Collection of arbitrary mathematical facts

Inhaltsverzeichnis

An undeniable fact: It holds $0 \in \mathbb{N}$. If you do not see that this is obviously, inarguably true, then you are lost.

1 Set Theory

1.1 Zorn's Lemma

Let X be a partially ordered set, in which every chain has an upper bound. Then X has a maximal element.

Proof Show that the set $\mathcal{X} \subseteq 2^X$ of chains in X has a maximal element, so X has a maximal chain (whose upper bound then is the required maximal element).

Let $f : 2^X \setminus \{\emptyset\} \to X$ be a choice function for X, so $f(S) \in S$ for each $S \subseteq X$. Then define

$$g : \mathcal{X} \to \mathcal{X}, \quad C \mapsto \begin{cases} C, & \text{if } C \text{ maximal} \\ C \cup \{f(\{x \in X \mid x \text{ comparable with } C\})\}, & \text{otherwise} \end{cases}$$

where we say that an element $x \in X$ is comparable with a set $S \subseteq X$, if x is comparable with s for all $s \in S$.

Definition Tower Call a subset $\mathcal{T} \subseteq \mathcal{X}$ tower, if

- $\emptyset \in \mathcal{T}$
- If $C \in \mathcal{T}$, then $g(C) \in \mathcal{T}$
- If $\mathcal{S} \subseteq \mathcal{T}$ is a chain, then $\bigcup \mathcal{S} \in \mathcal{T}$

The intersection of towers is a tower, so have a smallest tower $\mathcal{R} := \bigcap\{\mathcal{T} \subseteq \mathcal{X} \mid \mathcal{T} \text{ tower}\}$ in $\mathcal{X}$. We show that $\mathcal{R}$ is a chain. Consider the set $\mathcal{C} := \{A \in \mathcal{R} \mid A \text{ comparable to } \mathcal{R}\}$ of comparable elements in $\mathcal{R}$.

Show $\mathcal{C}$ is a tower, so $\mathcal{R} = \mathcal{C}$ and therefore, $\mathcal{R}$ is a chain.

Trivially, we have $\emptyset \in \mathcal{C}$ as $\emptyset \subseteq A$ for each $A \in \mathcal{R}$. For a chain $\mathcal{S} \subseteq \mathcal{C}$ and any $A \in \mathcal{R}$, have either $A \subseteq S$ for some $S \in \mathcal{S}$, so $A \subseteq \bigcup \mathcal{S}$, or $S \subseteq A$ for each $S \in \mathcal{S}$, so $\bigcup \mathcal{S} \subseteq A$. Therefore, it is left to show that for $\mathcal{C}$ is closed under g. Let $B \in \mathcal{C}$.

Show The set $\mathcal{U} := \{A \in \mathcal{R} \mid A \subseteq B \vee g(B) \subseteq A\} \subseteq \mathcal{R}$ is a tower. It then follows that $\mathcal{R} = \mathcal{U}$, so for each $A \in \mathcal{R}$, have $A \subseteq B \subseteq g(B)$ or $g(B) \subseteq A$. Hence, $g(B)$ is comparable to $\mathcal{R}$. Obviously, $\emptyset \in \mathcal{U}$ and for a chain $\mathcal{S} \subset \mathcal{U}$, also $\bigcup \mathcal{S} \in \mathcal{U}$. Additionally, for $U \in \mathcal{U}$, have:

If $g(B) \subseteq U$, then also $g(B) \subseteq g(U)$.

Otherwise, $U \subseteq B$. If $B = U$, then $g(B) \subseteq g(U)$, so we may assume $U \subsetneq B$. We have that $U \in \mathcal{R}$, so $g(U) \in \mathcal{R}$ (because $\mathcal{R}$ is a tower) and therefore, B is comparable to $g(U)$. $\Rightarrow g(U) \subseteq B$, because if $B \subsetneq g(U)$, we would have $U \subsetneq B \subsetneq g(U)$, however, $g(U) \setminus U$ has at most one element. Hence, $g(U) \in \mathcal{U}$, so $\mathcal{U} = \mathcal{C} = \mathcal{R}$ are towers.

Show The set $C := \bigcup \mathcal{R}$ is a maximal element in $\mathcal{X}$.

