

# Collection of arbitrary mathematical facts

## Inhaltsverzeichnis

<b>1</b>	<b>Set Theory</b>	<b>3</b>
1.1	Zorn's Lemma . . . . .	3
1.2	Ultrafilter Lemma . . . . .	4
1.3	Product Cardinality . . . . .	4
1.3.1	Lemma . . . . .	4
1.4	Power Cardinality . . . . .	5
1.5	Ordinal arithmetic . . . . .	5
<b>2</b>	<b>Logic</b>	<b>6</b>
2.1	Deduction theorem . . . . .	6
2.2	Constant lemma . . . . .	6
2.3	Gödel's completeness theorem . . . . .	6
2.4	Compactness theorem . . . . .	7
2.5	Löwenheim-Skolem . . . . .	7
2.6	Separation lemma . . . . .	7
2.7	Vaught's test . . . . .	7
2.8	Quantifier elimination . . . . .	8
<b>3</b>	<b>Algebra</b>	<b>8</b>
3.1	Cauchy-Schwarz . . . . .	8
3.2	Sylow Theorems . . . . .	8
3.3	Mordell's inequality . . . . .	8
3.4	Facts about finite rings . . . . .	9
3.5	Chinese Remainder theorem . . . . .	10
3.6	Main theorem of finitely generated modules over PIDs . . . . .	10
3.7	Smith normal form . . . . .	10
3.8	The module $\mathbb{Z}^n$ . . . . .	10
3.9	Hilbert's basis theorem . . . . .	10
<b>4</b>	<b>Probabilities</b>	<b>11</b>
4.1	Chernoff-Hoeffding . . . . .	11

<b>5</b>	<b>Analysis</b>	<b>11</b>
5.1	Inequalities . . . . .	11
5.2	Transformation . . . . .	11
<b>6</b>	<b>Topology</b>	<b>12</b>
6.1	Separation axioms . . . . .	12
6.2	Universal nets . . . . .	12
6.3	Initial topologies . . . . .	12
6.4	Characterization of compactness . . . . .	12
6.5	Tychonoffs Theorem . . . . .	13
6.6	Urysohn's Lemma . . . . .	13
6.7	Tietze's extension theorem . . . . .	13
6.8	Extension of uniformly continuous functions . . . . .	13
<b>7</b>	<b>Discrete</b>	<b>14</b>
7.1	Gamma Function . . . . .	14
<b>8</b>	<b>Functional analysis</b>	<b>14</b>
8.1	Minkowski-functional . . . . .	14
8.2	Kolmogorov's normability criterion . . . . .	14
8.3	Baire's theorem . . . . .	15
8.4	Open mapping theorem . . . . .	15
8.4.1	Lemma . . . . .	15
8.5	Hahn-Banach dominated extension theorem . . . . .	15
8.6	Banach-Alaoglu . . . . .	16
<b>9</b>	<b>Operator theory</b>	<b>16</b>
9.1	Neumann series . . . . .	16
9.2	Riesz lemma . . . . .	16
9.3	Riesz Representation theorem . . . . .	16
9.4	Compact Operators and spaces . . . . .	17
9.5	Arzela-Ascoli . . . . .	17
9.6	Closed range theorem . . . . .	17
9.7	Projection theorem . . . . .	18
9.8	Frechet-Riesz representation theorem . . . . .	18
9.9	Spectra . . . . .	18
9.10	Decomposition compact operator . . . . .	19
9.11	Spectral theorem for compact, normal operators . . . . .	19
9.11.1	Lemma . . . . .	19
9.11.2	Lemma (Spectrum of compact operators) . . . . .	20
9.12	Singular value decomposition . . . . .	20
<b>10</b>	<b>(Algebraic) Number Theory</b>	<b>20</b>
10.1	Propositions . . . . .	20

10.2 Minkowski's theorem (Neukirch 4.4) . . . . .	20
10.3 The Class group (Neukirch 6.3) . . . . .	21
10.4 Dirichlet's unit theorem . . . . .	21
10.5 Square number fields . . . . .	21
10.6 Ramification (de: Verzweigung) . . . . .	22
10.7 Quadratic Reciprocity . . . . .	23
<b>11 Elliptic Curves</b>	<b>23</b>
11.1 Definition . . . . .	23
11.2 Picard group structure . . . . .	24
11.3 Isogenies . . . . .	25
11.4 Nonconstant isogenies are surjective . . . . .	25
<b>12 Computational Algebraic Number theory and Cryptanalysis</b>	<b>25</b>
12.1 Primality test . . . . .	25
12.2 Hidden Subgroup Problem . . . . .	27
<b>13 Algorithms</b>	<b>27</b>
13.1 Parameterized Algorithms design techniques . . . . .	27
13.2 Treewidth . . . . .	28

**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  $\mathcal{S} \subset \mathcal{U}$ , 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  $g$ .

## 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  $\text{card}(X) = \text{card}(X \times X)$ . For a proof, consider the following lemma

### 1.3.1 Lemma

Let  $f : \text{On} \rightarrow \text{On}$  be an increasing function with

- $f(\aleph_0) = \aleph_0$
- If  $\text{card}(\alpha) = \text{card}(\beta)$  then  $\text{card}(f(\alpha)) = \text{card}(f(\beta))$
- For limit ordinal  $\lambda$  have  $f(\lambda) = \bigcup_{\delta < \lambda} f(\delta)$

Then  $f(\aleph_\delta) = \aleph_\delta$  for each  $\delta \in \text{On}$ . This lemma is easy to show by transfinite induction.

**Proof** Consider the order  $\leq$  on  $\text{On}^2$  given by

$$(a_0, a_1) \leq (b_0, b_1) :\Leftrightarrow \begin{cases} \max\{a_0, a_1\} < \max\{b_0, b_1\} \vee \\ \max\{a_0, a_1\} = \max\{b_0, b_1\}, a_0 < b_0 \vee \\ \max\{a_0, a_1\} = \max\{b_0, b_1\}, a_0 = b_0, a_1 \leq b_1 \end{cases}$$

Then  $f : \text{On} \rightarrow \text{On}, \alpha \mapsto \text{ord}(\alpha \times \alpha)$  fulfills the conditions from the lemma.  $\square$

## 1.4 Power Cardinality

For an infinite set  $X$  and any set  $Y$  have  $\text{card}(X^Y) = \max\{\text{card}(X), \text{card}(\mathfrak{P}(Y))\}$ .

**Proof** Have bijections

$$\mathfrak{P}(Y)^Y \rightarrow (2^Y)^Y \rightarrow 2^{Y \times Y} \rightarrow \mathfrak{P}(Y^2)$$

So by the previous proposition,  $\text{card}(\mathfrak{P}(Y)^Y) = \text{card}(\mathfrak{P}(Y))$ . So in the case  $\text{card}(X) \leq \text{card}(\mathfrak{P}(Y))$  the claim is already shown.

