Collection of arbitrary mathematical facts

Inhaltsverzeichnis

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

1 Set Theory

1.1 Zorn's Lemma

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.3.1 Lemma

Let $f : \mathrm{On} \to \mathrm{On}$ be an increasing function with

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

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

Proof Consider the order $\leq$ on 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 $f : \mathrm{On} \to \mathrm{On},\ \alpha \mapsto \mathrm{ord}(\alpha \times \alpha)$ fulfills the conditions from the lemma. □

1.4 Power Cardinality

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

Proof Have bijections

$$\mathfrak{P}(Y)^Y \to \left(2^Y\right)^Y \to 2^{Y\times Y} \to \mathfrak{P}(Y^2)$$

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

Otherwise have $\gamma = \mathrm{card}(Y)$ 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 $\mathrm{card}(\mu^\gamma) = \mathrm{card}(\mu)$ for all $\mu \geq 2^\gamma$.

Consider the order $\leq$ on On^γ 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 $\mathrm{On} \to \mathrm{On},\ \alpha \mapsto \mathrm{ord}(\alpha^\gamma)$ fulfills the conditions of the modified lemma, and the claim follows as $\mathrm{card}(X) \geq 2^\gamma$. □

1.5 Ordinal arithmetic

For $\alpha, \beta \in \text{On}$ define $\alpha + \beta := \text{ord}((\{0\} \times \alpha) \cup (\{1\} \times \beta))$ (with lexiographic 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 λ

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 λ

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

Let $\mathcal{L}$ be a formal language.

Definition Proof

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

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

2.1 Deduction theorem

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

2.2 Constant lemma

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

2.3 Gödel's completeness theorem

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

Proof idea First we construct a witness extension for Σ, 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 ϕ with the only free variable x have $\Sigma' \vdash \phi(x/c_\phi)$ for a constant c_ϕ. This can be done by recursivly adding witnesses for each suitable formula and then unifying the chain of languages that were creates.

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

2.5 Löwenheim-Skolem

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

- If Σ has a model, then it has one of cardinality $\leq \kappa_{\mathcal{L}}$
- If Σ has an infinite model, then it has one of cardinality κ 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 Σ (stays consistent by the compactness theorem).

2.6 Separation lemma

Let $\Sigma_1, \Sigma_2, \Gamma \subseteq \mathrm{Sen}(\mathcal{L})$. 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 $\mathrm{Mod}_{\mathcal{L}}(\Sigma_1)$ and $\mathrm{Mod}_{\mathcal{L}}(\Sigma_2)$ (i.e. $\mathrm{Mod}_{\mathcal{L}}(\Sigma_1) \subseteq \mathrm{Mod}_{\mathcal{L}}(\gamma^*)$ and $\mathrm{Mod}_{\mathcal{L}}(\Sigma_2) \subseteq \mathrm{Mod}_{\mathcal{L}}(\neg\gamma^*)$).

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

2.7 Vaught's test

Let T be an $\mathcal{L}$-theory. If T has only infinite models and is κ-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 κ, which then are isomorphic. This is a contradiction. □

2.8 Quantifier elimination

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

- for every $\mathcal{L}$-formula ϕ there is a quantifier-free $\mathcal{L}$-formula ψ with no additional free variables such that $\Sigma \vdash \phi \leftrightarrow \psi$.
- for every substructure $\mathcal{A}$ of a model of Σ have that $\Sigma \cup \mathcal{D}(\mathcal{A}) \subseteq \mathrm{Sen}(\mathcal{L}(\mathcal{A}))$ is complete.
- for every two models $\mathcal{M}_1, \mathcal{M}_2$ of Σ and a joint substructure $\mathcal{A}$ of $\mathcal{M}_1$ and $\mathcal{M}_2$ have that:
$$(\mathcal{M}_1, \mathrm{id}_{|\mathcal{A}|}) \models \phi \;\Leftrightarrow\; (\mathcal{M}_2, \mathrm{id}_{|\mathcal{A}|}) \models \phi$$
for every formula $\phi \in \mathrm{Sen}(\mathcal{L}(\mathcal{A}))$ of the form $\phi = \exists x \psi$ with a quantifier-free ψ.

Proof idea Use the separation lemma 2.6.

3 Model Theory

Let $\mathcal{L}$ be a formal language.

3.1 Extending embeddings

Let $\mathcal{S} \subset \mathcal{M}$ be an $\mathcal{L}$-substructure and $f : \mathcal{S} \to \mathcal{N}$ and elementary embedding. Then there is an elementary embedding $F : \langle |\mathcal{S}|, a\rangle \to \mathcal{N}$ that extends f with $F(a) = b$ if and only if b realizes $f(\mathrm{tp}^{\mathcal{M}}(a/|\mathcal{S}|))$.

Proof idea The condition $F(a) = b$ uniquely defines F, so just check well-definedness.

3.2 Chains

Let $(\mathcal{M}_\beta)_{\beta<\alpha}$ be an α-chain. Then

$$\bigcap_{\beta<\alpha} \mathrm{Th}_{\forall\exists}(\mathcal{M}_\beta) \subseteq \mathrm{Th}_{\forall\exists}\Big(\bigcup_{\beta<\alpha} \mathcal{M}_\beta\Big)$$

If $(\mathcal{M}_\beta)_{\beta<\alpha}$ is elementary, then even

$$\mathcal{M}_\beta \prec \bigcup_{\gamma<\alpha} \mathcal{M}_\gamma \text{ for all } \beta < \alpha$$

Proof idea Part (i) is easily proven by considering a large enough β such that all finitely many elements required for a counterexample are in $\mathcal{M}_\beta$. Part (ii) is proven via transfinite induction and a similar argument in the transfinite case.

3.3 Embeddings and saturated structures

Let $\mathcal{M}, \mathcal{N}$ be $\mathcal{L}$-structure, $\mathcal{N}$ is $\mathrm{card}(\mathcal{M})$-saturated.

- If $\mathrm{Th}_\exists(\mathcal{M}) \subseteq \mathrm{Th}_\exists(\mathcal{N})$ then $\mathcal{M}$ embeds into $\mathcal{N}$
- If $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$ then $\mathcal{M}$ embeds elementarily into $\mathcal{N}$

Proof idea Let $(a_\beta)_{\beta<\kappa}$ be the elements of $\mathcal{M}$. Then construct by transfinite induction a chain of maps $f_\beta : A_\beta := \{a_\gamma \mid \gamma < \beta\} \to \mathcal{N}$ such that

$$\mathrm{Th}_\exists(\mathcal{M}, (a_\gamma)_{\gamma<\beta}) \subseteq \mathrm{Th}_\exists(\mathcal{N}, f) \quad \text{resp.} \quad \mathrm{Th}(\mathcal{M}, (a_\gamma)_{\gamma<\beta}) = \mathrm{Th}(\mathcal{N}, f)$$

In the inductive step, the next element is found by considering the types $f(\mathrm{tp}_\exists^{\mathcal{M}}(a_\beta/A_\beta))$ resp $f(\mathrm{tp}^{\mathcal{M}}(a_\beta/A_\beta))$ over $\mathcal{N}$.

3.4 Back-and-forth Argument

Well, I guess the theorem is correct and still misses the whole point. The way it currently goes, we could just extend f to $M \to B$ first and then to $M \to N$. However, the interesting thing is the cardinality, so the fact that if one alternatively extends the maps correctly, there will always be elements "left" on the other side.

Let M, N be sets of same cardinality κ and $\mathcal{G}$ a class of bijective maps $A \to B$ for subsets $A \subseteq M, B \subseteq N$. Assume that $\mathcal{G}$ is invariant under monotonous unions and for $f : A \to B \in \mathcal{G}$ and $a \in M \setminus A,\ b \in N \setminus B$ there are extensions $f_a : A \cup \{a\} \to B',\ f_b : A' \to B \cup \{b\}$. Then there is a bijective map $F : M \to N$ in $\mathcal{G}$.

Proof Let $(a_\beta)_{\beta<\kappa}$ be the elements of M and $(b_\beta)_{\beta<\kappa}$ be the elements of N. Construct $f_\beta : A_\beta \to B_\beta$ in $\mathcal{G}$ by transfinite induction such that $a_\gamma \in A_\beta,\ b_\gamma \in B_\beta$ for all $\gamma < \beta$. Thus $A_\kappa = M$ and $B_\kappa = N$. The claims for the induction follow directly by the assumptions.