$\mathcal{R}$ is a chain and a tower, so $C \in \mathcal{R}$. We also have $g(C) \in \mathcal{R}$, as $\mathcal{R}$ is a tower. $\Rightarrow g(C) \subseteq C$ and therefore $C = g(C)$, so C is maximal in $\mathcal{X}$ by definition of g.

2 Algebra

2.1 Cauchy-Schwarz

For $x, y \in V$ inner product space, have

$$\langle x, y\rangle^2 \leq \langle x, x\rangle \langle y, y\rangle$$

Proof idea Start with

$$\langle x, x\rangle \left\langle y - \frac{\langle x, y\rangle}{\langle x, x\rangle} x,\ y - \frac{\langle x, y\rangle}{\langle x, x\rangle} x \right\rangle \geq 0$$

2.2 Sylow Theorems

For a finite group G with $|G| = n = p^e m,\ p \in \mathbb{P},\ p \perp m$ have:

- There is $U \leq G$ with $|U| = p^e$
- For $U, V \leq G$ with $|U| = |V| = p^e$ have $U = gVg^{-1}$ for $g \in G$
- Let s be the count of $U \leq G,\ |U| = p^e$. Then $s|m$ and $s \equiv 1 \mod p$

Proof idea Use group operations, for 1. on $\chi := \{U \leq G \mid |U| = p^e\}$, for 2. on $\chi := \{gU \mid g \in G\}$ and for 3. on $\chi := \{U \leq G \mid |U| = p^e\}$ with conjugation.

2.3 Mordell's inequality

Have $\gamma_d \leq \gamma_{d-1}^{(d-1)/(d-2)}$. Inductively, it follows $\gamma_d \leq \gamma_k^{(d-1)/(k-1)}$ (γ here is Hermite's constant).

Proof Let L be a d-rank lattice for which Hermite's constant is reached, with dual L^* and $x \in L^*$ with $\|x\| = \lambda(L^*)$.

$$\begin{aligned}
&\Rightarrow \left(\langle x\rangle^\perp \cap L\right)^* = \pi_{\langle x\rangle^\perp}(L^*) \;\Rightarrow\; \mathrm{vol}(L^*) = \|x\| \;\mathrm{vol}\left(\langle x\rangle^\perp \cup L\right)^* \\
&\Rightarrow \sqrt{\gamma_{n-1}}^{1-n}\lambda(L)^{n-1} \leq \mathrm{vol}\left(\langle x\rangle^\perp \cap L\right) = \|x\| \;\mathrm{vol}(L) \leq \sqrt{\gamma_n}\mathrm{vol}(L^*)^{\frac{1}{n}}\mathrm{vol}(L) \\
&\Rightarrow \sqrt{\gamma_n}\sqrt{\gamma_{n-1}}^{n-1} \geq \frac{\lambda(L)^{n-1}}{\mathrm{vol}(L)^{\frac{n-1}{n}}} = \sqrt{\gamma_n}^{n-1} \;\Rightarrow\; \sqrt{\gamma_n}^{n-2} \geq \sqrt{\gamma_{n-1}}^{n-1}
\end{aligned}$$

where M^* denotes the unique "dual" of M in $\langle M\rangle$.

2.4 Facts about finite rings

- $\mathbb{F}_q^*$ is cyclic for $q = p^n$

Proof By the theorem on finitly generated abelian groups, have

$$\mathbb{F}_q^* \cong \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_s\mathbb{Z}$$

with $n_1|...|n_s$. Assume $s > 1$ and $n_1 \neq 1$. Then $n_s < N := |\mathbb{F}_q^*|$. For $x \in \mathbb{F}_q^*$, have therefore that $\mathrm{ord}(x)|n_s$, so $p(x) = 0$ with $p(X) := X^{n_s} - 1$. But this is a contradiction, as p is a polynomial of degree n_s with $N > n_s$ roots in the field $\mathbb{F}_q$.

- $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ is cyclic if $p > 2$ or $\alpha \leq 2$

Proof Use induction over α.

$\alpha = 1$ Follows directly from the previous point, as $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ as rings.