Otherwise have  $\gamma = \text{card}(Y)$  and use a variant of the lemma 1.3.1, where all conditions and the result only hold for ordinals  $\geq \gamma$  to show that  $\text{card}(\mu^\gamma) = \text{card}(\mu)$  for all  $\mu \geq 2^\gamma$ .

Consider the order  $\leq$  on  $\text{On}^\gamma$  given by

$$(a_y)_y \leq (b_y)_y :\Leftrightarrow \begin{cases} \sup_y a_y < \sup_y b_y \vee \\ \sup_y a_y = \sup_y b_y, (a_y)_y \leq_{\text{lexiographic}} (b_y)_y \end{cases}$$

Then the function  $\text{On} \rightarrow \text{On}, \alpha \mapsto \text{ord}(\alpha^\gamma)$  fulfills the conditions of the modified lemma, and the claim follows as  $\text{card}(X) \geq 2^\gamma$ .  $\square$

## 1.5 Ordinal arithmetic

For  $\alpha, \beta \in \text{On}$  define  $\alpha + \beta := \text{ord}((\{0\} \times \alpha) \cup (\{1\} \times \beta))$  (with lexicographic ordering). Then have the following properties (which also define  $+$  by transfinite recursion)

- $\alpha + 0 = \alpha$
- $\alpha + (\beta + 1) = (\alpha + \beta) + 1$
- $\alpha + \lambda = \bigcup_{\beta < \lambda} \alpha + \beta$  for limit ordinal  $\lambda$

Furthermore have then

- $0 + \alpha = \alpha$
- $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
- $\alpha + \beta = \alpha + \gamma \Rightarrow \beta = \gamma$  (but in general not for right-addition)

Then define  $\cdot$  by  $\alpha \cdot \beta := \text{ord}(\alpha \times \beta)$  (with lexicographic ordering). Then have the following properties (which also define  $\cdot$  by transfinite recursion)

- $\alpha \cdot 0 = 0$
- $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$
- $\alpha \cdot \lambda = \bigcup_{\beta < \lambda} \alpha \cdot \beta$  for limit ordinal  $\lambda$

Furthermore have then

- $0 \cdot \alpha = 0$
- $1 \cdot \alpha = \alpha \cdot 1 = \alpha$
- $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$
- $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$  (but in general no right-distributivity)
- $\alpha \cdot \beta = \alpha \cdot \gamma, \alpha \neq 0 \Rightarrow \beta = \gamma$  (but in general not for right-multiplication)

## 2 Logic

### Definition Proof

In 1st order logic proofs, we allow Modus Ponens and Generalization, and the following base axioms:

$$\begin{aligned} & \{ \forall x \phi \rightarrow \phi(x/t) \mid x \text{ is free in } \phi \text{ for } t \} \cup \{ \forall (\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \forall x \psi) \mid x \text{ free in } \phi \} \\ & \cup \{ x = x \mid \} \cup \{ x = y \rightarrow (y = z \rightarrow x = z) \mid \} \\ & \cup \{ x = y \rightarrow (R(v_1, \dots, v_i, x, v_{i+1}, \dots, v_n) \rightarrow R(v_1, \dots, v_i, y, v_{i+1}, \dots, v_n)) \mid \} \\ & \cup \{ x = y \rightarrow (f(v_1, \dots, v_i, x, v_{i+1}, \dots, v_n) = f(v_1, \dots, v_i, y, v_{i+1}, \dots, v_n)) \mid \} \end{aligned}$$

### 2.1 Deduction theorem

Let  $\Sigma \subseteq \text{Fml}(\mathcal{L}), \phi \in \text{Sen}(\mathcal{L}), \psi \in \text{Fml}(\mathcal{L})$ . If  $\Sigma \cup \{\phi\} \vdash \psi$  then  $\Sigma \vdash (\phi \rightarrow \psi)$ .

### 2.2 Constant lemma

Let  $\phi_1, \dots, \phi_n, \phi \in \text{Fml}(\mathcal{L})$  and  $x$  a variable not occurring in the  $\phi, \phi_i$  and  $\mathcal{L}'$  an extension of  $\mathcal{L}$  by a constant  $c$ . If  $\phi_1, \dots, \phi_n \vdash_{\mathcal{L}'} \phi$  then  $\phi_1(c/x), \dots, \phi_n(c/x) \vdash_{\mathcal{L}} \phi(c/x)$ .

### 2.3 Gödel's completeness theorem

Let  $\Sigma \subseteq \text{Fml}(\mathcal{L})$  and  $\alpha \in \text{Sen}(\mathcal{L})$ . If  $\Sigma \not\vdash \alpha$  then there is a model  $\mathcal{M}$  of  $\Sigma$  with  $\mathcal{M} \not\models \alpha$ .

**Proof idea** First we construct a witness extension for  $\Sigma$ , so an extension by constants  $\mathcal{L}'$  of  $\mathcal{L}$  and a consistent set  $\Sigma' \supseteq \Sigma$  of  $\mathcal{L}'$ -sentences such that whenever  $\Sigma' \vdash \exists x \phi$  for an  $\mathcal{L}'$ -formula  $\phi$  with the only free variable  $x$  have  $\Sigma' \vdash \phi(x/c_\phi)$  for a constant  $c_\phi$ . This can be done by recursively adding witnesses for each suitable formula and then unifying the chain of languages that were created.

Now have  $\Sigma \cup \{\neg\alpha\}$  is consistent, so contained in a maximally consistent theory  $T$ . Repeatedly considering witness extensions and maximally consistent supertheories, get that wlog  $T$  is a witness extension of  $\Sigma \cup \{\neg\alpha\}$ . Using this, construct a model where the universe are all variable-free terms of  $\mathcal{L}'$  modulo  $T$ -provable equality. This is then a model of  $\Sigma \cup \{\neg\alpha\}$  and the claim follows.

## 2.4 Compactness theorem

Let  $\Sigma \subseteq \text{Sen}(\mathcal{L})$ . If every finite subset of  $\Sigma$  has a model, then  $\Sigma$  has a model.

## 2.5 Löwenheim-Skolem

Let  $\Sigma \subseteq \text{Sen}(\mathcal{L})$ .

- If  $\Sigma$  has a model, then it has one of cardinality  $\leq \kappa_{\mathcal{L}}$
- If  $\Sigma$  has an infinite model, then it has one of cardinality  $\kappa$  for each  $\kappa \geq \kappa_{\mathcal{L}}$

**Proof idea** The construction in 2.3 creates a model of cardinality  $\leq \kappa_{\mathcal{L}}$ . Greater models can be constructed by adding as many constants and unequal-axioms to  $\Sigma$  (stays consistent by the compactness theorem).