3.5 Saturation and Isomorphisms

Let $\mathcal{M} \equiv \mathcal{N}$ be saturated. Then $\mathcal{M} \cong \mathcal{N}$.

Proof idea Use 3.4 with $\mathcal{G} = \{f : A \to B \mid \mathrm{Th}(\mathcal{M}, \mathrm{id}_A) = \mathrm{Th}(\mathcal{N}, f)\}$. The extension property follows by considering $\mathrm{tp}^{\mathcal{M}}(a/A)$ which is realized in $\mathcal{N}$ and vice versa.

3.6 Theorem of Los

Let $\Sigma \subseteq \mathrm{Sen}(\mathcal{L})$ and $S = \{\Delta \subseteq \Sigma \mid \Delta \text{ finite}\}$. For $\Delta \in S$ let $S_\Delta = \{\Delta' \in S \mid \Delta \subseteq \Delta'\}$ Now define $\mathcal{D} = \{S_\Delta \mid \Delta \in S\}$. Then $\prod_{\Delta \in S} \mathrm{M}_\Delta/\mathcal{U}$ is a model of Σ if $\mathcal{U}$ is an ultrafilter on $\mathcal{S}$ containing $\mathcal{D}$ and $\mathcal{M}_\Delta$ is a model of Δ.

Proof Follows from this lemma

3.6.1 Lemma

For an $\mathcal{L}$-formula ϕ have

$$\prod_s \mathcal{M}_s/\mathcal{U} \models \phi\Big[\prod_s h_s/\mathcal{U}\Big] \;\Leftrightarrow\; \{s \in S \mid \mathcal{M}_s \models \phi[h_s]\} \in \mathcal{U}$$

Proof idea Use induction on the structure of ϕ. The nontrivial case is $\phi = \forall x\psi$. To show $\Leftarrow$, consider $(a_s)_s \in \bigtimes_s |\mathcal{M}_s|$. Now $\{s \in S \mid \mathcal{M}_s \models \phi[h_s(x/a_s)]\}$ is a superset of the set above, thus in $\mathcal{U}$. By induction hypothesis, get the claim for $\overline{(a_s)_s}$. For $\Rightarrow$, consider $\neq \phi$ and use that $\mathcal{U}$ is an ultrafilter.

3.7 Saturation and Ultraproducts

Let $\mathcal{L}$ be countable and $(\mathcal{M}_n)_{n\in\mathbb{N}}$ be $\mathcal{L}$-structures. If $\mathcal{U}$ is a free ultrafilter on $\mathbb{N}$ then $\prod_n \mathcal{M}_n/\mathcal{U}$ is $\aleph_1$-saturated.

Proof idea The proof relies on diagonal sequences. Let $A \subseteq |\mathcal{M}|$ countable and $p(x) = \{\phi_1(x), \phi_2(x), ...\}$ a 1-type over A. Set $\psi_k := \phi_1 \wedge ... \wedge \phi_k$. As p is a type, ψ_k is realized by $\overline{(c_{k,n})_n}$. Now use the following lemma with $A_k = \{n \mid \mathcal{M}_n \models \psi_k(c_{k,n})\}$ and get that p is realized by $\overline{(c_{z_n,n})_n}$.

3.7.1 Lemma

Let $\mathcal{U}$ be a free ultrafilter on $\mathbb{N}$ and $(A_k)_k$ a sequence of sets in $\mathcal{U}$. Then there is a sequence of numbers $(z_n)_n$ such that

$$A^{(k)} := \{n \mid z_n \geq k \text{ and } n \in A_{z_n}\} \in \mathcal{U} \text{ for all } k \in \mathbb{N}$$

Proof idea Take for z_n the greatest $k \leq n$ with $n \in A_k$, or 0 if this does not exist. Now $A^{(k)} \supseteq A_k \setminus \{0, ..., k-1\} \in \mathcal{U}$ as $\mathcal{U}$ contains all cofinite sets..

3.8 Robinson's Test

Let $\Sigma \subseteq \mathrm{Sen}(\mathcal{L})$. Then the following are equivalent

- Σ is model-complete, i.e. $\Sigma \cup \mathcal{D}(\mathcal{M})$ is complete for all $\mathcal{M} \models \Sigma$
- If $\mathcal{M} \subset \mathcal{N}$ are models of Σ, then $\mathcal{M}$ is existentially closed in $\mathcal{N}$
- For all $\phi \in \mathrm{Fml}(\mathcal{L})$ there is a universal $\psi \in \mathrm{Fml}(\mathcal{L})$ with $\mathrm{Fr}(\psi) \subseteq \mathrm{Fr}(\phi),\ \Sigma \vdash \phi \leftrightarrow \psi$
- For all $\phi \in \mathrm{Fml}(\mathcal{L})$ there is an existential $\psi \in \mathrm{Fml}(\mathcal{L})$ with $\mathrm{Fr}(\psi) \subseteq \mathrm{Fr}(\phi),\ \Sigma \vdash \phi \leftrightarrow \psi$

Proof (iii)⇔(iv) follows by considering $\neg\phi$. (i)⇒(ii) and (iii)∧(iv)⇒(i) are easy. For (ii)⇒(iii) we consider special cases first.

If ϕ is an existential sentence, use the separation lemma 2.6. Let $\Gamma = \{\delta \in \mathrm{Sen}(\mathcal{L}) \mid \delta \text{ universal}\}$ and $\Sigma_1 = \Sigma \cup \{\phi\}, \Sigma_2 = \Sigma \cup \{\neg\phi\}$.

Assume there are $\mathcal{M}_1, \mathcal{M}_2 \models \Sigma$ not separated by Γ. Find a $\mathrm{card}(\mathcal{M}_2)$-saturated elementary extension $\mathcal{N}$ of $\mathcal{M}_1$. As Γ does not separate them, all existential sentences that hold in $\mathcal{M}_1$ hold in $\mathcal{M}_2$. By 3.3, get wlog $\mathcal{M}_2 \subset \mathcal{N}$, thus $\mathcal{M}_1 \prec \mathcal{N} \supset \mathcal{M}_2$. As $\mathcal{M}_2$ is existentially closed, get $\mathcal{M}_1 \models \phi$ if and only if $\mathcal{M}_2 \models \phi$.

The separation lemma now yields a universal γ^* such that $\Sigma \vdash \phi \leftrightarrow \gamma^*$. By introducing new constants, this can be generalized to all existential formulas ϕ. For arbitrary ϕ, proceed by induction on the construction of ϕ. The special case is used in the only nontrivial step, namely $\phi = \neg\psi$.

3.9 Characterization of Inductive classes

Let $\Sigma \subseteq \mathrm{Sen}(\mathcal{L})$. Then Σ is inductive (i.e. its models are preserved under monotonous unions) if and only if $\mathrm{Mod}_{\mathcal{L}}(\Sigma) = \mathrm{Mod}_{\mathcal{L}}(\mathrm{Ded}_{\forall\exists}(\Sigma))$.

Proof $\Leftarrow$ follows from 3.2. To show $\Rightarrow$, consider a model $\mathcal{M}_0$ of $\mathrm{Ded}_{\forall\exists}(\Sigma)$ and construct a sequence

$$\mathcal{M}_0 \subset \mathcal{N}_0 \subset \mathcal{M}_1 \subset \mathcal{N}_1 \subset ...$$

where $\mathcal{N}_i$ are models of Σ. To get $\mathcal{N}_i$, construct an extension of $\mathcal{M}_i$ such that the latter is existentially closed, by considering a model of the consistent set $\Sigma \cup \mathrm{Th}_{\forall}(\mathcal{M}_i, \mathrm{id}_{|\mathcal{M}_i|})$. To get $\mathcal{M}_{i+1}$ consider a sufficiently saturated elementary extension of $\mathcal{M}_i$. Now $\mathcal{M}_i \prec \bigcup_n \mathcal{M}_n = \bigcup_n \mathcal{N}_n$ which is a model of Σ.

