ref$. As $|G : D(\mathfrak{P})| = r$, we conclude $\left[L : L^{D(\mathfrak{P})}\right] = ef$. But then

$$|D(\mathfrak{P}) : I(\mathfrak{P})| = \left|\mathrm{Gal}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)\right| = f$$

and so $|I(\mathfrak{P})| = e$.

ii) First note that

$$e = e(\mathfrak{P} \mid \mathfrak{P}_I) \cdot e(\mathfrak{P}_I \mid \mathfrak{P}_D) \cdot e(\mathfrak{P}_D \mid \mathfrak{p}) \quad \text{and} \quad f = f(\mathfrak{P} \mid \mathfrak{P}_I) \cdot f(\mathfrak{P}_I \mid \mathfrak{P}_D) \cdot f(\mathfrak{P}_D \mid \mathfrak{p}).$$

By construction, $\mathrm{Gal}\left(L/L^{D(\mathfrak{P})}\right)$ fixes $\mathcal{P}$, but also acts transitively on prime ideals lying over $\mathfrak{P}$. It follows that $\mathfrak{P}_D$ is non-split in $L$. We deduce that

$$ef = \left[L : L^{D(\mathfrak{P})}\right] = e(\mathfrak{P} \mid \mathfrak{P}_D) \cdot f(\mathfrak{P} \mid \mathfrak{P}_D),$$

therefore $e(\mathfrak{P}_D \mid \mathfrak{p}) = f(\mathfrak{P}_D \mid \mathfrak{p}) = 1$.

iii) The inertia group of $\mathfrak{P}$ in $L/L^{D(\mathfrak{P})}$ is $I(\mathfrak{P})$. But then

$$f(\mathfrak{P}_I \mid \mathfrak{P}_D) = \left|\mathrm{Gal}\left(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})\right)\right| = |D(\mathfrak{P}) : I(\mathfrak{P})| = f.$$

This also shows that $e(\mathfrak{P}_I \mid \mathfrak{P}_D) = 1$.

iv) Evident from the previous two statements. □

**Lemma 6.1.8.** Let $p$ be an odd prime and $\zeta \in \mu_p^*(\mathbb{C})$. Then the unique quadratic subfield of $\mathbb{Q}(\zeta)$ is $\mathbb{Q}\left(\sqrt{p^*}\right)$, where $p^* = (-1)^{\frac{p-1}{2}}p$.

*Proof.* The extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois with cyclic Galois group isomorphic to $\mathbb{Z}_{p-1}$. It therefore has a unique subgroup of index 2, which gives us the sought after field. Denote it by $K = \mathbb{Q}\left(\sqrt{d}\right)$. As $p$ is the only ramified prime in $\mathbb{Q}(\zeta)/\mathbb{Q}$, it is also ramified in $K$. It follows that $p$ is the only prime number dividing $d$, but also note that $2 \nmid p$, as 2 is unramified. That also implies $d \equiv 1 \pmod 4$, therefore $d = (-1)^{\frac{p-1}{2}}p$, as required. $\square$

**Theorem 6.1.9.** Let $p$ be an odd prime, $\zeta \in \mu_p^*(\mathbb{C})$ and $p^* = (-1)^{\frac{p-1}{2}}p$. Then $q \in \mathbb{P}$ splits in $\mathbb{Q}\left(\sqrt{p^*}\right)$ if and only if $q$ lies under an even number of prime ideals in $\mathbb{Q}(\zeta)$.

*Proof.* Let $K = \mathbb{Q}\left(\sqrt{p^*}\right)$ and $L = \mathbb{Q}(\zeta)$. Suppose first that $q$ splits, that is $q\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$, where $\mathfrak{q}_1 \neq \mathfrak{q}_2 \in \mathcal{P}(\mathcal{O}_K)$. Choose an automorphism $\sigma \in \mathrm{Gal}\left(L/\mathbb{Q}\right)$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. Then $\sigma$ induces a bijection

$$\{\mathfrak{Q} \in \mathcal{P}(\mathcal{O}_L) \mid \mathfrak{Q} \mid \mathfrak{q}_1\} \to \{\mathfrak{Q} \in \mathcal{P}(\mathcal{O}_L) \mid \mathfrak{Q} \mid \mathfrak{q}_2\},$$

therefore the cardinality of the set $\{\mathfrak{Q} \in \mathcal{P}(\mathcal{O}_L) \mid \mathfrak{Q} \mid q\}$ is even.