## 2.6 Separation lemma

Let  $\Sigma_1, \Sigma_2, \Gamma \subseteq \text{Sen}(\mathcal{L})$ . If for each  $\mathcal{M}_1 \models \Sigma_1$  and  $\mathcal{M}_2 \models \Sigma_2$  have  $\gamma \in \Gamma$  that separates them (i.e.  $\mathcal{M}_1 \models \gamma, \mathcal{M}_2 \models \neg\gamma$ ), then there is  $\gamma^* = \bigvee_i \bigwedge_j \gamma_{ij}$  with  $\gamma_{ij} \in \Gamma$  separating  $\text{Mod}_{\mathcal{L}}(\Sigma_1)$  and  $\text{Mod}_{\mathcal{L}}(\Sigma_2)$  (i.e.  $\text{Mod}_{\mathcal{L}}(\Sigma_1) \subseteq \text{Mod}_{\mathcal{L}}(\gamma^*)$  and  $\text{Mod}_{\mathcal{L}}(\Sigma_2) \subseteq \text{Mod}_{\mathcal{L}}(\neg\gamma^*)$ ).

**Proof idea** Use the compactness theorem twice on covers by  $\text{Mod}_{\mathcal{L}}(\gamma), \gamma \in \Gamma$ .

## 2.7 Vaught's test

Let  $T$  be an  $\mathcal{L}$ -theory. If  $T$  has only infinite models and is  $\kappa$ -categorical for some  $\kappa \geq \kappa_{\mathcal{L}}$ , then  $T$  is complete.

**Proof** If  $T \cup \{\alpha\}$  and  $T \cup \{\neg\alpha\}$  would be consistent, Löwenheim-Skolem yields corresponding models of cardinality  $\kappa$ , which then are isomorphic. This is a contradiction.  $\square$

## 2.8 Quantifier elimination

A set  $\Sigma \subseteq \text{Sen}(\mathcal{L})$  has quantifier elimination, if any of the following equivalent definitions are fulfilled:

- for every  $\mathcal{L}$ -formula  $\phi$  there is a quantifier-free  $\mathcal{L}$ -formula  $\psi$  with no additional free variables such that  $\Sigma \vdash \phi \leftrightarrow \psi$ .
- for every substructure  $\mathcal{A}$  of a model of  $\Sigma$  have that  $\Sigma \cup \mathcal{D}(\mathcal{A}) \subseteq \text{Sen}(\mathcal{L}(\mathcal{A}))$  is complete.
- for every two models  $\mathcal{M}_1, \mathcal{M}_2$  of  $\Sigma$  and a joint substructure  $\mathcal{A}$  of  $\mathcal{M}_1$  and  $\mathcal{M}_2$  have that:

$$(\mathcal{M}_1, \text{id}_{|\mathcal{A}|}) \models \phi \Leftrightarrow (\mathcal{M}_2, \text{id}_{|\mathcal{A}|}) \models \phi$$

for every formula  $\phi \in \text{Sen}(\mathcal{L}(\mathcal{A}))$  of the form  $\phi = \exists x \psi$  with a quantifier-free  $\psi$ .

## 3 Algebra

### 3.1 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

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

### 3.2 Sylow Theorems

For a finite group  $G$  with  $|G| = n = p^e m$ ,  $p \in \mathbb{P}$ ,  $p \nmid m$  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  $s \mid m$  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.

### 3.3 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  $\|x\| = \lambda(L^*)$ .

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

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

### 3.4 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  $\mathbb{F}_q$ .

- if  $p > 2$  is prime then  $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$  is cyclic with generator  $g$  or  $g + p$ , where  $g \in \mathbb{F}_p^*$  is a generator of  $\mathbb{F}_p^*$ .

**Proof** First we show: If  $a^p \equiv 1 \pmod{p^\alpha}$  then  $a \equiv 1 \pmod{p^\beta}$  for all  $\beta < \alpha$  where  $\alpha \geq 2$ . If  $\beta = 1$  this is clear as  $p \mid a^p - 1$  iff  $p \mid a - 1$  as  $a^p \equiv a \pmod{p}$ . This shows the claim

So now let  $\beta > 1$ . Have  $p^\alpha \mid a^p - 1$  and by IH also  $p^{\beta-1} \mid a - 1$ . It follows that  $a = 1 + lp^{\beta-1}$  for some  $l \in \mathbb{Z}$  and we have

$$1 \equiv a^p \equiv (1 + lp^{\beta-1})^p = \sum_{k=0}^p \binom{p}{k} l^k p^{k(\beta-1)} \equiv 1 + lp^\beta \pmod{p^{\beta+1}}$$

as  $\beta+1 \leq \alpha$  and  $p^{\beta+1} \mid pp^{2\beta-2} \mid \binom{p}{k} p^{k\beta-2}$  for  $k \geq 2$ . Therefore  $p \mid l$  and so  $a \equiv 1 \pmod{p^\beta}$ .

We have for each prime  $l \mid p-1$  that

$$g^{p^{\alpha-1} \frac{p-1}{l}} \equiv 1 \pmod{p^\alpha} \Rightarrow g^{p^{\alpha-1} \frac{p-1}{l}} \equiv g^{\frac{p-1}{l}} \equiv 1 \pmod{p}$$

where the latter is a contradiction as  $g$  is a generator of  $\mathbb{F}_p^*$ . Therefore,  $g$  is a generator of  $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$  iff

$$g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$$

By using the claim recursively, this is implied by  $g^{p-1} \not\equiv 1 \pmod{p^2}$ . We have that

$$(g+p)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} g^{p-1-k} p^k \equiv g^{p-1} + (p-1)g^{p-2}p \equiv g^{p-1} - pg^{p-2} \pmod{p^2}$$

So if  $g^{p-1} \equiv 1$  then this is  $1 - pg^{-1} \not\equiv 1$  as  $g^{-1}$  is a unit in  $\mathbb{Z}/p^2\mathbb{Z}$ , so  $pg^{-1} \not\equiv 0$ . Hence  $g^{p-1} \not\equiv 1$  or  $(g+p)^{p-1} \not\equiv 1$  and as both  $g$  and  $g+p$  are generators of  $\mathbb{F}_p^*$ , this implies that one of them is a generator of  $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ .  $\square$

### 3.5 Chinese Remainder theorem

Let  $R$  be any commutative ring. For pairwise coprime ideals  $I_1, \dots, I_n \leq R$  have

$$R/(I_1 \cdot \dots \cdot I_n) \cong R/I_1 \times \dots \times R/I_n$$

### 3.6 Main theorem of finitely generated modules over PIDs

Let  $R$  be a principal ideal domain and  $M$  a finitely generated  $R$ -module. Then

$$M \cong R^d \oplus \bigoplus_{p \in \mathcal{P}} \bigoplus_{j \in \{1, \dots, n_p\}} R/(p^{e_{pj}})$$

where  $\mathcal{P} \subseteq R$  is a set of prime elements and  $n_p \in \mathbb{N}_{>0}$  for  $p \in \mathcal{P}$ . The set  $\mathcal{P}$  is unique, as are the exponents  $e_{pj}$  (up to order).