3.10 Omitting type Theorem

Let $\mathcal{L}$ be countable and $\Phi_1(\bar{x}), \Phi_2(\bar{x}), ...$ be non-isolated types over a theory T. Then T has a model that omits all Φ_n.

Proof idea Introduce countably many constant symbols C (these represent all elements whose existence is provable) and construct $\mathcal{L}(C)$ sentences Σ^* with

- For $\psi(x) \in \mathrm{Fml}(\mathcal{L}(C))$ have a $c \in C$ such that $\exists x \psi(x) \to \psi(c) \in \Sigma^*$
- For $\bar{c} \in C$ and $i \in \mathbb{N}$ have $\phi_i(\bar{x}) \in \Phi_i(\bar{x})$ such that $\neg\phi_i(\bar{c}) \in \Sigma^*$

Do this by recursively constructing consistent Σ_n such that $\Sigma_n \setminus T$ is finite. Then the substructure $\{c^{\mathcal{A}} \mid c \in C\}$ of a model $\mathcal{A}$ of Σ^* omits all Φ_n. We use the next lemma to perform this construction:

Satisfy (i) for $\psi_n \in \mathrm{Fml}(\mathcal{L}(C))$ during step $(n, \bot)$ by adding a sentence with a previously unused constant $c_n \in C$, and satisfy (ii) for $c_{\bar{j}}$ and j in step (n, m) where $\bar{j}, j$ are the images of some bijection $m \mapsto (\bar{j}, j) \in \{0, ..., n\}^N \times \mathbb{N}$ (here we require that $\Phi(\bar{x})$ is not isolated).

3.10.1 Lemma

There exists a bijective sequence $(x_n, y_n)_n$ with $x_n \in \mathbb{N}, y_n \in \mathbb{N} \cup \{\bot\}$ such that

- (n, m) does not occur before $(n, \bot)$ for all $n, m \in \mathbb{N}$
- $(n_2, \bot)$ does not occur before $(n_1, \bot)$ for $n_1 < n_2$

3.11 Ryll-Nardzewski Theorem

Let $\mathcal{L}$ be countable and T a complete theory. Then T is $\aleph_0$-categorical if and only if for every $n \in \mathbb{N}$ there are only countably many $\phi(x_1, ..., x_n) \in \mathrm{Fml}(\mathcal{L})$ up to provable equivalence in T.

In this case, each countable model of T is saturated.

Proof (i) $\overset{3.10}{\Leftrightarrow}$ all complete types are isolated $\Leftrightarrow$ $S_n(T)$ has discrete topology $\Leftrightarrow$ $S_n(T)$ is finite $\Leftrightarrow$ $S_n(T)$ has finitely many open sets $\Leftrightarrow$ (ii).

3.12 Characterization of small theories

Let $\mathcal{L}$ be countable and T complete. Then T is small (i.e. $S_n(T)$ countable) if and only if T has a countable, saturated model.

Proof idea $\Leftarrow$ holds as tuples over $\mathcal{M}$ determine each type $\Phi(\bar{x}) \in S_n(T)$. For $\Rightarrow$, consider an elementary chain $(\mathcal{M}_n)_n$ such that $\mathcal{M}_{n+1}$ realizes all types over $\mathcal{M}_n$.

3.13 Theorem of Vaught

Let $\mathcal{L}$ be countable and T complete. Then T cannot have exactly two countable models, up to isomorphism.

Proof idea wlog have that T is small (otherwise the claim is easy). Then there is a saturated, countable mode, a non-saturated, countable model realizing a non-isolated type Φ and a countable model omitting Φ (that or T is $\aleph_0$-categorical).

3.14 Amalgamation Method

Let $\mathcal{L}$ be countable and $\mathcal{K}$ a class of $\mathcal{L}$-structures. Then the following are equivalent:

- There is a countable $\mathcal{K}$-saturated $\mathcal{L}$-structure $\mathcal{M}$, i.e. $\mathcal{K}$ consists exactly of all finitely generated substructures of $\mathcal{M}$ and for $\mathcal{A}, \mathcal{B} \in \mathcal{K}$ with embeddings $f : \mathcal{A} \to \mathcal{M}, g : \mathcal{A} \to \mathcal{B}$ there is an embedding $h : \mathcal{B} \to \mathcal{M}$ such that $f = h \circ g$.
- $\mathcal{K}$ consists of finitely generated $\mathcal{L}$-structures and satisfies
  - for $\mathcal{M} \in \mathcal{K}$ each finitely generated substructure of $\mathcal{M}$ is in $\mathcal{K}$
  - every $\mathcal{M}_1, \mathcal{M}_\in \in \mathcal{K}$ can be jointly embedded into some $\mathcal{N} \in \mathcal{K}$
  - for $\mathcal{P}, \mathcal{M}_1, \mathcal{M}_2 \in \mathcal{K}$ and embeddings $f_i : \mathcal{P} \to \mathcal{M}_i$ find $\mathcal{N} \in \mathcal{K}$ and embeddings $g_i : \mathcal{M}_i \to \mathcal{N}$ such that $g_1 \circ f_1 = g_2 \circ f_2$.

Proof $\Rightarrow$ is easy. For $\Leftarrow$ use the combinatorial lemma 3.10.1 to construct a chain $\mathcal{M}_1 \subset \mathcal{M}_2 \subset ...$ such that

- each $\mathcal{M} \in \mathcal{K}$ embeds into some $\mathcal{M}_k$.
- for embeddings $f : \mathcal{A} \to \mathcal{M}_n,\ g : \mathcal{A} \to \mathcal{B}$ with $\mathcal{A}, \mathcal{B} \in \mathcal{K}$ have embedding $h : \mathcal{B} \to \mathcal{M}_k$ such that $\mathcal{M}_n \subset \mathcal{M}_k$ and $h \circ g = f$.

As $\mathcal{K}$ is countable up to isomorphism ($\mathcal{L}$ is countable), we can satisfy (i) during the steps $(n, \bot)$. During step (n, m) we satisfy then (ii) for $\mathcal{A}_{n,m}, \mathcal{B}_{n,m}, \mathcal{M}_n, f_{n,m}, g_{n,m}$, where $\mathcal{A}_{n,m}, \mathcal{B}_{n,m}, f_{n,m}, g_{n,m}$ runs through all possible choice of these values as m runs through $\mathbb{N}$ (if we count $\mathcal{A}, \mathcal{B}$ only up to isomorphism, these are countably many). Now $\mathcal{M}^* := \bigcup_n \mathcal{M}_n$ satisfies the claim.

3.15 The Standard Lemma

Let I, J be infinite ordered sets and $(a_i)_{i \in I}$ a sequence in $|\mathcal{M}|$. Then there is an $\mathcal{L}$-structure $\mathcal{N}$ and a sequence of indiscernibles $(b_j)_{j \in J}$ in $|\mathcal{N}|$ such that $\mathcal{M} \equiv \mathcal{N}$ and $(b_j)_j$ realizes the Ehrenfeucht-Mostowski-type

$$\mathrm{EM}^{\mathcal{M}}((a_i)_i) := \{\phi(x_1, ..., x_n) \mid n \in \mathbb{N},\ (\mathcal{M}, \mathrm{id}_{|\mathrm{M}|}) \models \phi(a_{i_1}, ...a_{i_n}) \text{ for all } i_1 < ... < i_n\}$$

i.e. for $\phi(x_1, ..., x_n) \in \mathrm{EM}^{\mathcal{M}}((a_i)_i)$ have

$$(\mathcal{M}, \mathrm{id}_{|\mathcal{M}|}) \models \phi(b_{j_1}, ..., b_{j_n}) \text{ for all } j_1 < ... < j_n$$