$\alpha > 1$ Consider the canonical ring homomorphism

$$\pi : \mathbb{Z}/p^\alpha\mathbb{Z} \to (\mathbb{Z}/p^\alpha\mathbb{Z}) \;/\; ([p^{\alpha-1}]), \quad x \mapsto [x]$$

Then the restriction of π to $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$

$$f : (\mathbb{Z}/p^\alpha\mathbb{Z})^* \to \left((\mathbb{Z}/p^\alpha\mathbb{Z}) \;/\; ([p^{\alpha-1}])\right)^*, \quad x \mapsto \pi(x)$$

is a surjective group homomorphism. We have

$$\ker(f) = \pi^{-1}(\{1\}) = 1 + ([p^{\alpha-1}]) = \left\{1 + k[p^{\alpha-1}] \;\middle|\; k \in \{0, ..., p-1\}\right\}$$

As $[p^{\alpha-1}]^2 = 0$, have $\ker(f) = \langle 1 + [p^{\alpha-1}] \rangle$ by the binomial theorem. On the other hand, by the second isomorphism theorem, have the ring isomorphy $((\mathbb{Z}/p^\alpha\mathbb{Z}) \ / \ ([p^{\alpha-1}])) \cong \mathbb{Z}/p^{\alpha-1}\mathbb{Z}$, which is cyclic by the induction hypothesis. Therefore, $G/\mathrm{im}(f) \cong \ker(f)$ yields:

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^*/\langle 1 + [p^{\alpha-1}] \rangle \cong \langle [g] \rangle \text{ for some } g \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$$

Assume now that $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ is not cyclic. Then $\mathrm{ord}(g) \neq (p-1)p^{\alpha-1}$, so $\mathrm{ord}(g) = (p-1)p^{\alpha-2}$, as $\mathrm{ord}(1 + [p^{\alpha-1}]) = p$. If $\alpha = 2$, then $\mathrm{ord}(g) = p - 1 \perp p$, and the Chinese Remainder theorem yields that

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/(p-1)p^{\alpha-2}\mathbb{Z} \cong \mathbb{Z}/(p-1)p^{\alpha-1}\mathbb{Z}$$

and we are done. Therefore, let $\alpha > 2$ and $p > 2$ and consider the mapping

$$\phi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/(p-1)p^{\alpha-2}\mathbb{Z} \to (\mathbb{Z}/p^\alpha\mathbb{Z})^*, \quad (k, n) \mapsto (1 + k[p^{\alpha-1}])g^n$$

which is a homomorphism, as $(1 + k[p^{\alpha-1}])(1 + l[p^{\alpha-1}]) = 1 + (l + k)[p^{\alpha-1}]$ and $\mathrm{ord}(g) = (p-1)p^{\alpha-2}$ and bijective, so an isomorphism. How to continue from here?

3 Probabilities

3.1 Chernoff-Hoeffding

$X_1, ..., X_n$ independent, $0 \leq X_i \leq 1$. Then

$$\Pr\left[\sum X_i - \mathrm{E}\left[\sum X_i\right] \geq t\right] \leq \exp\left(-2\frac{t^2}{n}\right)$$

4 Analysis

4.1 Inequalities

Young's inequality

$$xy \leq \frac{x^p}{p} + \frac{y^q}{q} \text{ for } \frac{1}{p} + \frac{1}{q} = 1, \ x, y \geq 0$$

Proof By convexity of log, have

$$\begin{aligned} \frac{1}{p}\log x^p + \frac{1}{q}\log y^q &\leq \log\left(\frac{1}{p}x^p + \frac{1}{q}y^q\right) \\ \Rightarrow \ \log(xy) &\leq \log\left(\frac{1}{p}x^p + \frac{1}{q}y^q\right) \end{aligned}$$

Hölder's inequality For measurable functions f, g and $\frac{1}{p} + \frac{1}{q} = 1$ (w.r.t measure μ) have:

$$\|fg\|_1 = \int |fg| d\mu \leq \left(\int |f|^p d\mu\right)^{\frac{1}{p}} \left(\int |g|^q d\mu\right)^{\frac{1}{q}} = \|f\|_p \|g\|_q$$

Proof By Young's inequality have

$$\begin{aligned} \frac{|fg|}{\|f\|_p\|g\|_q} &\le \frac{|f|^p}{p\|f\|_p^p} + \frac{|g|^q}{q\|f\|_q^q} \\ \Rightarrow \frac{|fg|}{\|f\|_p\|g\|_q} &\le \frac{1}{p\|f\|_p^p}\|f\|_p^p + \frac{1}{q\|g\|_q^q}\|f\|_q^q = 1 \end{aligned}$$

4.2 Transformation

$\phi : U \to \mathbb{R}^n$ injective. Then

$$\int_{\phi(U)} f(x)dx = \int_U f(\phi(x))|\det(D\phi)(u)|dx$$

5 Topology

5.1 Tychonoffs Theorem

For a collection of compact topological spaces $(X_i)_{i\in I}$ the product space $\prod_{i\in I} X_i$ is compact.

