

# Collection of arbitrary mathematical facts

## Inhaltsverzeichnis

|          |   |          |
|----------|---|----------|
| <b>1</b> | <b>Set Theory</b>                                     | <b>2</b> |
| 1.1      | Zorn's Lemma . . . . .                                | 2        |
| 1.2      | Ultrafilter Lemma . . . . .                           | 3        |
| 1.3      | Product Cardinality . . . . .                         | 3        |
| <b>2</b> | <b>Algebra</b>  | <b>4</b> |
| 2.1      | Cauchy-Schwarz . . . . .                              | 4        |
| 2.2      | Sylow Theorems . . . . .                              | 4        |
| 2.3      | Mordell's inequality . . . . .                        | 4        |
| 2.4      | Facts about finite rings . . . . .                    | 5        |
| <b>3</b> | <b>Probabilities</b>                                  | <b>6</b> |
| 3.1      | Chernoff-Hoeffding . . . . .                          | 6        |
| <b>4</b> | <b>Analysis</b>                                       | <b>6</b> |
| 4.1      | Inequalities . . . . .                                | 6        |
| 4.2      | Transformation . . . . .                              | 6        |
| <b>5</b> | <b>Topology</b>                                       | <b>7</b> |
| 5.1      | Separation axioms . . . . .                           | 7        |
| 5.2      | Universal nets . . . . .                              | 7        |
| 5.3      | Initial topologies . . . . .                          | 7        |
| 5.4      | Characterization of compactness . . . . .             | 7        |
| 5.5      | Tychonoffs Theorem . . . . .                          | 8        |
| 5.6      | Urysohn's Lemma . . . . .                             | 8        |
| 5.7      | Tietze's extension theorem . . . . .                  | 8        |
| 5.8      | Extension of uniformly continuous functions . . . . . | 8        |
| <b>6</b> | <b>Discrete</b>                                       | <b>9</b> |
| 6.1      | Gamma Function . . . . .                              | 9        |

|          |   |           |
|----------|---|-----------|
| <b>7</b> | <b>Functional analysis</b>                        | <b>9</b>  |
| 7.1      | Minkowski-functional . . . . .                    | 9         |
| 7.2      | Kolmogorov's normability criterion . . . . .      | 9         |
| 7.3      | Baire's theorem . . . . .                         | 9         |
| 7.4      | Open mapping theorem . . . . .                    | 10        |
| 7.4.1    | Lemma . . . . .                                   | 10        |
| 7.5      | Hahn-Banach dominated extension theorem . . . . . | 10        |
| 7.6      | Banach-Alaoglu . . . . .                          | 10        |
| <b>8</b> | <b>Operator theory</b>                            | <b>11</b> |
| 8.1      | Neumann series . . . . .                          | 11        |
| 8.2      | $l^p$ spaces . . . . .                            | 11        |
| 8.3      | Riesz lemma . . . . .                             | 11        |
| 8.4      | Compact Operators and spaces . . . . .            | 11        |
| 8.5      | Arzela-Ascoli . . . . .                           | 11        |
| 8.6      | Proposition of Schauder . . . . .                 | 12        |
| 8.7      | Closed range theorem . . . . .                    | 12        |
| 8.8      | Projection theorem . . . . .                      | 13        |
| 8.9      | Frechet-Riesz representation theorem . . . . .    | 13        |
| 8.10     | Orthonormal bases . . . . .                       | 13        |
| <b>9</b> | <b>(Algebraic) Number Theory</b>                  | <b>13</b> |
| 9.1      | Propositions (from Neukirch) . . . . .            | 13        |
| 9.2      | Minkowski's theorem (Neukirch 4.4) . . . . .      | 14        |
| 9.3      | Dirichlet's unit theorem . . . . .                | 14        |
| 9.4      | Square number fields . . . . .                    | 14        |
| 9.5      | Ramification (de: Verzweigung) . . . . .          | 14        |

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

define

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

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  $\mathcal{S} \subseteq \mathcal{U}$ , 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  $g$ .