Proof Introduce constants $C = \{c_j \mid j \in J\}$ and define a corresponding order on C. Now a model of

$$\begin{aligned}&\mathrm{Th}(\mathcal{M}) \cup \Sigma_C \cup \Gamma_{C,\mathrm{Fml}(\mathcal{L})}\\ &\text{where } \Sigma_D = \{\psi(\bar{c}) \mid \psi(\bar{c}) \in \mathrm{EM}^{\mathcal{M}}((a_i)_i),\ \bar{c} \in D^n \text{ increasing}\}\\ &\qquad \Gamma_{D,\Delta} = \{\phi(\bar{c}) \leftrightarrow \phi(\bar{d}) \mid \phi(\bar{x}) \in \Delta,\ \bar{c}, \bar{d} \in D^n \text{ increasing}\}\end{aligned}$$

shows the claim. So use the compactness theorem. A finite subset of these sentences is contained in $\mathrm{Th}(\mathcal{M}) \cup \Sigma_D \cup \Gamma_{D,\Delta}$ for finite $D \subseteq C, \Delta \subseteq \mathrm{Fml}(\mathcal{L})$. Now we find $(a_d)_{d\in D}$ such that

$$(\mathcal{M}, (a_d)_d) \models \mathrm{Th}(\mathcal{M}) \cup \Sigma_D \cup \Gamma_{D,\Delta}$$

This can be done by choosing increasing elements from an infinite set B, where $B \subseteq \{a_i \mid i \in I\}$ such that $\bar{b} \sim \bar{d}$ for increasing $\bar{b}, \bar{d} \in B^n$. Here $\sim$ is defined by

$$\bar{b} \sim \bar{d} :\Leftrightarrow (\mathcal{M}, \mathrm{id}_{\mathcal{M}}) \models \phi(\bar{b}) \leftrightarrow \phi(\bar{d}) \text{ for all } \phi(\bar{x}) \in \Delta$$

We get this set B from Ramsey's theorem, as the partition $\Omega_n(\{a_i \mid i \in I\})/\sim$ is finite (Δ is finite).

3.15.1 Ramsey's theorem

Let A be infinite, $n \in \mathbb{N}$ and set $\Omega_n(A) := \{B \subseteq A \mid \mathrm{card}(B) = n\}$. For a finite partition $\Omega_n(A) = \bigcup_{k\le N} C_k$ have an infinite $\tilde{A} \subseteq A$ with $\Omega_n(\tilde{A}) \subseteq C_k$ for some $k \in \mathbb{N}$.

Proof idea By induction on n.

3.16 Skolem Theory

For a language $\mathcal{L}$ there is a Skolem theory T_{Skol}, i.e. a $\mathcal{L}_{\mathrm{Skol}}$-theory with

- T_{Skol} has quantifier elimination
- T_{Skol} has a universal axiomatization
- Every $\mathcal{L}$-structure can be extended to a model of T_{Skol}
- $\mathcal{L}_{\mathrm{Skol}}$ is an extension of $\mathcal{L}$ with same cardinality

Proof idea Introduce function symbols for all $\forall \bar{x} \exists y\ \psi(\bar{x}, y)$.

3.17 Stability and transcendence

Let $\mathcal{L}$ be countable and T a complete $\mathcal{L}$-theory.

- T is κ-categorical for uncountable $\kappa \Rightarrow T$ is ω-stable
- T is ω-stable $\Rightarrow T$ is totally transcendental
- T totally transcendental $\Rightarrow T$ is κ-stable for every infinite κ

T is defined to be κ-stable, if $\mathrm{card}(S_n^{\mathcal{M}}(A)) \leq \kappa$ for models $\mathcal{M}$ and $A \subseteq |\mathcal{M}|, \mathrm{card}(A) \leq \kappa$. T is defined to be totally transcendental, if there is no model $\mathcal{M}$ with a binary tree of consistent $\mathcal{L}(\mathcal{M})$-formulas.

Proof idea For (i), assume there is a model $\mathcal{N}$ and a countable $A \subseteq |\mathcal{N}|$ such that there are distinct 1-types $(p_\alpha(x))_{\alpha<\aleph_1}$. Now have $\mathcal{M}_0 \prec \mathcal{N}$ of cardinality $\aleph_1$ containing A and realizing all p_α by Skolem-Löwenheim. Thus have $\mathcal{M} \succ \mathcal{M}_0$ of cardinality κ by Skolem-Löwenheim. Now construct a model of cardinality κ realizing only countably many types.

Let $\mathcal{N}^*$ be a model of $T \cup T_{\mathrm{Skol}}$ such that there is a sequence of distinct indiscernibles $(a_\alpha)_{\alpha<\kappa}$ by 3.15. Let $\mathcal{A}$ be the substructure generated by the a_i. Then $\mathcal{A} \prec \mathcal{N}^*$ has $T \cup T_{\mathrm{Skol}}$ is universal (T_{Skol} has quantifier elimination). Each element of $\mathcal{A}$ is now $t(a_{i_1}, ..., a_{i_m})$ for an $\mathcal{L}$-term t, so its type is determined only by t and the relative order of $i_1, ..., i_m$, giving only countably many choices.

For (ii), note that a binary tree induces $2^{\aleph_0}$ many different complete types. For (iii), recursively construct a binary tree of consistent $\mathcal{L}(\mathcal{M})$-formulas by considering "large" formulas, defined as those contained in more than κ many types. By the following lemma, each large formula has suitable, large tree children.

3.17.1 Lemma

Let X be an infinite set of cardinality κ and $\mathcal{C} \subseteq 2^X$ with $\mathrm{card}(\mathcal{C}) > \kappa$. Then there is $x \in X$ such that $\mathcal{C}_x := \{A \in \mathcal{C} \mid x \in A\}$ and $\mathcal{C} \setminus \mathcal{C}_x$ are of cardinality $> \kappa$.

Proof Assume not, so wlog $\mathrm{card}(\mathcal{C}_x) \leq \kappa$. Then also $\mathcal{C} \setminus \{\emptyset\} = \bigcup_{x \in X} \mathcal{C}_x$ is of cardinality $\leq \mathrm{card}(\kappa \times \kappa) = \kappa$, a contradiction.

3.18 Saturation and categoricity

Let $\mathcal{L}$ be countable, T a complete theory and κ be an infinite cardinal. Then T is κ-categorical if and only if every model of T of cardinality κ is saturated.

Proof idea Showing $\Leftarrow$ is easy. For $\Rightarrow$, if $\kappa = \aleph_0$ the claim follows by 3.11. Otherwise, note that a model $\mathcal{M}$ is κ-stable by 3.17, thus for $\lambda < \kappa$ we find an elementary extension that is λ^+-saturated and of same cardinality. All of them are isomorphic by assumption, thus $\mathcal{M}$ is saturated.

3.19 Constructible Prime Extensions

Let $\mathcal{L}$ be countable, T a totally transcendental theory and $\mathcal{M}$ a model. Then every $A \subseteq |\mathcal{M}|$ has a constructible elementary prime extension $\mathcal{M}_0$, so $\mathcal{M}_0$ is constructible over A and every partial elementary map $A \to \mathcal{N}$ extends to an elementary embedding $\mathcal{M}_0 \to \mathcal{N}$.

Proof idea A maximal constructible subset of $|\mathcal{M}|$ already defines an elementary substructure of $\mathcal{M}$ and an elementary prime extension of A.

3.20 Theorem of Lachlan

Let $\mathcal{L}$ be countable and T totally transcendental with an uncountable model $\mathcal{M}$. Then there are arbitrarily large $\mathcal{N} \succ \mathcal{M}$ that omit every possible countable type, i.e. every countable type omitted in $\mathcal{M}$.

Proof idea Call an $\mathcal{L}(\mathcal{M})$-formula "large", if it has uncountably many realizations in $\mathcal{M}$. As $\mathcal{M}$ has no binary tree of consistent formulas, there is an $\mathcal{L}(\mathcal{M})$-formula $\phi_0(x)$ which does not have two large tree children (i.e. either $\phi_0 \wedge \psi$ or $\phi_0 \wedge \neg\psi$ are not large). Thus $p(x) = \{\psi(x) \in \mathrm{Fml}(\mathcal{L}(\mathcal{M})) \mid \phi_0 \wedge \psi \text{ large}\}$ is a complete type over $\mathcal{M}$.