By the Chinese Remainder theorem, we get for finitely generated abelian groups  $G$  that

$$G \cong \mathbb{Z}^d \oplus \bigoplus_{j \in \{1, \dots, s\}} \mathbb{Z}/n_j\mathbb{Z}$$

for  $n_1 | n_2 | \dots | n_s$  with  $s \in \mathbb{N}$ .

### 3.7 Smith normal form

Let  $A \in R^{m \times n}$  for a principal ideal domain  $R$ . Then there are  $U \in \text{SL}_m(R)$  and  $V \in \text{SL}_n(R)$  such that

$$UAV = \text{diag}(n_1, \dots, n_s, 0, \dots, 0) \in R^{m \times n}$$

where  $n_1 | n_2 | \dots | n_s$  with  $s \in \mathbb{N}$ .

### 3.8 The module $\mathbb{Z}^n$

$\mathbb{Z}^n$  is a free, Noetherian  $\mathbb{Z}$ -module.

### 3.9 Hilbert's basis theorem

If  $R$  is a Noetherian ring, then so is  $R[s_1, \dots, s_n]$  for  $s_1, \dots, s_n \in S$  with a ring extension  $S \supseteq R$ .

## 4 Probabilities

### 4.1 Chernoff-Hoeffding

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

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

## 5 Analysis

### 5.1 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

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

### 5.2 Transformation

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

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

## 6 Topology

### 6.1 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

### 6.2 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.

### 6.3 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  $f_\alpha : X \rightarrow (X_\alpha, \tau_\alpha)$ .

### 6.4 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  $\bigcap \mathcal{D} \neq \emptyset$ .

## 6.5 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.

## 6.6 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  $f(x) := \inf\{q \in \mathbb{Q} \cap [0, 1] \mid x \in U_q\} \cup \{1\}$ .

## 6.7 Tietze's extension theorem

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

**Proof idea** Prove extension of  $f : C \rightarrow ]-1, 1[$  to  $\tilde{f} : X \rightarrow ]-1, 1[$ , then the result follows by using a homeomorphism  $] - 1, 1[ \rightarrow \mathbb{R}$ . By Urysohn's Lemma, it suffices to extend  $f : C \rightarrow [-1, 1]$  to  $\tilde{f} : X \rightarrow [-1, 1]$ . For this, construct a sequence  $h_n : X \rightarrow (\frac{2}{3})^n [-\frac{1}{3}, \frac{1}{3}]$  of continuous functions such that  $\sum_n h_n$  converges uniformly.

## 6.8 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.

## 7 Discrete

### 7.1 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

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

## 8 Functional analysis

### 8.1 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

### 8.2 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.

### 8.3 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

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

### 8.4 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:

#### 8.4.1 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  $n \rightarrow \infty$ .

### 8.5 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  $F$ .

## 8.6 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

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

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

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

## 9 Operator theory

### 9.1 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.

### 9.2 Riesz lemma

Let  $U \subsetneq X$  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.

### 9.3 Riesz Representation theorem

Let  $K$  be a compact metric space (compact Hausdorff space??). Consider  $(C(X), \|\cdot\|_\infty)$  and the space of complex regular Borel measures  $M(X)$  on  $X$ . Then  $C(K)' \cong M(K)$  under

$$M(K) \rightarrow C(K)', \quad \mu \mapsto \left( f \mapsto \int_K f d\mu \right)$$



## 9.4 Compact Operators and spaces

From 9.2 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.

## 9.5 Arzela-Ascoli

Let  $X$  be a compact metric 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  $X = \text{cl}(\{s_n \mid n \in \mathbb{N}\})$ . 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  $\|\cdot\|_\infty$ .

## 9.6 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 8.4.1. It follows that  $\text{ran}(T) = \text{ran}(\tilde{T})$  is closed, as  $X$  is closed.

## 9.7 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.

**Proof** We have  $\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2$ . For any sequence  $(x_n)_n$  in  $K$  that has  $\|x_n - x\| \rightarrow d := \inf_{y \in K} \|y - x\|$  we then have:

$$\frac{1}{4}\|x_n - x_m\|^2 \leq \frac{1}{2}\|x_n - x\|^2 + \frac{1}{2}\|x_m - x\|^2 - \underbrace{\left\| \frac{1}{2}x_n + \frac{1}{2}x_m - x \right\|^2}_{\in K}$$

If we choose  $n, m$  large enough that  $\|x_n - x\|^2, \|x_m - x\|^2 \leq d^2 + \epsilon$  then it follows

$$\frac{1}{4}\|x_n - x_m\|^2 \leq d^2 + \epsilon - d^2 = \epsilon \quad \text{so} \quad \|x_n - x_m\| \leq 4\epsilon$$

So  $(x_n)_n$  is a Cauchy sequence and converges to the searched point  $y \in K$  (as  $K$  is closed).

## 9.8 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 9.7 the claim follows.

## 9.9 Spectra

Let  $T \in \mathcal{L}(X)$  for a Banach space  $X$ . With

$$\begin{aligned} \text{point spectrum} \quad \sigma_p(T) &:= \{\lambda \in \mathbb{K} \mid \ker(T - \lambda) \neq \emptyset\} \\ \text{continuous spectrum} \quad \sigma_c(T) &:= \{\lambda \in \mathbb{K} \mid \ker(T - \lambda) = \emptyset, \text{cl}(\text{im}(T - \lambda)) \neq X\} \\ \text{residual spectrum} \quad \sigma_r(T) &:= \{\lambda \in \mathbb{K} \mid \ker(T - \lambda) = \emptyset, \text{cl}(\text{im}(T - \lambda)) = X, \text{im}(T - \lambda) \neq X\} \\ \text{spectrum} \quad \sigma(T) &:= \sigma_p(T) \cup \sigma_c(T) \cup \sigma_r(T) \end{aligned}$$

have that  $\sigma(T)$  compact and bounded by  $\|T\|_{\text{op}}$ .

**Proof idea** Use the Neumann series.

### 9.10 Decomposition compact operator

Let  $T \in \mathcal{K}(X)$  for Banach space  $X$ . Then  $X = \ker((T - 1)^p) \oplus \text{im}((T - 1)^p)$  for some  $p \in \mathbb{N}$  (where the direct sum is a decomposition in the topological sense).