Let $\mathfrak{Q} \in \mathcal{P}(\mathcal{O}_L)$ be such that $\mathfrak{Q} \mid q$ and suppose that the cardinality $r$ of the set $\{\mathfrak{Q}' \in \mathcal{P}(\mathcal{O}_L) \mid \mathfrak{Q}' \mid q\}$ is even. Then

$$r = \left|\mathrm{Gal}\left(L/\mathbb{Q}\right) : D(\mathfrak{Q})\right|$$

is even, therefore

$$\left[L^{D(\mathfrak{Q})} : \mathbb{Q}\right]$$

is even and therefore contains the unique quadratic subfield $K$ of $L$. By theorem 6.1.7, we have

$$e\left(\mathfrak{Q} \cap L^{D(\mathfrak{Q})} \;\middle|\; q\right) = f\left(\mathfrak{Q} \cap L^{D(\mathfrak{Q})} \;\middle|\; q\right) = 1$$

and therefore $e(\mathfrak{q}_i \mid \mathfrak{q}) = f(\mathfrak{q}_i \mid \mathfrak{q}) = 1$, hence $q$ splits. $\square$

**Theorem 6.1.10** (Quadratic reciprocity law)**.** Let $p$ and $q$ be distinct odd primes. Then

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

*Proof.* As before, let $p^* = (-1)^{\frac{p-1}{2}}p$ and $K = \mathbb{Q}\left(\sqrt{p^*}\right)$. Then

$$\left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \left(\frac{p}{q}\right).$$

Note that $\left(\frac{p^*}{q}\right) = 1$ is equivalent to $q$ splitting in $K$, which is in turn equivalent to $q$ lying under an even number of prime ideals in $\mathbb{Q}(\zeta)$.

Denote $f = \mathrm{ord}_{\mathbb{Z}_p^*}(\overline{q})$. Then $q$ lies under precisely

$$\frac{[\mathbb{Q}(\zeta) : \mathbb{Q}]}{f} = \frac{\varphi(p)}{f} = \frac{p-1}{f}$$

prime ideals. The number $\frac{p-1}{f}$ is even if and only if $f \;\middle|\; \frac{p-1}{2}$, which is equivalent to $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \equiv 1 \pmod p$. $\square$

## 6.2 Frobenius elements

**Definition 6.2.1.** Let $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be unramified. The *Frobenius element* of $\mathfrak{P}$, denoted by

$$\left(\frac{L/K}{\mathfrak{P}}\right) \in \operatorname{Gal}\left(L/K\right)$$

is the unique automorphism of $L/K$ that maps to the Frobenius automorphism of $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$. In other words, $\sigma = \left(\frac{L/K}{\mathfrak{P}}\right)$ is the unique automorphism such that $\sigma(\alpha) - \alpha^q \in \mathfrak{P}$ for $q = N(\mathfrak{p})$.

**Lemma 6.2.2.** Let $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be unramified. Then $\operatorname{ord}\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right) = f(\mathfrak{P} \mid \mathfrak{p})$.

*Proof.* The proof is obvious and need not be mentioned. □

**Lemma 6.2.3.** Let $\tau \in \operatorname{Gal}\left(L/K\right)$, $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ and $\mathfrak{P}' = \tau(\mathfrak{P})$. Then

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \tau \left(\frac{L/K}{\mathfrak{P}}\right) \tau^{-1}.$$

*Proof.* By definition, we have $\sigma \in D(\mathfrak{P})$, therefore $\tau\sigma\tau^{-1} \in D(\mathfrak{P}')$. But then

$$\sigma\left(\tau^{-1}(\alpha)\right) - \tau^{-1}(\alpha)^q \in \mathfrak{P}$$

for all $\alpha \in \mathcal{O}_L$, which implies

$$\tau\left(\sigma\left(\tau^{-1}(\alpha)\right)\right) - \alpha^q \in \mathfrak{P}'.$$

□

**Remark 6.2.3.1.** If the Galois group is abelian, this defines a unique Frobenius element for each $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$.