Now consider a constructible elementary prime extension $\mathcal{N}$ of $|\mathcal{M}| \cup \{a\}$, where a realizes p (in some elementary extension of $\mathcal{M}$) by 3.19. Let $\Phi(x) \subseteq \mathrm{tp}^{\mathcal{N}}(b/\mathcal{M})$ be a countable type realized in $\mathcal{N}$, then it is by constructibility isolated by some $\chi(a, y)$.

$$\Psi(x) := \{\forall y\ (\chi(x, y) \to \phi(y)) \mid \phi \in \Phi\} \subseteq p \quad \text{is a countable subset}$$

We show that it is realized in $\mathcal{M}$, so we find an element $\tilde{a} \in |\mathcal{M}|$ "sufficiently like a" such that it can be used to isolate Φ. Then clearly Φ is realized in $\mathcal{M}$.

Let $\Psi = \{\psi_n \mid n \in \mathbb{N}\}$. Then the set R_n of realizations of $\phi_0 \cap \neg\psi_n$ is countable, so also $\bigcup_{n\in\mathbb{N}} R_n$ is. However ϕ_0 has uncountably many realizations, so find one not in $\bigcup_n R_n$. This then realizes all ψ_n, hence Ψ.

Now repeat this construction to get an arbitrarily long elementary chain, yielding arbitrarily large elementary extensions.

3.21 Morley's Theorem

Let $\mathcal{L}$ be countable and T an $\mathcal{L}$-theory. Then the following are equivalent:

- T is $\aleph_1$-categorical
- T is κ-categorical for some uncountable cardinal κ
- T is κ-categorical for all uncountable cardinals κ

Proof idea Show only (ii) $\Rightarrow$ (i), the direction (i) $\Rightarrow$ (iii) was not proven. Consider a non-saturated model $\mathcal{M}$ of T of cardinality $\aleph_1$. Then $\mathcal{M}$ omits some countable type. Using 3.17 and 3.20 we lift it to a non-saturated elementary extension of cardinality κ. Now get a contradiction by 3.18.

4 Algebra

4.1 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

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

4.2 Sylow Theorems

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

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

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

4.3 Mordell's inequality

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

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

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

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

4.4 Facts about finite rings

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

Proof By the theorem on finitely generated abelian groups, have

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

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

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

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 $a \equiv 1 \mod p^\beta$.

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

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

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

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

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

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

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 $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$. □

4.5 Chinese Remainder theorem

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

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

4.6 Main theorem of finitely generated modules over PIDs

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

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

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

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

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

4.7 Smith normal form

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

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

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

4.8 The module $\mathbb{Z}^n$

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

4.9 Hilbert's basis theorem

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

4.10 Noether Normalization Theorem

Let A be a finitely generated ring extension of a field K and $I \leq A$ a proper ideal. Then there are $y_1, ..., y_d \in A$ algebraically independent such that A is finitely generated over $K[y_1, ..., y_d]$ and $I \cap K[y_1, ..., y_d] = \langle y_{\delta+1}, ..., y_d \rangle$.

Proof idea Use induction on the number n of generators $x_1, ..., x_n$ of A. An algebraic relation between them gives rise to a monic polynomial $f \in K[x_1, ..., x_{n-1}][X]$ with $f(x_n) = 0$ by the following lemma. Satisfying the condition with I can be done using the same idea, although the proof becomes quite technical.

4.10.1 Lemma

Let A be a finitely generated ring extension of a field K and $f \in K[x_1, ..., x_n] \setminus \{0\}$. Then there are $r_1, ..., r_{n-1} \in \mathbb{N}$ such that $a^{-1} f(x_1 + x_n^{r_1}, ..., x_{n-1} + x_n^{r_{n-1}}, x_n)$ is monic with $a \in K^*$.

4.11 Hilbert's Nullstellensatz

Let $I \leq K[x_1, ..., x_n]$. Then

- (weak Nullstellensatz) $1 \notin I$ if and only if $\mathbb{V}(I) \neq \emptyset$
- (strong Nullstellensatz) $\mathbb{I}(\mathbb{V}(I)) = \text{Rad}(I)$
- (projective Nullstellensatz) If I is homogeneous, then $\mathbb{I}^+(Z^+(I)) = \text{Rad}(I)$

Proof idea For (ii), let $f \in \mathbb{I}(\mathbb{V}(I)) \setminus \{0\}$ and consider $J = \langle I \rangle + \langle Xf - 1 \rangle \leq K[x_1, ..., x_n, X]$. As f vanishes on $\mathbb{V}(I)$ get $\mathbb{V}(J) = \emptyset$, so by the weak Nullstellensatz $1 \in J$. Thus $1 = h_1 g_1 + ... h_s g_s + k(Xf - 1)$ so $1 = h_1(x_1, ..., x_n, \frac{1}{f})g_1 + ... + h_s(x_1, ..., x_n, \frac{1}{f})g_s$. The claim follows.

4.12 Krull's Principal Ideal Theorem

Let R be an integral ring that is a finitely generated ring extension of a field K. Then every minimal prime divisor $\mathfrak{y} \supseteq \langle a \rangle$ with $a \in R \setminus R^* \setminus \{0\}$ has height 1.

Proof idea Let $\mathfrak{y}, \mathfrak{y}_2, ..., \mathfrak{y}_s \supseteq \langle a \rangle$ be the minimal prime divisors and consider the localization R_g where $g \in \bigcap_{i>1} \mathfrak{y}_i \setminus \mathfrak{y}$. Now $\mathfrak{y} = \text{Rad}(\langle a \rangle)$ (but the height of $\mathfrak{y}$ is unchanged). Using a Noether normalization, transfer this into a polynomial ring $K[y_1, ..., y_n]$ so $\text{Rad}(\langle \tilde{a} \rangle) = \langle \tilde{b} \rangle$ for irreducible $\tilde{b}$ as polynomial rings are UFDs. Clearly $\langle \tilde{b} \rangle$ has height 1.

4.13 Krull's Height Theorem

Let R be a finitely generated ring extension of a field K and let $I = \langle a_1, ..., a_m \rangle \leq R$. Then every minimal prime divisor $\mathfrak{y}$ of I has height at most m.

Proof idea Use induction on m. By taking the quotient by the first component of a maximal prime ideal chain, have wlog that R is an integral domain. The base case follows by 4.12. In the inductive case, find a maximal prime ideal chain $\mathfrak{y}_1 \subsetneq ... \subsetneq \mathfrak{y}_s \subsetneq \mathfrak{y}$ such that $\mathfrak{y}_s$ is a minimal prime divisor of $\langle a_1, ..., a_{m-1} \rangle$ and then apply 4.12.

5 Algebraic Geometry

5.1 Main Theorem of Elimination Theory

Let $V \subseteq \mathbb{P}^n$ be a projective K-variety with $(1 : 0 : ... : 0) \notin V$. Let

$$\pi : V \to \mathbb{P}^{n-1}, \ [a_0 : ... : a_n] \mapsto [a_1 : ... : a_n]$$

Then $\pi(V)$ is closed.

In particular, it follows that for a morphism $\phi : V \to \mathbb{P}^m$ have

$$\phi(V) = \pi_{x_{n+1},...,x_{n+m}}(\underbrace{\{(a,b) \mid b = \phi(a)\}}_{\text{closed in the product space of } \mathbb{P}^n \text{ and } \mathbb{P}^m})$$

is closed.

We show the following Let $U \subseteq \mathbb{P}_k^{n-1}$ such that for all $[a_1 : ... : a_n] \in U$ there is $a \in k$ with $[a_0 : a_1 : ... : a_n] \in V$. Then this also holds for $W := \overline{U}$.

Proof Have that for all $[a_1 : ... : a_n] \in U$ it holds that

$$1 \notin \langle f_1(x, a_1, ..., a_n), ..., f_m(x, a_1, ..., a_n)\rangle \leq k[x]$$

where $\mathbb{I}^+(V) = \langle f_1, ..., f_m\rangle$ homogeneous ideal. We show that there is a joint solution α in the algebraic closure K of $k(W)$ of the equations

$$\langle f_1(x, y_1, ..., y_n), ..., f_m(x, y_1, ..., y_n\rangle \leq k[W][x]$$

Assume not, then Hilbert's Nullstellensatz yields that $1 = \sum_i \tilde{g}_i f_i(x, y_1, ..., y_n)$ for $\tilde{g}_i \in k(W)[x]$ (here we use the nontrivial fact that $IK[x] \cap k(W)[x] = I$ for $I \leq k(W)[x]$). In particular, we find

$$g = \sum_i g_i f_i(x, y_1, ..., y_n)$$

for $g_i \in k[W][x]$ and $g \in k[W] \setminus \{0\}$.