**Proof idea** Show that the sequence of  $N_i = \ker((T - 1)^i)$  is stationary. Assume not, then have  $x_i \in N_i$  with  $\|x_i\| = 1$  and distance  $\frac{1}{2}$  to  $N_{i-1}$  by Riesz Lemma. Applying  $T$  then yields a non-Cauchy sequence as for  $m < n$  have

$$Tx_n - Tx_m = x_n - x_m + (T - 1)(x_n - x_m) \in x_n - x_m + \underbrace{\ker((T - 1)^{n-1})}_{=N_{n-1}}$$

a contradiction to the compactness of  $T$ . Similar show that  $\text{im}((T - 1)^i)$  is stationary and for an index  $p \in \mathbb{N}$  at which both are constant the claim holds. The closedness of  $\text{im}((T - 1)^p)$  follows as  $(T - 1)^p$  is open by the open mapping theorem.  $\square$

### 9.11 Spectral theorem for compact, normal operators

Let  $T \in \mathcal{K}(H)$  on a Hilbert space  $H$  be normal (if  $\mathbb{K} = \mathbb{C}$ ) resp. self-adjoint (if  $\mathbb{K} = \mathbb{R}$ ). Then there is a countable orthonormal system  $E$  and  $\lambda_e \in \mathbb{K} \setminus \{0\}$  for  $e \in E$  such that

$$T = \sum_{e \in E} \lambda_e \langle \cdot, e \rangle e$$

Additionally,  $\{\lambda_e \mid e \in E\}$  has 0 as only accumulation point, is bounded by  $\|T\|_{\text{op}}$  and  $\lambda_e$  takes the same value for only finitely many  $e \in E$ . Also  $H = \ker T \oplus \text{cl}(\text{span}(E))$ .

**Proof** For  $\lambda, \mu \in \sigma(T)$  with  $\lambda \neq \mu$  have that  $\ker(T - \lambda) \perp \ker(T - \mu)$  as  $\mu v = Tv = \lambda v$  implies  $v = 0$ . Therefore, take for  $\lambda \in \sigma(T)$  orthonormal basis  $\{e_{\lambda,1}, \dots, e_{\lambda,n_\lambda}\}$  of  $\ker(T - \lambda)$  and set

$$E = \{e_{\lambda,i} \mid \lambda \in \sigma(T) \setminus \{0\}\}, \quad \lambda_{e_{\lambda,i}} = \lambda$$

Now consider  $H_2 := (\ker T + \text{cl}(\text{span}(E)))^\perp$ . Then  $T(H_2) \subseteq H_2$  and  $T_2 := T|_{H_2} : H_2 \rightarrow H_2$  is compact and self-adjoint. If  $T_2 = 0$  then  $\ker(T_2) \subseteq H_2 \cap \ker(T) = \{0\}$  so we are done. So assume  $T_2 \neq 0$ . Then  $T_2 x = \lambda x$  for some  $\lambda \neq 0$  (see next lemma). However, then  $x \in \ker(T - \lambda)$ , a contradiction. The rest of the proposition follows from the two lemmas:

#### 9.11.1 Lemma

A compact operator  $T \in \mathcal{K}(H)$  that is normal (if  $\mathbb{K} = \mathbb{C}$ ) resp. self-adjoint (if  $\mathbb{K} = \mathbb{R}$ ) has  $\lambda \in \sigma(T)$  where  $|\lambda| = \|T\|_{\text{op}}$ .

### 9.11.2 Lemma (Spectrum of compact operators)

Let  $T \in \mathcal{K}(X)$ . Then  $\sigma(T)$  is countable with only accumulation point 0.

**Proof idea** Assume there are infinitely many  $\lambda_n \in \sigma(T)$  pairwise distinct with  $|\lambda_n| > \epsilon > 0$ . By 9.10 each  $T - \lambda_n$  is injective iff surjective, so have  $Tx_n = \lambda_n x_n$  for non-zero  $x_n$ . It follows that they are linearly independent. By Riesz lemma, have  $y_n \in \text{span}\{x_1, \dots, x_n\}$  with distance  $\frac{1}{2}$  to  $\text{span}\{x_1, \dots, x_{n-1}\}$  and  $\|y_n\| = 1$ . Then  $Ty_n$  has distance  $\frac{1}{2}\epsilon$  from  $\text{span}\{Tx_1, \dots, Tx_{n-1}\}$ , but this contradicts the compactness of  $T$ .

### 9.12 Singular value decomposition

Let  $T \in \mathcal{K}(H_1, H_2)$ . Then there is  $N = \{1, \dots, n\}$  or  $N = \mathbb{N}$  and orthonormal systems  $\{e_n \mid n \in N\}$  of  $H_1$  and  $\{f_n \mid n \in N\}$  of  $H_2$  and  $\{s_n \mid n \in N\} \subseteq \mathbb{R}_{>0}$  with 0 as only accumulation point such that

$$T = \sum_{n \in N} s_n \langle \cdot, e_n \rangle f_n$$

**Proof idea** The operator  $T^* \circ T$  is positive, self-adjoint and compact, so has a unique positive, self-adjoint compact root  $S$  with  $S \circ S = T^* \circ T$  (take the root of each eigenvalue in the representation of 9.11). Then  $T = U \circ S$  for a unitary operator  $U$  and with  $S = \sum_{e \in E} \lambda_e \langle \cdot, e \rangle e$  have that

$$T = \sum_{e \in E} \lambda_e \langle \cdot, e \rangle Ue$$

which is of the specified form. □

## 10 (Algebraic) Number Theory

### 10.1 Propositions

Let  $K|\mathbb{Q}$  separable and  $\mathcal{O}_K$  integral closure of  $\mathbb{Z}$ . The following basic propositions can be found in Neukirch's book.

**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).

### 10.2 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  $X \cap \Gamma \neq \emptyset$ .

### 10.3 The Class group (Neukirch 6.3)

Let  $K$  be a number field with ring of integers  $\mathcal{O}_K$ . Then the set of fractional ideals is a group and the principal ideals form a subgroup. The quotient group is finite and called the class group  $\text{Cl}_K$ . In particular, every  $c \in \text{Cl}_K$  contains an integral ideal  $I$  of norm

$$N(I) := [\mathcal{O}_K : I] \leq M_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}$$

where  $s$  is the number of pairs of complex embeddings  $K \rightarrow \mathbb{C}$  and  $n = [K : \mathbb{Q}]$ .

**Proof idea** Consider an equivalence class  $[\mathfrak{a}]$ . Then  $\gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$  for some  $\gamma \in \mathcal{O}_K$ . By Minkowski's theorem, there is a  $a \in \gamma\mathfrak{a}^{-1}$  of norm

$$N_{K|\mathbb{Q}}(a) \leq \left(\frac{2}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|} N(\gamma\mathfrak{a}^{-1}) = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|} N(\gamma) N(\mathfrak{a})^{-1}$$

Therefore for the ideal  $a\gamma^{-1}\mathfrak{a}$  in  $[\mathfrak{a}]$  we have

$$N(a\gamma^{-1}\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|d_K|}$$

This is integral, as  $(\gamma) = \gamma\mathfrak{a}^{-1}\mathfrak{a} \mid a\mathfrak{a}$ . □

### 10.4 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  $K \rightarrow \mathbb{C}$ .

### 10.5 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,  $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{d_K})]$ .