## 1.2 Ultrafilter Lemma

For each filter  $\mathcal{F}$  on a set  $X$  there is a ultrafilter  $\mathcal{U}$  such that  $\mathcal{F} \subseteq \mathcal{U}$ .

## 1.3 Product Cardinality

For infinite set  $X$  have  $\text{card}(X) = \text{card}(X \times X)$ .

**Proof idea** Proof the statement for all cardinals  $\aleph_\alpha$  by transfinite induction on  $\alpha$  to show that  $\text{ord}(\aleph_\alpha \times \aleph_\alpha) = \aleph_\alpha$  (using some defined well-order on  $\aleph_\alpha \times \aleph_\alpha$ ).

If  $\alpha = \beta + 1$  then show that for each  $\mu < \aleph_\alpha$  have  $\text{card}(\mu \times \mu) < \aleph_\alpha$  by transfinite induction. For the limit ordinal case, use that  $\text{card}(\mu \times \mu) < \aleph_\alpha$  iff  $\text{card}(\mu \times \mu) \leq \aleph_\beta$  and  $\text{card}(\aleph_\beta \times \aleph_\beta) = \aleph_\beta$ . It follows that then  $\text{ord}(\mu \times \mu) < \aleph_\alpha$ , so  $\text{ord}(\aleph_\alpha \times \aleph_\alpha) = \bigcup_{\mu < \aleph_\alpha} \text{ord}(\mu \times \mu) \leq \aleph_\alpha$ .

If  $\alpha$  is a limit ordinal, then  $\text{ord}(\aleph_\alpha \times \aleph_\alpha) = \bigcup_{\beta < \alpha} \text{ord}(\aleph_\beta \times \aleph_\beta) = \bigcup_{\beta < \alpha} \aleph_\beta = \aleph_\alpha$ .

## 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  $s \equiv 1 \pmod{p}$

**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  $\gamma_d \leq \gamma_k^{(d-1)/(k-1)}$  ( $\gamma$  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  $\|x\| = \lambda(L^*)$ .

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

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 finitely generated abelian groups, have

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

with  $n_1 | \dots | n_s$ . Assume  $s > 1$  and  $n_1 \neq 1$ . Then  $n_s < N := |\mathbb{F}_q^*|$ . For  $x \in \mathbb{F}_q^*$ , have therefore that  $\text{ord}(x) | n_s$ , 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  $\alpha$ .

$\alpha = 1$  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

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

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

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

is a surjective group homomorphism. We have

$$\ker(f) = \pi^{-1}(\{1\}) = 1 + ([p^{\alpha-1}]) = \{1 + k[p^{\alpha-1}] \mid k \in \{0, \dots, p-1\}\}$$

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 isomorphism  $((\mathbb{Z}/p^\alpha\mathbb{Z}) / ([p^{\alpha-1}])) \cong \mathbb{Z}/p^{\alpha-1}\mathbb{Z}$ , which is cyclic by the induction hypothesis. Therefore,  $G/\text{im}(f) \cong \ker(f)$  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  $\text{ord}(g) \neq (p-1)p^{\alpha-1}$ , so  $\text{ord}(g) = (p-1)p^{\alpha-2}$ , as  $\text{ord}(1 + [p^{\alpha-1}]) = p$ . If  $\alpha = 2$ , then  $\text{ord}(g) = p-1 \perp p$ , 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

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

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

## 3 Probabilities

### 3.1 Chernoff-Hoeffding

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

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

## 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  $\mu$ ) 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

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

### 4.2 Transformation

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

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

## 5 Topology

### 5.1 Separation axioms

- T0** for distinct points  $x, y$ , have either  $x \in U, y \notin U$  or  $x \notin U, y \in U$  for open  $U$
- T1** for distinct points  $x, y$  have  $x \in U, y \notin U$  and  $x \notin V, y \in V$  for open  $U, V$  (equivalent to singletons are closed)
- T2** or Hausdorff; points can be separated by open sets
- T3** T1 + points can be separated from closed sets by open sets
- T4** T1 + closed sets can be separated from closed sets by open sets

### 5.2 Universal nets

Every net  $(x_i)_{i \in I}$  has a universal subnet.