Consider now the open subset $S := W \setminus \mathbb{V}(g) \subseteq W$. Now for each $b \in S$ we find a well-defined ring homomorphism

$$k[W] \to k, \quad f \in R \mapsto f(b)$$

In particular, the image of $f_i(x, y_1, ..., y_n)$ under this map is $f_i(x, b_1, ..., b_n)$. Thus we find a representation

$$g(b_1, ..., b_n) = \sum_i g_i' f_i(x, b_1, ..., b_n) \in k^*$$

where $g_i' \in k[x]$ is the image of $g_i \in k[W][x]$. This shows that for $b \in S$ there is no $b_0 \in k$ with $[b_0 : ... : b_n] \in V$. However, U is dense in W and S is open, so $U \cap S \neq \emptyset$, a contradiction.

So let now $\alpha \in K$ be a universal solution of $f_i(x, y_1, ..., y_n)$. Further, let $t \in k[W]$ such that $t\alpha$ is integral over $k[W]$. Consider the minimal polynomial $F \in k[W][T]$ of $t\alpha$ over $k(W)$. Now let $b \in W$. As $F \in k[W][T]$ is monic, $F(b) \in k[T]$ is a well-defined, non-constant polynomial. Hence, it has a root $\beta \in k$ and we can consider the "evaluation map"

$$k[W][t\alpha] \to k, \quad y_i \mapsto b_i,\ t\alpha \mapsto \beta$$

As the f_i are homogenous, find $f_i(t\alpha, ty_1, ..., ty_n) = t^{\deg f_i}(\alpha, y_1, ..., y_n) = 0$. Hence, taking the image under the above ring homomorphism yields

$$0 = f_i(\beta, t(b)b_1, ..., t(b)b_n)$$

Thus there is $[\beta, t(b)b_1, ..., t(b)b_n] \in V$, but since $[1 : 0 : ... : 0] \notin V$ by assumption, we see that $t(b) \neq 0$ and the claim is shown. □

6 Probabilities

6.1 Chernoff-Hoeffding

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

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

7 Analysis

7.1 Inequalities

Young's inequality

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

Proof By convexity of log, have

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

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

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

Proof By Young's inequality have

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

8 Measure and Integration theory

8.1 Dominated convergence theorem

Riemann-integral Let (f_n) be a sequence of Riemann-integrable functions $\mathbb{R} \to \mathbb{C}$ that converges pointwise to $f : \mathbb{R} \to \mathbb{C}$. If

- (f_n) is dominated, i.e. there is a Riemann-integrable function $g : \mathbb{R} \to \mathbb{R}_+$ with finite integral and $|f_n(x)| \leq g(x)$ for all $x \in \mathbb{R}$
- f is Riemann-integrable

then

$$\lim_{n \mapsto \infty} \int_{-\infty}^{\infty} f_n(x)dx = \int_{-\infty}^{\infty} f(x)dx$$

Measure integral Let (f_n) be a sequence of measurable functions $S \to \mathbb{C}$ in a measure space (S, Σ, μ) that converges pointwise to $f : S \to \mathbb{C}$ and is dominated by a measurable function $g : S \to \mathbb{R}_+$ with finite integral. Then f is measurable and

$$\lim_{n \mapsto \infty} \int f_n(x)dx = \int f(x)dx$$

8.2 Transformation

Let $\phi : U \to \mathbb{R}^n$ be injective and $f : \mathbb{R}^n \to \mathbb{R}$ be Riemann-integrable. Then

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

8.3 Fubini's theorem

Let X and Y be σ-finite measure spaces and consider a $X \times Y$-measurable function $f : X \times Y \to \mathbb{C}$. If

$$\int_{X \times Y} |f(x, y)| d(x, y) \quad \text{is finite}$$

then

$$\int_X \int_Y f(x, y)dy \; dx = \int_{X \times Y} f(x, y)d(x, y) = \int_Y \int_X f(x, y)dy \; dx$$

9 Topology

9.1 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

9.2 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.

9.3 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 $f_\alpha : X \to (X_\alpha, \tau_\alpha)$.

9.4 Characterization of compactness

The following are equivalent, where (X, τ) 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 κ 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 κ is infinite, so a limit ordinal. Therefore $\mathcal{A}$ is a monotone union of sets in $\mathcal{S}$ (by minimality of κ), so in $\mathcal{S}$. Then $\mathcal{S} = 2^{\mathcal{D}}$ so $\mathcal{D} \in \mathcal{S}$ and therefore $\bigcap \mathcal{D} \neq \emptyset$.

9.5 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.

9.6 Urysohn's Lemma

For closed C_0, C_1 in a T4 space X there is a continuous $f : X \to [0,1]$ 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 $f(x) := \inf\{q \in \mathbb{Q} \cap [0,1] \mid x \in U_q\} \cup \{1\}$.

9.7 Tietze's extension theorem

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

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

9.8 Extension of uniformly continuous functions

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

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

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

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 $\tilde{f}(x_i) \to \tilde{f}(x)$. Construct a net $(w_j)_{j\in J}$ in D such that $w_j \to x$ and $\tilde{f}(w_j)$ is outside of the closure of a fixed neighborhood N of $\tilde{f}(x)$. This contradicts the assumption.

9.9 Irreducibility

If X is a noetherian topological space, then there are only finitely many irreducible components.

Proof idea Consider a minimal closed set A that is not a finite union of irreducible closed sets. However, A cannot be the union of two proper closed subsets as these would be a finite union of irreducible closed sets. Thus $A = X$ and the claim follows.

10 Combinatorics

10.1 LYM inequality

Let $\mathcal{F} \subseteq \mathcal{P}(n)$ be an antichain. Then

$$\sum_{i=0}^{n} \frac{|\mathcal{F} \cap [n]^{(i)}|}{\binom{n}{i}} \leq 1$$

with equality iff $\mathcal{F} = [n]^{(r)}$. In particular, Sperner's lemma "the maximal size of an antichain is $\binom{n}{\lfloor n/2 \rfloor}$" follows

Proof idea Use "local LYM": For any $\mathcal{A} \subseteq [n]^{(r)}$ have

$$\frac{|\partial \mathcal{A}|}{\binom{n}{r-1}} \geq \frac{|\mathcal{A}|}{\binom{n}{r}}$$

with equality iff $\mathcal{A} = \emptyset$ or $\mathcal{A} = [n]^{(r)}$. This can easily be shown by using double counting on the edges of the bipartite graph $[n]^{(r)} \sqcup [n]^{(r-1)}$. Using this inductively with sets

$$\mathcal{G}_r := (\mathcal{F} \cap [n]^r) \cup \mathcal{G}_{r+1}$$

we can show the LYM inequality. □

10.2 Dilworth's Theorem

Let P be a finite poset. Then

$$m := \min\{|\mathcal{C}| \mid \mathcal{C} \subseteq \mathcal{P}(P) \text{ chain decomposition}\} = \max\{|A| \mid A \subseteq P \text{ antichain}\}$$

Proof idea Induction on $|P|$. In the inductive step, consider a maximal chain $C \subseteq P$. Assume that $P \setminus C$ has an antichain A of size m, otherwise the claim follows by the induction hypothesis. Then consider

$$S^+ := \{x \in P \mid x \geq a \text{ for some } a \in A\}$$
$$S^- := \{x \in P \mid x \leq a \text{ for some } a \in A\}$$

Now apply the induction hypothesis on S^+ and S^- and deduce the claim. □

10.3 Symmetric chain decomposition

There exists a decomposition of $\mathcal{P}(n)$ into symmetric chains.

Proof idea Use induction on n, and for a chain $C \subseteq \mathcal{P}(n-1)$ build two chains

$$C^+ := C \cup \{\max C \cup \{n\}\} \quad \text{and} \quad C^- := \{A \cup \{n\} \mid A \in C, A \neq \max C\}$$

10.4 Kleitman's (first) theorem

Let $x_1, ..., x_n \in \mathbb{R}^k$ with $\|x_i\| \geq 1$ and $K \subseteq \mathbb{R}^k$ with diameter less than 1. Then there are at most $\binom{n}{\lfloor n/2 \rfloor}$ sets $A \subseteq [n]$ such that $x_A := \sum_{i \in A} x_i \in K$.