In the case  $D > 1$ , have that  $\mathcal{O}_K^* = \langle \epsilon_1 \rangle$ , where  $\epsilon_1 = \frac{1}{2}(x + y\sqrt{d})$  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.

## 10.6 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 and separable field extension  $L|K$ . Then  $\mathcal{O}$  is a Dedekind domain.

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

**8.2** Have  $\sum e_i f_i = n := [L : K]$  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  $\alpha \in \mathcal{O}$ . If  $\mathfrak{p}$  is a prime ideal that does not divide the leader  $\mathcal{F}$  of  $\mathcal{R}[\alpha]$  (the largest ideal contained in  $\mathcal{R}[\alpha]$ ), 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  $f_i = \deg(p_i)$ .

By definition of  $\mathcal{F}$ , note that for a number field  $K$  (i.e.  $\mathcal{R} = \mathbb{Z}$ ) it is sufficient if  $\mathfrak{p} = (p) \nmid ([\mathcal{O} : \mathbb{Z}[\alpha]])$ .

If  $L|K$  is galoisch, we can consider the effect of the Galois group on the prime ideals  $\mathfrak{B} \leq \mathcal{O}$  over some prime ideal  $\mathfrak{p} \leq \mathcal{R}$ . Fix some prime ideal  $\mathfrak{B} \leq \mathcal{O}$  over  $\mathfrak{p}$  and consider

$$\begin{aligned} \text{"Zerlegungsgruppe"} \quad G_{\mathfrak{B}} &:= \{\sigma \in G \mid \sigma\mathfrak{B} = \mathfrak{B}\} && \text{with fixed field } Z_{\mathfrak{B}} = L^{G_{\mathfrak{B}}} \\ \text{"Trägheitsgruppe"} \quad I_{\mathfrak{B}} &:= \ker(\phi) && \text{with fixed field } T_{\mathfrak{B}} = L^{I_{\mathfrak{B}}} \end{aligned}$$

where

$$\phi_{\sigma} : \mathcal{O}/\mathfrak{B} \rightarrow \mathcal{O}/\mathfrak{B}, \quad [a] \mapsto [\sigma a]$$

Let then be  $e$  resp.  $f$  be the “Verzweigungsindex” (maximal power such that  $\mathfrak{B}^e | \mathfrak{p}$ ) resp. “Trägheitsindex” (the index of  $\mathcal{O}/\mathfrak{B} | \mathcal{R}/\mathfrak{p}$ ) of  $\mathfrak{B}$  over  $\mathfrak{p}$ . If  $\mathcal{O}/\mathfrak{B} | \mathcal{R}/\mathfrak{p}$  is separable, have the following representation:

$$\mathfrak{p} \begin{array}{c} \frac{1}{\subseteq} \\ 1 \end{array} \mathfrak{B}_Z := \mathfrak{B} \cap Z_{\mathfrak{B}} \begin{array}{c} \frac{f}{\subseteq} \\ 1 \end{array} \mathfrak{B}_T := \mathfrak{B} \cap T_{\mathfrak{B}} \begin{array}{c} \frac{1}{\subseteq} \\ e \end{array} \mathfrak{B}$$

where the “Verzweigungsindizes” are written over the corresponding ideal decompositions and the “Trägheitsindizes” are written below, respectively.

## 10.7 Quadratic Reciprocity

For  $a \in \mathbb{Z}$  and  $p \in \mathbb{P}$  and  $n = \prod_p p^{e_p} \in \mathbb{N}_{\geq 2}$  define

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if there is } x \text{ with } a \equiv x^2 \pmod{p} \\ -1 & \text{otherwise} \end{cases} \quad \text{and} \quad \left(\frac{a}{n}\right) := \prod_p \left(\frac{a}{p}\right)^{e_p}$$

Then for odd  $a, n$  have

$$\left(\frac{a}{n}\right) = \begin{cases} -\left(\frac{n}{a}\right) & \text{if } a \equiv n \equiv 3 \pmod{4} \\ \left(\frac{n}{a}\right) & \text{otherwise} \end{cases} \quad \text{and} \quad \left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8} \\ -1 & \text{if } n \equiv \pm 3 \pmod{8} \end{cases}$$

## 11 Elliptic Curves

Let  $\mathbb{P}^2 := \mathbb{P}_{\bar{K}}^2$  be the 2 dimensional projective space over the algebraic closure  $\bar{K}$  of a field  $K$ . Furthermore, denote a rational map  $\phi$  defined on a variety  $V$  that is given by  $\phi_1, \dots, \phi_n \in K(V)$  with homogeneous, equal-degree numerators and denominators by  $\phi = [\phi_1, \dots, \phi_n]$ .

### 11.1 Definition

An elliptic curve is a pair  $(E, O)$  where  $E$  is a nonsingular curve of genus one in  $\mathbb{P}^2$  and  $O \in E$ . It can be shown (Arithmetic of Elliptic Curves, III 3.1) that if  $E$  is defined over  $K$  there is always an (variety-) isomorphism  $[x, y, 1]$  that maps

$$[x, y, 1] : E \rightarrow \mathcal{Z} \left( (Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6)^{\text{hom}} \right)$$

for  $a_1, \dots, a_6 \in K$  where the defining polynomial is also called Weierstraß equation. If  $\text{char}(K) \notin \{2, 3\}$  then there is even a degree-1 isomorphism between  $\text{im}[x, y, 1]$  and a curve of the form

$$E' = \mathcal{Z} \left( (Y^2 - X^3 - AX - B)^{\text{hom}} \right)$$

Usually we do not explicitly mention the homogenization or the projective nature and say the projective curve  $E' = \mathcal{Z}((f - g)^{\text{hom}})$  is given by the equation  $E' : f = g$ .

For a curve  $E'$  given by the last equation, define the discriminant

$$\Delta(E') := -16(4A^3 + 27B^2)$$

and the j-invariant

$$j(E') := -1728 \frac{64A^3}{\Delta}$$

For an elliptic curve  $E$  given by  $E : Y^2 + a_1XY + a_3Y - X^3 + a_2X^2 + a_4X + a_6$  also define a group law on  $E$  via

$$\begin{aligned} -(x_1, y_1) &:= (x_1, -y_1 - a_1x_1 - a_3) \\ \lambda &:= \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1}{2y_1 + a_1x_1 + a_3} & \text{otherwise} \end{cases} \\ x_3 &:= -x_1 - x_2 - a_2 + \lambda(\lambda + a_1) \\ (x_1, y_1) + (x_2, y_2) &:= (x_3, -y_1 - a_3 - a_1x_3 + \lambda(x_1 - x_3)) \end{aligned}$$

It can be shown that this group law has the following geometric interpretation: For  $P, Q \in E$  there is exactly one line through  $P$  and  $Q$  (with multiplicity, i.e. if  $P = Q$  then this is the tangent line). Then  $-(P + Q)$  is defined as the third point of intersection of this line with  $E$ .