**Proof idea** Consider the filter  $\mathcal{F} = \{F \subseteq I \mid \exists i \in I \forall j \in I : j \geq i \Rightarrow j \in F\}$  and use ultrafilter  $\mathcal{U} \supseteq \mathcal{F}$  as index set.

### 5.3 Initial topologies

$\{\bigcap_{\alpha \in \mathcal{F}} f_\alpha^{-1}(U_\alpha) \mid \mathcal{F} \subseteq \mathcal{A} \text{ finite, } U_\alpha \in \tau_\alpha\}$  is a basis for the initial topology of  $f_\alpha : X \rightarrow (X_\alpha, \tau_\alpha)$ .

### 5.4 Characterization of compactness

The following are equivalent, where  $(X, \tau)$  is a topological space

- Every open cover of  $X$  has a finite subcover
- For all  $\mathcal{D} \subseteq 2^X$  of nonempty, closed sets with  $\bigcap \mathcal{F} \neq \emptyset$  for each finite  $\mathcal{F} \subseteq \mathcal{D}$  have that  $\bigcap \mathcal{D} \neq \emptyset$
- For each chain  $\mathcal{C} \subseteq 2^X$  of nonempty, closed sets have  $\bigcap \mathcal{C} \neq \emptyset$
- Each universal net converges
- Each net has a convergent subnet
- Each closed  $S \subseteq X$  is compact w.r.t the subspace topology

**Proof** Interesting is only (iii)  $\Rightarrow$  (ii). Given  $\mathcal{D} \subseteq 2^X$  consider  $\mathcal{S} := \{\mathcal{A} \subseteq \mathcal{D} \mid \bigcap \mathcal{A} \neq \emptyset\}$ . Then by assumption,  $\mathcal{S}$  contains all finite sets. Also,  $\mathcal{S}$  is also closed w.r.t monotone unions, as for a chain  $\mathcal{C} \subseteq \mathcal{S}$  have that  $\{\bigcap C \mid C \in \mathcal{C}\}$  is a chain of nonempty closed sets, so  $\bigcap \{\bigcap C \mid C \in \mathcal{C}\} \neq \emptyset$  by assumption. But this is a lower bound for each  $C \in \mathcal{C}$ , so for  $\bigcup \mathcal{C}$ . Therefore,  $\bigcup \mathcal{C} \in \mathcal{S}$ .

Assume  $\mathcal{A} \subseteq 2^{\mathcal{D}}$  is a set of smallest cardinality  $\kappa$  not in  $\mathcal{S}$ . Then we can well-order  $\mathcal{A} = \{a_\xi \mid \xi \in \kappa\}$  and get  $\mathcal{A} = \bigcup_{\chi \in \kappa} \{a_\xi \mid \xi \in \chi\}$  as  $\kappa$  is infinite, so a limit ordinal. Therefore  $\mathcal{A}$  is a monotone union of sets in  $\mathcal{S}$  (by minimality of  $\kappa$ ), so in  $\mathcal{S}$ . Then  $\mathcal{S} = 2^{\mathcal{D}}$  so  $\mathcal{D} \in \mathcal{S}$  and therefore  $\bigcap \mathcal{D} \neq \emptyset$ .

## 5.5 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.

**Proof idea** Follows directly from the fact that projections of universal nets are universal, and a space is compact iff every universal net converges.

## 5.6 Urysohn's Lemma

For closed  $C_0, C_1$  in a T4 space  $X$  there is a continuous  $f : X \rightarrow [0, 1]$  with  $f|_{C_0} = 0$  and  $f|_{C_1} = 1$ .