Proof idea Call a set system $\mathcal{F} \subseteq \mathcal{P}(n)$ sparse, if $\|x_A - x_B\| \geq 1$ for all $A, B \in \mathcal{F}, A \neq B$. A partition of $\mathcal{P}(n)$ is called symmetric, if it satisfies the modified conditions of a symmetric chain decomposition (i.e. there is r such that an element of the partition contains exactly one set from $[n]^{(r)}, ..., [n]^{(n-r)}$ and no other sets).

By induction on n we create a symmetric decomposition into sparse sets, and the claim follows. By induction hypothesis, have a symmetric decomposition into sparse sets of $\mathcal{P}(n-1)$, and for one of these sparse sets $S = \{F_1, ..., F_l\}$ with wlog

$$\langle x_{F_1}, \frac{x_n}{\|x_n\|} \rangle, ..., \langle x_{F_{l-1}}, \frac{x_n}{\|x_n\|} \rangle \ \leq \ \langle x_{F_l}, \frac{x_n}{\|x_n\|} \rangle$$

define

$$S^+ := S \cup \{F_l \cup \{n\}\} \quad \text{and} \quad S^- := \{F_1 \cup \{n\}, ..., F_{l-1} \cup \{n\}\}$$

Using that $\|x_{F_l \cup \{n\}} - x_{F_i}\| \geq \langle x_{F_l \cup \{n\}} - x_{F_i}, \frac{x_n}{\|x_n\|} \rangle$, one can show that these are sparse.□

10.5 Kruskal-Katona theorem

Let $\mathcal{F} \subseteq [n]^{(r)}$ and let $\mathcal{A} \subseteq [n]^{(r)}$ be the first $|\mathcal{F}|$ sets of $[n]^{(r)}$ in colex-order. Then

$$|\partial \mathcal{F}| \geq |\partial \mathcal{A}|$$

Proof idea Use a compression operator: For $U, V \subseteq \mathbb{N}$ with $|U| = |V|$ finite, let

$$C_{UV}(A) := \begin{cases} (A \setminus V) \cup U & \text{if } V \subseteq A, U \cap A = \emptyset \\ A & \text{otherwise} \end{cases}$$

and

$$C_{UV}(\mathcal{A}) := \{C_{UV}(A) \mid A \in \mathcal{A}\} \cup \{A \in \mathcal{A} \mid C_{UV}(A) \in \mathcal{A}\}$$

First show the following claim: If U, V are disjoint and

$$\forall u \in U \ \exists v \in V : \ C_{(U \setminus \{u\})(V \setminus \{v\})}(\mathcal{F}) = \mathcal{F}$$

then $|\partial C_{UV}(\mathcal{F})| \leq |\partial \mathcal{F}|$. Now we can apply C_{UV} for all $U <_{\text{colex}} V$ in order of increasing $|U| = |V|$ and get the initial colex segment. By the claim, the size of the shadow never increased. □

10.6 Erdös-Ko-Rado theorem

Let $\mathcal{A} \subseteq [n]^{(r)}$ be intersecting, then $|\mathcal{A}| \leq \binom{n-1}{r-1}$.

Proof idea Either apply Kruskal-Katona often, or use the "Katona circle method": Call $A \in \mathcal{A}$ interval w.r.t. $\pi : [n] \to \mathbb{Z}/n\mathbb{Z}$ bijection, if $\pi(A) = \{k, k+1, ..., k+r-1\}$ for some k. w.r.t. one π, there are only at most r intervals in $\mathcal{A}$. On the other hand, each $A \in \mathcal{A}$ is an interval w.r.t. $nr!(n-r)!$ different π. Thus double-counting (A, π) interval pairs, we see that $|\mathcal{A}|nr!(n-r)! \leq n!r$ and the claim follows. □

10.7 Two families theorem

Let $A_1, ..., A_k, B_1, ..., B_k$ be finite sets such that for $i \neq j$ have

$$A_i \cap B_i = \emptyset \quad \text{and} \quad A_i \cap B_j \neq \emptyset$$

Then $\sum_i \binom{|A_i|+|B_i|}{|A_i|}^{-1} \leq 1$. In particular, if $|A_i| = a, |B_i| = b$ then $k \leq \binom{a+b}{a}$.

Proof idea Consider uniformly random permutations $\pi \in S_n$ and say $A <_\pi B :\Leftrightarrow \max \pi(A) < \min \pi(B)$. Then

$$\Pr[A_i <_\pi B_i] = \binom{|A_i| + |B_i|}{|A_i|}^{-1}$$

and applying union bound yields the result. □

10.8 Polynomial Bounding Method

Consider $\mathcal{F} = \{A_1, ..., A_m\} \subseteq \mathcal{P}(n)$ and $V = \{\chi_F \mid F \in \mathcal{F}\} \subseteq \mathbb{A}^n$. If we find polynomials $f_1, ..., f_m \in k[x_1, ..., x_n]_{\leq s}$ such that

$$(f_i(\chi_{A_j}))_{ij} = \begin{pmatrix} f_1(\chi_{A_1}) & \cdots & f_1(\chi_{A_m}) \\ \vdots & \ddots & \vdots \\ f_m(\chi_{A_1}) & \cdots & f_m(\chi_{A_m}) \end{pmatrix}$$

is invertible, then $\dim_k k[x_1, ..., x_n]_{\leq s}/\mathbb{I}(V) \geq \dim_k k[x_1, ..., x_n]/\mathbb{I}(V)$. In particular, it follows that

$$k[x_1, ..., x_n]_{\leq s}/\mathbb{I}(V) = k[x_1, ..., x_n]/\mathbb{I}(V) = k[V]$$

and $|\mathcal{F}| = |V| = \dim_k k[x_1, ..., x_n]_{\leq s}/\mathbb{I}(V) \leq \dim_k k[x_1, ..., x_n]_{\leq s}/I$ for any $I \subseteq \mathbb{I}(V)$. Note further that if $x_i - x_i^j \in \mathbb{I}(V)$ for all i, j, then

$$\dim_k k[x_1, ..., x_n]_{\leq s}/\mathbb{I}(V) \leq \sum_{i=0}^{s} \binom{n}{i}$$

10.9 Sauer-Shelah theorem

If $\mathcal{F} \subseteq \mathcal{P}(n)$ has VC-dimension at most d, then $|\mathcal{F}| \leq \sum_{i=0}^{d} \binom{n}{i}$.

Proof idea Boring inductive proof on $n + d$. An alternative is to consider with $V = \{\chi_F \mid F \in \mathcal{F}\} \subseteq \mathbb{A}^n_{\mathbb{R}}$. We show that $\mathbb{R}[x_1, ..., x_n]_{\leq d}/\mathbb{I}(V) = \mathbb{R}[x_1, ..., x_n]/\mathbb{I}(V)$ and are done, as $|\mathcal{F}| = |V| = \dim_{\mathbb{R}} \mathbb{R}[V]$ and

$$\dim_{\mathbb{R}} \mathbb{R}[x_1, ..., x_n]_{\leq d}/\mathbb{I}(V) \leq \dim_{\mathbb{R}} \mathbb{R}[x_1, ..., x_n]_{\leq s}/\langle x_i - x_i^j \mid i \leq n, j\rangle = \sum_{i=0}^{d} \binom{n}{i}$$

Assume not, i.e. there is $\overline{f} \in \mathbb{R}[V] \setminus \mathbb{R}[x_1, ..., x_n]_{\leq d}/\mathbb{I}(V)$. wlog $f \in \mathbb{R}[x_1, ..., x_n]$ has minimal degree $\deg(f) > d$ among all representatives of $\overline{f}$. wlog $f = \prod_{i \in A} x_i$ is a monomial. However $|A| > d$ so there is $B \subseteq A$ with $F \cap A \neq B$ for all $F \in \mathcal{F}$. Then

$$q := \prod_{i \in B} x_i \prod_{i \in A \setminus B} (1 - x_i) \in \mathbb{I}(V)$$

but $q - p$ has degree $< \deg(p)$, a contradiction. □

10.10 Kleitman's (second) theorem

Let $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}(n)$ be downsets. Then

$$|\mathcal{A} \cap \mathcal{B}| \geq \frac{|\mathcal{A}||\mathcal{B}|}{2^n}$$

Proof Idea Induction on n. Decompose $\mathcal{A}$ and $\mathcal{B}$ as

$$\mathcal{A}^+ = \{A \subseteq [n-1] \mid A \cup \{n\} \in \mathcal{A}\}$$
$$\mathcal{A}^- = \{A \subseteq [n-1] \mid A \in \mathcal{A}\}$$

and similarly for $\mathcal{B}$. Using the induction hypothesis, one can directly show the claim now. □

10.11 Fisher's Inequality

Let $k \geq 1$ and $\mathcal{F} \subseteq \mathcal{P}(n)$ such that for all $A, B \in \mathcal{F}, A \neq B$ have $|A \cap B| = k$. Then $\mathcal{F} \leq n$.