6 Discrete

6.1 Gamma Function

Defined for $\mathbb{C} \setminus -\mathbb{N}$. Possible definitions:

$$\begin{aligned} \Gamma(z) &:= \int_0^\infty t^{z-1}e^{-t}dt \quad \text{if } \mathrm{Re}(z) > 0 \\ \frac{1}{\Gamma(z)} &= \lim_{n\mapsto\infty} \binom{n+z-1}{n} n^{1-z} \end{aligned}$$

We get

$$\Gamma(z+1) = z\Gamma(z)$$

7 Functional analysis

7.1 Minkowski-functional

For an absorbing set $A \subseteq X$ the functional

$$p_A : X \to \mathbb{R}, \quad x \mapsto \inf\{t \ge 0 \mid x \in tA\}$$

is

- subadditive if A is convex

- homogenous if A is balanced
- point-separating if A is bounded and X Hausdorff

7.2 Kolmogorov's normability criterion

X is normable, iff an open, bounded, convex set $A \subseteq X$ exists.

Proof idea Use the Minkowski-functional for $\tilde{A} = A \cap -A$ which is open, nonempty, bounded, convex.

7.3 Baire's theorem

X complete and metric, $(A_n)_n$ open and dense $\Rightarrow \bigcap A_n$ is dense.

Proof idea For each $y \in X$, construct sequence $(x_n)_n$ with

$$x_n \in B_{\frac{1}{n}}(y) \cap \left(\bigcap_{k \leq n} A_n \right) \Rightarrow y = \lim x_n \in \mathrm{cl} \left(\bigcap_{i \leq k} A_i \right) \text{ for all } k$$

7.4 Open mapping theorem

X, Y Banach and $T : X \to Y$ linear, continuous and surjective. Then T is open.

Proof idea

$$\bigcup_{K \in \mathbb{N}} \mathrm{cl}\left(T(B_K(0))\right) = Y \Rightarrow \mathrm{cl}\left(T(B_K(0))\right)^\circ \neq \emptyset \text{ for some } K$$

by Baire's theorem. It follows that $B_\epsilon(0) \subseteq T(B_1(0))$, so T is open, by the following lemma:

7.4.1 Lemma

Let $T \in \mathcal{L}(X, Y)$ such that $0 \in \mathrm{cl}(T(B_X))^\circ \neq \emptyset$. Then $0 \in T(B_X)^\circ$, where $B_X = B_1(0)$ is the unit ball.

Proof The idea is, that T is linear and continuous, so we can work with series. Let $y \in \epsilon B_Y \subseteq \mathrm{cl}(T(B_X))$. Recursivly construct sequences $(x_n)_{n \in \mathbb{N}}$ in X and $(y_n)_{n \in \mathbb{N}}$ in Y with

$$\begin{gathered} y_0 = y, \quad \|y_n\| < 2^{-n}\epsilon, \\ \|x_n\| < 2^{-n}, \quad \|y_n - T(x_n)\| < 2^{-n-1}\epsilon \\ y_{n+1} = y_n - T(x_n) \end{gathered}$$

This is possible as $T(2^{-n}B_X)$ is dense in $2^{-n}\epsilon B_Y$ for each $n \in \mathbb{N}$. By completeness of X have then that $\sum_n x_n$ converges to $x \in X$. Therefore, $T(x) = \sum_n T(x_n) = \sum_n y_n - y_{n+1} = y_0 = y$ as $y_n \to 0$ for $n \to 0$.

7.5 Hahn-Banach dominated extension theorem

Let X be a $\mathbb{R}$-vector space, $p : X \to \mathbb{R}$ sublinear (i.e. subadditive and homogenous w.r.t $\lambda \geq 0$) and $Y \subseteq X$ a subspace. A form $f : Y \to \mathbb{R}$ with $f \leq p$ can be extended to $F : X \to \mathbb{R}$ with $F \leq p$.