**Lemma 6.2.4.** Let $K \subseteq M \subseteq L$ be number fields such that $L/K$ is abelian.[7] For unramified (in $L$) $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ we have

$$\left.\left(\frac{L/K}{\mathfrak{p}}\right)\right|_M = \left(\frac{M/K}{\mathfrak{p}}\right).$$

*Proof.* Let $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be a prime ideal such that $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Denote $q = |\mathcal{O}_K/\mathfrak{p}|$ and $\sigma = \left(\frac{L/K}{\mathfrak{p}}\right)$. Since $M/K$ is Galois, we have that $\sigma|_M \in \operatorname{Gal}\left(M/K\right)$. It follows that

$$\sigma(\alpha) - \alpha^q \in \mathcal{O}_M \cap \mathfrak{P}.$$

□

**Theorem 6.2.5** (Quadratic reciprocity law)**.** Let $p$ and $q$ be distinct odd primes. Then

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

[7] That is, it is Galois with abelian Galois group.

*Proof.* As before, we will prove that $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. Let $\zeta \in \mu_p^*(\mathbb{C})$ and denote $L = \mathbb{Q}(\zeta)$ and $K = \mathbb{Q}\left(\sqrt{p^*}\right)$. Since ${}^{L}\!/\!_{\mathbb{Q}}$ is abelian, we have

$$\left.\left(\frac{L/\mathbb{Q}}{q}\right)\right|_K = \left(\frac{K/\mathbb{Q}}{q}\right) = \left(\frac{p^*}{q}\right)$$

as an element of $\mathrm{Gal}\left({}^{K}\!/\!_{\mathbb{Q}}\right) \cong S^0$. But by definition, $\left(\frac{L/\mathbb{Q}}{q}\right)(\zeta) = \zeta^q$. The map

$$\mathbb{Z}_p^* \cong \mathrm{Gal}\left({}^{L}\!/\!_{\mathbb{Q}}\right) \to \mathrm{Gal}\left({}^{K}\!/\!_{\mathbb{Q}}\right) \cong S^0$$

induced by the restriction has kernel $\left(\mathbb{Z}_p^*\right)^2$, as it is the only subgroup of index 2. Thus the element $\left.\left(\frac{L/\mathbb{Q}}{q}\right)\right|_K$ is trivial if and only if $q$ is a square modulo $p$, hence

$$\left.\left(\frac{L/\mathbb{Q}}{q}\right)\right|_K = \left(\frac{q}{p}\right).$$

□

## 6.3 Chebotarev's density theorem

**Definition 6.3.1.** Let $K$ be a number field and $S \subseteq \mathcal{P}(\mathcal{O}_K)$. We say that $S$ has *natural density* $\delta \in [0,1]$ if

$$\lim_{M\to\infty} \frac{|\{\mathfrak{p} \in S \mid N(\mathfrak{p}) \leq M\}|}{|\{\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K \mid N(\mathfrak{p}) \leq M\}|} = \delta.$$

**Theorem 6.3.2** (Chebotarev)**.** Let $K$ and $L$ be number fields with ${}^{L}/{}_{K}$ being Galois and denote $G = \mathrm{Gal}\left({}^{L}/{}_{K}\right)$. Furthermore, let $C \subseteq G$ be a conjugacy class. Then

$$\left\{\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K) \;\middle|\; \left(\frac{L/K}{\mathfrak{p}}\right) = C\right\}$$

has density $\frac{|C|}{|G|}$.

**Corollary 6.3.2.1.** In a quadratic number field, half of the prime numbers split and half are inert (asymptotically).

**Corollary 6.3.2.2.** The completely split primes have density $\frac{1}{[L:K]}$.

**Corollary 6.3.2.3.** Every class in $\mathcal{C}(\mathcal{O}_K)$ contains infinitely many prime ideals.

**Theorem 6.3.3** (Dirichlet)**.** Let $a, b \in \mathbb{N}$ be coprime. Then there are infinitely many prime numbers of the form $a + bn$ for $n \in \mathbb{N}$. Furthermore, their density is equal to $\frac{1}{\varphi(b)}$.

*Proof.* Let $K = \mathbb{Q}(\zeta)$, where $\zeta \in \mu_b^*(\mathbb{C})$. Then $\mathrm{Gal}\left({}^{K}/{}_{\mathbb{Q}}\right) \cong \mathbb{Z}_b^*$. Note that $\left(\frac{K/\mathbb{Q}}{p}\right) = p + b\mathbb{Z}$ for $p \nmid b$. Such primes have density $\frac{1}{|\mathrm{Gal}({}^{K}/{}_{\mathbb{Q}})|} = \frac{1}{\varphi(b)}$. $\square$

# Index