**Proof idea** Construct by induction open sets  $U_q$  for  $q \in \mathbb{Q} \cap [0, 1]$  with  $C_0 \subseteq U_q \subseteq \bar{U}_q \subseteq U_r \subseteq \bar{U}_r \subseteq C_1^c$  for  $q < r$ . Then take  $f(x) := \inf\{q \in \mathbb{Q} \cap [0, 1] \mid x \in U_q\} \cup \{1\}$ .

## 5.7 Tietze's extension theorem

For closed  $C$  in a T4 space  $X$  and continuous  $f : C \rightarrow \mathbb{R}$  there is a continuous extension  $\tilde{f} : X \rightarrow \mathbb{R}$ .

## 5.8 Extension of uniformly continuous functions

Let  $S$  be a set in a metric space  $M$  and  $f : S \rightarrow \mathbb{R}$  uniformly continuous. Then  $f$  can be continuously extended to  $\tilde{f} : M \rightarrow \mathbb{R}$ .

**Proof idea** Use the following result: If  $X$  is a topological space and  $Y$  is T3, then for  $D \subseteq X$  and continuous  $f : D \rightarrow Y$  we can extend  $f$  to  $\bar{D} \rightarrow Y$  if

$$\forall x \in \partial D \exists y \in Y \forall (x_i)_{i \in I} \text{ net in } D : x_i \rightarrow x \Rightarrow f(x_i) \rightarrow y$$

This condition already determines the extension function  $\tilde{f}$ , and its continuity can be proven by contradiction. Assume a universal net  $(x_i)_{i \in I}$  in  $\bar{D}$  converges to  $x \in \bar{D}$  but not  $\tilde{f}(x_i) \rightarrow \tilde{f}(x)$ . Construct a net  $(w_j)_{j \in J}$  in  $D$  such that  $w_j \rightarrow x$  and  $\tilde{f}(w_j)$  is outside of the closure of a fixed neighborhood  $N$  of  $\tilde{f}(x)$ . This contradicts the assumption.



## 6 Discrete

### 6.1 Gamma Function

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

$$\Gamma(z) := \int_0^\infty t^{z-1} e^{-t} dt \quad \text{if } \operatorname{Re}(z) > 0$$
$$\frac{1}{\Gamma(z)} = \lim_{n \rightarrow \infty} \binom{n+z-1}{n} n^{1-z}$$

We get

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

## 7 Functional analysis

### 7.1 Minkowski-functional

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

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

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

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

## 7.4 Open mapping theorem

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

**Proof idea**

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

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  $0 \in \text{cl}(T(B_X))^\circ \neq \emptyset$ . 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  $y \in \epsilon B_Y \subseteq \text{cl}(T(B_X))$ . Recursively construct sequences  $(x_n)_{n \in \mathbb{N}}$  in  $X$  and  $(y_n)_{n \in \mathbb{N}}$  in  $Y$  with

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

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  $Y$  we 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  $y_n \rightarrow 0$  for  $n \rightarrow \infty$ .

## 7.5 Hahn-Banach dominated extension theorem

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

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

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

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,  $\hat{x} : X' \rightarrow \mathbb{K}$ ,  $\phi \mapsto \phi(x)$ ).

**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  $\text{cl}(T(B_X))$  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.  $\forall x \in X, \epsilon > 0 \exists \text{neighborhood } N \text{ of } x \forall x \in M : x(N) \subseteq B_\epsilon(x(s))$ ), 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, recursively construct subsequences

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

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  $K := \text{cl}(T(B_X))$  is compact metric space. For  $(y'_n)_{n \in \mathbb{N}}$  have

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

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

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

**Proof** Show (ii)  $\Leftrightarrow$  (iv), the rest is relatively easy. Let  $x' \in (\ker(T))^\perp$ . Then have  $z' : \text{ran}(T) \rightarrow \mathbb{K}$  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  $Z := \text{cl}(\text{ran}(T))$ . By the Hahn-Banach theorem, we can extend functionals on  $Z$  to functionals on  $Y$ , so  $\text{ran}(T') \simeq Z'$  by the isomorphism  $\text{ran}(T') \rightarrow Z', T'(y') \mapsto y'|_Z$ .