Proof idea Let $F : U \to \mathbb{R}$ be the maximal element (exists by Zorn's lemma) in

$$\left\{F : U \to \mathbb{R} \mid Y \subseteq U \subseteq X,\ F\big|_Y = f,\ F \leq p\right\}$$

Then $U = X$, as for $v \in X \setminus U$ have $p(v + y) - F(y) \geq \lambda \geq F(z) - p(z - v)$ for $y, z \in U$ by the reverse triangle inequality. Then $F'(u + tv) := F(u) + \lambda t$ is greater than F.

7.6 Banach-Alaoglu

$V \subseteq X$ neighborhood of 0 $\Rightarrow$ $K = \{\phi \in X' \mid |\phi(V)| \leq 1\}$ compact w.r.t weak-*-topology (weakest topology on X' so that all $\hat{x} \in X''$ are continuous, $\hat{x} : X' \to \mathbb{K},\ \phi \mapsto \phi(x)$).

Proof idea Let $\gamma(x) > 0$ with $x \in \gamma(x)V$ for all $x \in X$. Then

$$\mathbb{K}^X = \bigtimes_{x\in X} \mathbb{K} \ \Rightarrow\ K \subseteq \bigtimes_{x\in X} B_{\gamma(x)}(0) \text{ compact by Tychonoff's theorem}$$

The topologies on the sets match, as the weak-*-topology on K has a local base of finite intersections of $\hat{x_i}^{-1}(]-\epsilon_i, \epsilon_i[)$ and

$$\bigtimes_{x\in X} B_{\gamma(x)}(0) \cap X' \text{ has one of sets } \bigcap_{1\leq i\leq n}]-\epsilon_i, \epsilon_i[\times \bigtimes_{x\neq x_i} \mathbb{K} \cap X'$$

8 Operator theory

8.1 Neumann series

Let $T \in \mathcal{L}(X)$. If $\sum_{n\in\mathbb{N}} T^n$ converges, then $1 - T$ is invertible with

$$(1 - T)^{-1} = \sum_{n\in\mathbb{N}} T^n$$

To get convergence, it is sufficient to have $\|T\| < 1$ and X is complete.

8.2 l^p spaces

Note that from 4.1 we get that $l^p \simeq (l^q)'$ for $p > 1$ and $\frac{1}{p} + \frac{1}{q} = 1$.

8.3 Riesz lemma

Let $U \subsetneq$ closed subspace of a normed space. For $\delta > 0$ have then $x \in X$ with $\|x\| = 1$ and distance greater than $1 - \delta$ from U.

Proof idea Consider any $x \in X \setminus U$ and an almost closest point $u \in U$. Then scale $x - u$ appropriately.

8.4 Compact Operators and spaces

From 8.3 one can conclude that the unit ball B_X is compact iff $\dim X < \infty$. Therefore, consider operators $T \in \mathcal{L}(X, Y)$ such that $\mathrm{cl}(T(B_X))$ compact, these are a Banach space $\mathcal{K}(X, Y)$.

Proof idea To show that $\mathcal{K}(X, Y)$ is closed in $\mathcal{L}(X, Y)$, consider diagonal sequences.

8.5 Arzela-Ascoli

Let X be a compact topological space. Then the continuous functions $C(X)$ from X to $\mathbb{R}$ are normed via $\|\cdot\|_\infty$. If a $M \subseteq C(X)$ is bounded, closed and equicontinuous (i.e. $\forall x \in X, \epsilon > 0\ \exists$neighborhood N of x $\forall x \in M:\ x(N) \subseteq B_\epsilon(x(s)))$, then M is compact.

Proof Let $(x_n)_{n\in\mathbb{N}}$ be a sequence in M. As X is compact, it is separable, so have $X = \{s_n \mid n \in \mathbb{N}\}$. Therefore, recursivly construct subsequences

$$\left(x_n^{(k)}\right)_{n\in\mathbb{N}} \text{ such that } \left(x_n^{(k)}(s_k)\right)_{n\in\mathbb{N}} \text{ converges}$$

and consider the diagonal sequence $(y_n)_{n\in\mathbb{N}}$. Then $(y_n(s_k))_{n\in\mathbb{N}}$ converges for each $k \in \mathbb{N}$.

By equicontinuity, have for each $k \in \mathbb{N}$ a neighborhood N_k of s_k such that $\forall x \in M$: $x(N_k) \subseteq B_\epsilon(x(s_k))$. Therefore, there is a subcover N_i for $i \in I$ finite. As $(y_n(s_k))_{n\in\mathbb{N}}$ converges for each k, it simultaneously converges for each $i \in I$. This yields that $(y_n)_{n\in\mathbb{N}}$ is a Cauchy-sequence w.r.t $\|\cdot\|_\infty$.