## 11.2 Picard group structure

Let  $(E, O)$  be an elliptic curve. Then the map

$$\sigma : \text{Div}^0(E) \rightarrow E, \quad D \mapsto \text{unique point } (P) \sim D + (O)$$

is well-defined, surjective and  $\sigma(D_1) = \sigma(D_2)$  iff  $D_1 \sim D_2$ . Furthermore

$$\bar{\sigma} : \text{Pic}^0(E) \rightarrow E, \quad \bar{D} \mapsto \sigma(D)$$

is a group isomorphism. From the number theoretic perspective,  $K[E] = K[x, y] = K[X, Y]/(Y^2 - f(X))$  is a Dedekind domain and the map

$$\phi : E \rightarrow \text{Cl}(K[E]), \quad (\lambda : \mu : 1) \mapsto \overline{\langle x - \lambda, y - \mu \rangle}, \quad (0 : 0 : 1) \mapsto \overline{\langle 1 \rangle}$$

is a group isomorphism.

**Proof** See (Arithmetic of Elliptic Curves, III 3.4) for the first part. To show that  $K[E]$  is a Dedekind domain, note that  $K[x]$  is and hence the integers  $B$  in  $K(E)$  are. Now  $K[E]$  is an order in  $B$  and as  $d(K[E])$  is square-free, it must already be the maximal order  $B$ .

That  $\phi$  is injective follows from a lengthy elementary computation and a degree argument (note that  $f$  has odd degree), for details see Cryptanalysis lecture. By unique factorization of ideals,  $\text{Cl}(K[E])$  is generated by  $\text{im } \phi$ . Note that  $\langle x - \lambda, y - \mu \rangle \langle x - \lambda, y + \mu \rangle =$



$\langle x - \lambda \rangle$  is principal, so  $\text{im}\phi$  is inversion-closed. Lastly show that  $\text{im}\phi$  is addition-closed. I think it should be possible to compute the third point on the line and show that the product of the respective ideals is principal. In Cryptanalysis, a more complex approach was chosen, so check this again.  $\square$

### 11.3 Isogenies

Let  $\psi : E_1 \rightarrow E_2$  be an isogeny between elliptic curves  $E_1, E_2$ , i.e. a morphism  $\psi$  satisfying  $\psi(O) = O$ . Then  $\psi$  is group homomorphism.

**Proof** If  $\psi$  is a morphism, then

$$\psi^* : K[E_2] \rightarrow K[E_1], \quad \bar{f} \mapsto \overline{f(\psi)}$$

is a ring homomorphism. In particular,  $\psi^*$  is also a group isomorphism between the class groups. Now have  $\psi = \phi^{-1} \circ \psi^* \circ \phi$  for the  $\phi$  from 11.2.

This proposition is also useful if one applies it to the isomorphism between any elliptic curve and a corresponding elliptic curve given in Weierstraß form. For this, see Arithmetic of Elliptic Curves, III 4.8) which uses a similar idea with  $\psi_*$  between the Picard groups.  $\square$

### 11.4 Nonconstant isogenies are surjective

Let  $E_1, E_2$  be elliptic curves and  $\phi : E_1 \rightarrow E_2$  an isogeny. Then  $\phi$  is either constant or surjective (note that it is crucial that the points of  $E_1$  resp.  $E_2$  are in  $\mathbb{P}^2 = \mathbb{P}_L^2$  for an algebraically closed field  $L|K$ ).

The statement follows directly from this theorem of algebraic geometry: A morphism between irreducible projective curves is either constant or surjective.

## 12 Computational Algebraic Number theory and Cryptanalysis

### 12.1 Primality test

Let  $n \in \mathbb{N}_{>2}$  be odd with  $n - 1 = d2^s$ ,  $d \perp 2$  and consider

$$U_n := \{a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv 1 \pmod{n}\} \leq \mathbb{Z}_n^* \quad (\text{Fermat})$$

$$V_n := \{x \in \mathbb{Z}_n^* \mid x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right) \pmod{n}\} \leq \mathbb{Z}_n^* \quad (\text{Solovay-Strassen})$$

$$W_n := \{a \in \mathbb{Z}_n^* \mid a^d \equiv 1 \text{ or } a^{2^r d} \equiv -1 \text{ for some } r < s\} \quad (\text{Miller-Rabin})$$

If  $n$  is prime, then  $U_n = V_n = W_n = \mathbb{Z}_n^*$  and otherwise,  $V_n, W_n \neq \mathbb{Z}_n^*$ . Furthermore, if  $n$  is composite, then  $\#W_n \leq \frac{1}{4}n$ .

**Proof** That  $U_n, V_n \leq \mathbb{Z}_n^*$  are subgroups can be seen easily (note that  $(\frac{\cdot}{n})$  is multiplicative). Similarly, see that  $V_n \subseteq U_n$  and if  $n$  is prime, then all are equal by using that  $\mathbb{Z}_n^*$  is cyclic.

For the other parts, use some key ideas: First, for each prime  $p$  (so in particular for  $p|n$ ) have  $\mathbb{Z}_p^*$  is cyclic of even order (wlog  $n$  odd) and we get that  $a$  is a square if  $2\text{ord}[a]_p \mid p-1$ . Furthermore, we have the CRT and if  $a^k \equiv -1$  then  $[a]_p^k = [-1]$  for each prime factor  $p|n$ .

If  $n = \prod_i p_i^{e_i}$  is composite, consider  $x \in \mathbb{Z}_n^*$  which is congruent to a non-square modulo  $p_1$  and congruent to 1 modulo every other  $p_i$ . Then note that  $x \notin V_n$  as

$$x^{\frac{n-1}{2}} \equiv 1^{\frac{n-1}{2}} \equiv 1 \not\equiv -1 \pmod{p_i} \text{ for some } i \neq 1 \quad \text{so} \quad x^{\frac{n-1}{2}} \not\equiv -1$$

where congruences are modulo  $n$  unless otherwise mentioned.

Now we consider  $W_n$ . Let  $n = \prod_i p_i^{e_i}$  be odd and  $a \in W_n$ .