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

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

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

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

## 8.8 Projection theorem

Let  $H$  be a Hilbert space and  $K \subseteq H$  convex and closed. Then for  $x \in H$  the infimum  $\inf_{y \in K} \|y - x\|$  is reached by some  $y \in K$ . In particular, for  $U \subseteq H$  closed subspace,  $U^\perp$  is also closed and  $H = U \oplus U^\perp$  is a topological decomposition.

## 8.9 Frechet-Riesz representation theorem

Let  $H$  be a Hilbert space. Then a isometric, bijective, conjugate linear map is given by

$$\phi : H \rightarrow H', \quad y \mapsto \langle \cdot, y \rangle$$

**Proof** Show surjectivity, the rest is clear: For  $x' \in H'$  have that  $(\ker(x'))^\perp$  has dimension 1. By using 8.8 the claim follows.

## 8.10 Orthonormal bases

Let  $H$  be a Hilbert space and  $S \subseteq H$  a maximal orthonormal system. As

$$\left\langle x - \sum_{s \in F} \langle x, s \rangle s, x - \sum_{s \in F} \langle x, s \rangle s \right\rangle \geq 0 \Rightarrow \sum_{s \in F} |\langle x, s \rangle|^2 \leq \langle x, x \rangle$$

for finite  $F \subseteq S$ , get that  $\sum_{s \in S} \langle x, s \rangle s$  converges absolutely, and if  $x \in \text{cl}(\text{span}(S))$ , to  $x$ . For a maximal orthonormal system  $S \subseteq H$  have that  $\text{cl}(\text{span}(S)) = H$ , so it is an orthonormal basis.

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

**2.10** Each finitely 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  $\text{vol}(X) > 2^n \text{vol}(\Gamma)$ , 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  $K \rightarrow \mathbb{R}$  and  $s$  is the number of conjugate pairs of complex  $\mathbb{Q}$ -embeddings  $K \rightarrow \mathbb{C}$ .

## 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  $D \equiv 1 \pmod{4}$  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  $\dots = 4$  if this has no integral solution).

In the case  $D < 0$ , have that

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

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

$$N_{K|\mathbb{Q}}(\epsilon) = \frac{1}{4}(u^2 - d_K v^2) \in \{-1, 1\} \Rightarrow u^2 - d_K v^2 = \pm 4$$

By Dirichlet's unit theorem have fundamental unit  $\epsilon = \frac{1}{2}(u + v\sqrt{d_K})$  and as  $-\epsilon$  and  $\epsilon^{-1}$  together with  $-1$  also generate  $\mathcal{O}_K^*$ , we may assume  $u, v \geq 0$ . Therefore,  $\epsilon^k = \frac{1}{2}(x + y\sqrt{d_K})$  and as in

$$\frac{1}{2}(w + t\sqrt{d_K}) \frac{1}{2}(u + v\sqrt{d_K}) = \frac{1}{4}(wu + d_K tv + (ut + vw)\sqrt{d_K})$$

the part  $\frac{1}{4}(wu + d_K tv)$  is greater than  $\frac{1}{2}w$  as wlog  $u \geq 2$ , have that  $u, v$  must be the smallest solution of Pell's equation.

## 9.5 Ramification (de: Verzweigung)

Let  $\mathcal{R}$  be a Dedekind domain,  $K = \text{Quot}(\mathcal{R})$  and  $\mathcal{O}$  the integral closure of  $\mathcal{R}$  in an algebraic 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  $\mathfrak{p}\mathcal{O} = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_r^{e_r}$  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  $\mathfrak{p} = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_r^{e_r}$  for  $\mathfrak{B}_i = \mathfrak{p}\mathcal{O} + p_i(\alpha)\mathcal{O}$ , where the minimal polynomial  $p$  of  $\alpha$  splits into irreducible factors mod  $\mathfrak{p}\mathcal{O}$

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

Also have  $f_i = \deg(p_i)$