8.6 Proposition of Schauder

For $T \in \mathcal{L}(X, Y)$ between Banach-spaces, have that T is compact if and only if $T' \in \mathcal{L}(Y', X')$ is compact.

Proof Prove $\Rightarrow$, the other direction follows. Then $K := \mathrm{cl}(T(B_X))$ is compact metric space. For $(y_n')_{n\in\mathbb{N}}$ have

$$\left(y_n'|_K\right)_{n\in\mathbb{N}} \text{ is a sequence in } C(K)$$

It also fulfills the conditions of 8.5, so there is a convergent subsequence indexed by $(n_k)_{k\in\mathbb{N}}$. Then also $(T'y_{n_k})_{k\in\mathbb{N}}$ converges, so $T'(B_{Y'})$ is relatively compact.

8.7 Closed range theorem

Let X, Y be Banach spaces, $T \in \mathcal{L}(X, Y)$. The the following are equivalent

- $\operatorname{ran}(T)$ closed
- $\operatorname{ran}(T) = (\ker(T'))_\perp$
- $\operatorname{ran}(T')$ closed
- $\operatorname{ran}(T') = (\ker(T))^\perp$

Proof Show (ii) $\Leftrightarrow$ (iv), the rest is relativly easy. Let $x' \in (\ker(T))^\perp$. Then have $z' : \operatorname{ran}(T) \to \mathbb{K}$ linear with $z' \circ T = x'$ (isomorphism theorem). A complex computation using the open mapping theorem shows that z' is continuous. A Hahn-Banach extension of z' to Y then yields a preimage under T' of x'.

For the other direction, consider $Z := \operatorname{cl}(\operatorname{ran}(T))$. By the Hahn-Banach theorem, we can extend functionals on Z to functionals on Y, so $\operatorname{ran}(T') \simeq Z'$ by the isomorphism $\operatorname{ran}(T') \to Z',\ T'(y') \mapsto y'\big|_Z$.

Therefore, for all $y' \in Y'$ have that $\|y'\big|_Z\| \leq c\|y' \circ T\|$ where $c > 0$.

Consider any $y \in Z$ with $\|y\| \leq 1$. If $y \notin \operatorname{cl}(T(2cB_X))$, the Hahn-Banach separation theorem yields $y' \in Y'$ such that

$$2c\|y' \circ T\| = \sup\left(2c(y' \circ T)(B_X)\right) \leq y'(y) = \|y'\big|_Z(y)\| \leq \|y'\big|_Z\| \leq c\|y' \circ T\|$$

a contradiction. Therefore, $\operatorname{cl}(T(B_X))^\circ \neq \emptyset$ and so $\tilde{T} : X \to Z,\ x \mapsto T(x)$ is open by 7.4.1. It follows that $\operatorname{ran}(T) = \operatorname{ran}(\tilde{T})$ is closed, as X is closed.

9 (Algebraic) Number Theory

9.1 Propositions (from Neukirch)

Let $K/\mathbb{Q}$ separable and $\mathcal{O}_K$ integral closure of $\mathbb{Z}$.

2.9 For $\alpha_1, ..., \alpha_n \in \mathcal{O}_K$ basis of K, then $d(\alpha_1, ..., \alpha_n)\mathcal{O}_K \subseteq \alpha_1\mathbb{Z} + ... + \alpha_n\mathbb{Z}$.

2.10 Each finitly generated $\mathcal{O}_K$-module $M \subseteq K$ is a free $\mathbb{Z}$-module.

3.1 $\mathcal{O}_K$ is a Dedekind domain, so noetherian, integrally closed and each prime ideal $p \neq 0$ is maximal.

3.3 Each ideal except $(0), (1)$ has a unique factorization in prime ideals (up to order).

9.2 Minkowski's theorem (Neukirch 4.4)

Let V be a n-dimensional euclidean vector space, $\Gamma \subseteq V$ be a complete lattice, $X \subseteq V$ convex and balanced with $\operatorname{vol}(X) > 2^n\operatorname{vol}(\Gamma)$, then $X \cap \Gamma \neq \emptyset$.