If  $a^d \equiv 1$  then the order  $\text{ord}[a]_{p_i}$  is odd for each  $i$ , and therefore  $a$  is a square modulo  $p_i$  by using that  $\mathbb{Z}_{p_i}^*$  is cyclic of even order. Therefore,

$$\left(\frac{a}{n}\right) = 1 \equiv a^{\frac{n-1}{2}} \text{ so } a \in V_n$$

If  $a^{2^r d} \equiv -1$  for  $r < s$  have that  $[a]_{p_i}^{2^r d} = [-1]$ . It follows that  $\text{ord}[a]_{p_i} = 2^{r+1}d_i$  for  $d_i \perp 2$ , as  $2^k f := \text{ord}[a] \mid 2^{r+1}d$ ,  $f \perp 2$  and if  $k \leq r$  then

$$[-1] = [a]^{2^r d_i} = ([a]^{2^k f})^{\frac{d_i}{f} 2^{r-k}} = [1]^{\frac{d_i}{f} 2^{r-k}} = [1], \quad \text{a contradiction}$$

So  $\text{ord}[a]_{p_i} = 2^{r+1}d_i$ , hence  $2^{r+1} \mid p_i - 1$ . We set  $p_i = 2^{r+1}b_i + 1$ .

As above,  $\mathbb{Z}_{p_i}^*$  is cyclic of even order, so we get

$$\left(\frac{a}{p_i}\right) = -1 \Leftrightarrow 2\text{ord}[a]_{p_i} \nmid p_i - 1 \Leftrightarrow 2^{r+2}d_i \nmid p_i - 1 \Leftrightarrow 2^{r+2} \nmid p_i - 1 \Leftrightarrow b_i \perp 2$$

This yields

$$\left(\frac{a}{p_i}\right) = (-1)^{b_i} \Rightarrow \left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i} = (-1)^{\sum_i b_i e_i}$$

Furthermore we get for the representation of  $n$  modulo  $2^{2r+2}$  that

$$n = \prod_i p_i^{e_i} = \prod_i (2^{r+1}b_i + 1)^{e_i} \equiv \prod_i (2^{r+1}b_i e_i + 1) \equiv 1 + 2^{r+1} \sum_i b_i e_i \pmod{2^{2r+2}}$$

so

$$2^{s-1}d = \frac{n-1}{2} \equiv 2^r \sum_i b_i e_i \pmod{2^{2r+1}} \Rightarrow 2^{s-r-1} \equiv 2^{s-r-1}d \equiv \sum_i b_i e_i \pmod{2}$$

and at last we get

$$a^{\frac{n-1}{2}} = a^{2^{s-1}d} = (a^{2^r d})^{2^{s-r-1}} = (-1)^{2^{s-r-1}} = (-1)^{\sum_i b_i e_i} = \left(\frac{a}{n}\right)$$

□

## 12.2 Hidden Subgroup Problem

Given a group  $G$  together with a group homomorphism  $f : G \rightarrow X$  that is constant on all cosets of some subgroup  $H \leq G$  and different on different cosets, find a generating set of  $H$ .

**Quantum Algorithm for  $G = \mathbb{Z}$**  Each subgroup  $H \leq \mathbb{Z}$  is of the form  $H = q\mathbb{Z}$ , so  $f$  is periodic with periode  $b \in \mathbb{Z}$ . Now consider some big  $N = 2^n \in \mathbb{Z}$  and consider

$$\sum_{x=0}^{N-1} |x\rangle |f(x)\rangle$$

With a  $N$ -th root of unity  $\zeta$ , applying the QFT yields

$$\frac{1}{N} \sum_{x=0}^{N-1} \sum_{k=0}^{N-1} \zeta^{kx} |k\rangle |f(x)\rangle$$

When measuring both states, the probability to get some  $k \in \{0, \dots, N-1\}$ ,  $f(x_0) \in X$  is equal to

$$\begin{aligned} \frac{1}{N^2} \left| \sum_{x=0, f(x)=f(x_0)}^{N-1} \zeta^{kx} \right|^2 &= \frac{1}{N^2} \left| \sum_{l=0}^M \zeta^{k(x_0+bl)} \right|^2 = \frac{1}{N^2} \left| \zeta^{kx_0} \sum_{l=0}^M \zeta^{kbl} \right|^2 \\ &= \frac{1}{N^2} \left| \sum_{l=0}^M \zeta^{kbl} \right|^2 = \frac{1}{N^2} \left| \frac{1 - \zeta^{kb(M+1)}}{1 - \zeta^{kb}} \right|^2 = \frac{1}{N^2} \left| \frac{\sin(2\pi \frac{kb(M+1)}{N})}{\sin(2\pi \frac{kb}{N})} \right|^2 \end{aligned}$$

where  $M = \lfloor \frac{N-x_0}{b} \rfloor \approx \frac{N}{b}$  and the denominators are non-zero as  $b$  is wlog odd.

TODO

## 13 Algorithms

### 13.1 Parameterized Algorithms design techniques

#### Kernelization

Given an instance  $(X, k)$ , compute an instance  $(X', k')$  such that  $(X, k)$  is a YES-instance if and only if  $(X', k')$  is a YES-instance and the size of  $X'$  is bounded by  $f(k)$  (this is usually done via reduction rules).

#### Bounded search tree

Given an instance  $(X, k)$  compute instances  $(X_1, k_1), \dots, (X_n, k_n)$  such that  $(X, k)$  is a YES-instance if and only if at least one of the  $(X_i, k_i)$  is a YES-instance. Additionally, it must hold that  $d_i := k - k_i > 0$ . Then applying this algorithm recursively on all the  $(X_i, k_i)$  yields an FPT algorithm with running time  $O(\lambda^k \text{poly}(n))$  where  $\lambda$  is the positive

root of the branching vector polynomial equation (there exactly one, as the  $m-1, \dots, 0$ -th derivatives all are non-positive up to some point, and then positive)

$$X^m = \sum_{i=1}^m X^{m-d_i}$$

### Iterative Compression

Usually this is used for problems where solutions are (in some way) parts/subsets of the instance and behave monotonously (i.e. supersets of solutions are also solutions). In this case, one normally has the size of the searched solution as parameter. Then it is easy to reduce the original problem to its “compression variant”

**Input** Given an instance  $(X, k)$  and a solution to  $Z \leq X$  of size exactly  $k + 1$

**Problem** Find a solution of size at most  $k$  (or find that it does not exist)

By trying all  $2^k$  subsets, we can further reduce it to the “disjoint variant” of the problem:

**Input** Given an instance  $(X, k)$  and a solution  $Y \leq X$  of size exactly  $k + 1$

**Problem** Find a solution of size at most  $k$  that is disjoint to  $Y$  (or that it does not exist)

## 13.2 Treewidth

A tree  $T$  with nodes in  $2^V$  is called a tree decomposition of  $G = (V, E)$ , if

- for  $\{u, v\} \in E$  have a tree node containing  $u, v$
- for  $u \in V$  have a tree node containing  $u$
- for  $u \in V$  have that all tree nodes containing  $u$  form a subtree of  $T$

The width of a tree decomposition  $T$  is the cardinality of its largest node minus 1. The treewidth of a graph  $G = (V, E)$  is the minimal width of a tree decomposition.