9.3 Dirichlet's unit theorem

For $K/\mathbb{Q}$ finite with ring of integers $\mathcal{O}_K$, have $\mathcal{O}_K^* \cong \mu(K) \oplus G$, where $\mu(K)$ are the roots of unity and G is a free group of rank $r+s-1$, where r is the number of real $\mathbb{Q}$-embeddings $K \to \mathbb{R}$ and s is the number of conjugate pairs of complex $\mathbb{Q}$-embeddings $K \to \mathbb{C}$.

9.4 Square number fields

For a square-free $D \in \mathbb{Z},\ D \neq 0, 1$ have $K = \mathbb{Q}(\sqrt{D})$. Then $d := d_K = D$ if $D \equiv 1 \mod 4$ and $d := d_K = 4D$ otherwise. Furthermore, $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(d_K + \sqrt{d_K})]$.

In the case $D > 1$, have that $\mathcal{O}_K^* = \langle \epsilon_1 \rangle$, where $\epsilon_1 = \frac{1}{2}(x + y\sqrt{d_K})$ for the smallest solution $x, y \geq 0$ of $x^2 - dy^2 = -4$ (or ... $= 4$ if this has no integral solution).

In the case $D < 0$, have that

$$\mathcal{O}_K^* = \begin{cases} \{1, -1, i, -i\} & \text{if } D = -1 \\ \left\{ e^{\frac{2\pi i k}{6}} \middle| k \in \{0, ..., 5\} \right\} & \text{if } D = -3 \\ \{1, -1\} & \text{otherwise} \end{cases}$$

Proof idea of the second part For $\epsilon = \frac{1}{2}(u + v\sqrt{d_K}) \in \mathcal{O}_K^*$ with $\epsilon^{-1} = \frac{1}{2}(w + t\sqrt{d_K})$ have

$$uw + dtv = 4,\ ut + vw = 0 \quad \Rightarrow \quad w(u^2 - dv^2) = 4u,\ u(w^2 - dt^2) = 4w$$

so $(u^2 - dv^2)(w^2 - dt^2) = 16$. By using $u \equiv dv \mod 2,\ w \equiv dt \mod 2$ and $d \equiv d^2 \mod 4$ get that u, v also fulfill the equation (as $u^2 - dv^2, w^2 - dt^2 \equiv 0 \mod 4$). By Dirichlet's unit theorem, have that $\mathcal{O}_K^* = \langle \epsilon \rangle$ for $\epsilon = \frac{1}{2}(u + v\sqrt{d_K})$. Wlog have that $u, v \geq 0$ (maybe use ϵ^{-1}), then $\epsilon_1 = \epsilon^k,\ k > 0$. It must hold $k = 1$, otherwise u, v would solve $x^2 - dy^2 = \pm 4$ with $u^2 + dv^2 < x^2 + dy^2$ (which we consider as "smaller").

9.5 Ramification (DE: Verzweigung)

Let $\mathcal{R}$ be a Dedekind domain, $K = \mathrm{Quot}(\wr)$ and $\mathcal{O}$ integral closure of $\mathcal{R}$ in field extension $L|K$. Then $\mathcal{O}$ is a Dedekind domain.

For a prime ideal $\mathfrak{p}$ in $\mathcal{R}$, have

8.2 $L|K$ separable $\Rightarrow$ $\sum e_i f_i = n := [L : K]$ where $\mathfrak{p}\mathcal{O} = \mathfrak{B}_1^{e_1} ... \mathfrak{B}_r^{e_r}$ is the factorization of $\mathfrak{p}$ into prime ideals in $\mathcal{O}$ and $f_i = [\mathcal{O}/\mathfrak{B}_i : \mathcal{R}/\mathfrak{p}]$. The proof uses the CRT and the properties of $\mathcal{O}/\mathfrak{B}_i$ as $\mathcal{R}/\mathfrak{p}$-vector space.

8.3 Let $L = K(\alpha)$ for an integral, primitive element $\alpha \in \mathcal{O}$. Then $\mathfrak{p} = \mathfrak{B}_1^{e_1} ... \mathfrak{B}_r^{e_r}$ for $\mathfrak{B}_i = \mathfrak{p}\mathcal{O} + p_i(\alpha)\mathcal{O}$, where the minimal polynomial p of α splits into irreducible factors mod $\mathfrak{p}\mathcal{O}$

$$p(X) \equiv p_1(X)^{e_1} ... p_r(X)^{e_r} \mod \mathfrak{p}\mathcal{O}$$

Also have $f_i = \deg(p_i)$