Proof Idea If no $A \in \mathcal{F}$ satisfies $|A| = k$, one can show that all the $\chi_A, A \in \mathcal{F}$ are linearly independent.

10.12 Oddtown theorem

Let $\mathcal{F} \subseteq \mathcal{P}(n)$ such that $|A|$ is odd and $|A \cap B|$ is even for $A, B \in \mathcal{F}, A \neq B$. Then $|\mathcal{F}| \leq n$.

Proof Idea In $\mathbb{F}_2$ we have $\langle \chi_A, \chi_B \rangle = \delta_{AB}$. Writing this as a matrix product and using the rank directly shows the claim. □

10.13 Frankl-Wilson theorem

Let $\mathcal{F} \subseteq \mathcal{P}(n)$ and assume one of the following two cases

Modular version Let $S \subseteq \mathbb{Z}/p\mathbb{Z}$ for a prime p and suppose $\overline{|A|} \notin S$ and $\overline{|A \cap B|} \in S$ for all $A, B \in \mathcal{F}, A \neq B$

Normal version Let $S \subseteq \mathbb{N}$ and suppose $\mathcal{F}$ is S-intersection (i.e. $|A \cap B| \in S$ for all $A, B \in \mathcal{F}, A \neq B$)

Then

$$|\mathcal{F}| \leq \sum_{i=0}^{|S|} \binom{n}{i}$$

Proof Idea For the modular version, let

$$f_A := \prod_{s \in S} (s - \sum_{i \in A} x_i) \in \mathbb{F}_p[x_1, ..., x_n]$$

For the standard version, assume $\mathcal{F} = \{F_1, ..., F_m\}$ with $|F_i| \leq |F_j|$ for $i \leq j$ and consider

$$f_j = f_{F_j} = \prod_{s \in S, s < |F_j|} (s - \sum_{i \in F_j} x_i) \in \mathbb{R}[x_1, ..., x_n]$$

Now apply 10.8. □

10.14 Ray-Chaudhuri-Wilson theorem

Let $\mathcal{F} \subseteq [n]^{(r)}$ be S-intersecting. Then $|\mathcal{F}| \leq \binom{n}{|S|}$.

Proof Idea Again let

$$f_A := \prod_{s \in S} (s - \sum_{i \in A} x_i) \in \mathbb{R}[x_1, ..., x_n]$$

and note that they are linearly independent in $k[V]$ for $V = \{\chi_A \mid A \in \mathcal{F}\}$. So we no want to bound $\dim_{\mathbb{R}} \mathbb{R}[x_1, ..., x_n]_{\leq |S|} / \mathbb{I}(V)$. Note that $q := r - \sum_i x_i \in \mathbb{I}(V)$. So with $I = \langle x_i - x_i^j \mid i, j \rangle$ have

$$\dim_{\mathbb{R}} \mathbb{R}[x]_{\leq |S|} / \mathbb{I}(V) \leq \dim_{\mathbb{R}} \mathbb{R}[x]_{\leq |S|} / I - \dim_{\mathbb{R}} \underbrace{(q)_{\leq |S|} / (I \cap (q))}_{\cong \mathbb{R}[x]_{\leq |S|-1}/I} = \sum_{i=0}^{|S|} \binom{n}{i} - \sum_{i=0}^{|S|-1} \binom{n}{i}$$

11 Discrete

11.1 Gamma Function

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

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

We get

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

12 Functional analysis

12.1 Minkowski-functional

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

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

is

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

12.2 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.

12.3 Baire's theorem

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

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

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

12.4 Open mapping theorem

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

Proof idea

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

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

12.4.1 Lemma

Let $T \in \mathcal{L}(X, Y)$ such that $0 \in \operatorname{cl}(T(B_X))^\circ \neq \emptyset$. 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 $y \in \epsilon B_Y \subseteq \operatorname{cl}(T(B_X))$. Recursivly construct sequences $(x_n)_{n\in\mathbb{N}}$ in X and $(y_n)_{n\in\mathbb{N}}$ in Y with

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

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

12.5 Hahn-Banach dominated extension theorem

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

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

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

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

12.6 Banach-Alaoglu

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

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

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

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

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

13 Operator theory

13.1 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

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

13.2 Compact Operators and spaces

From 13.2.1 one can conclude that the unit ball B_X is compact iff $\dim X < \infty$. Therefore, consider operators $T \in \mathcal{L}(X, Y)$ such that $\mathrm{cl}(T(B_X))$ compact, these are a Banach space $\mathcal{K}(X, Y)$.

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

13.2.1 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.

13.3 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. $\forall x \in X, \epsilon > 0$ $\exists$neighborhood N of x $\forall x \in M:\ x(N) \subseteq B_\epsilon(x(s))$), then M is compact.

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

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

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

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

13.4 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 $\|x_n - x\| \to d := \inf_{y\in K} \|y - x\|$ we then have:

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

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

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

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

13.5 Frechet-Riesz representation theorem

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

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

Proof Show surjectivity, the rest is clear: For $x' \in H'$ have that $(\ker(x'))^\perp$ has dimension 1. By using 13.4 the claim follows.

13.6 Spectra

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

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

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

Proof idea Use the Neumann series $\sum_n T^n = (1-T)^{-1}$ if convergent.

13.7 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 λ_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 $\{e_{\lambda,1}, ..., e_{\lambda,n_\lambda}\}$ 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 $T_2 := T\big|_{H_2} : H_2 \to H_2$ 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 next lemmas:

13.7.1 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

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

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. □

13.7.2 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 $|\lambda| = \|T\|_{\text{op}}$.

13.7.3 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 13.7.1 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 $y_n \in \text{span}\{x_1, ..., x_n\}$ with distance $\frac{1}{2}$ to $\text{span}\{x_1, ..., x_{n-1}\}$ and $\|y_n\| = 1$. Then Ty_n has distance $\frac{1}{2}\epsilon$ from $\text{span}\{Tx_1, ..., Tx_{n-1}\}$, but this contradicts the compactness of T.

13.8 Singular value decomposition

Let $T \in \mathcal{K}(H_1, H_2)$. Then there is $N = \{1, ..., n\}$ 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 13.7). 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. □

14 (Algebraic) Number Theory

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

2.10 Each 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).

14.2 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 $X \cap \Gamma \neq \emptyset$.

14.3 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 Cl_K. In particular, every $c \in \mathrm{Cl}_K$ 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 $K \to \mathbb{C}$ 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 $(\gamma) = \gamma\mathfrak{a}^{-1}\mathfrak{a} \mid a\mathfrak{a}$. □

14.4 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 $K \to \mathbb{R}$ and s is the number of conjugate pairs of complex $\mathbb{Q}$-embeddings $K \to \mathbb{C}$.

14.5 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 $D \equiv 1 \mod 4$ 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 ... $= 4$ if this has no integral solution).

In the case $D < 0$, have that

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

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

14.6 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 $\mathfrak{p}\mathcal{O} = \mathfrak{B}_1^{e_1} ... \mathfrak{B}_r^{e_r}$ 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 $\mathfrak{p} = \mathfrak{B}_1^{e_1} ... \mathfrak{B}_r^{e_r}$ for $\mathfrak{B}_i = \mathfrak{p}\mathcal{O} + p_i(\alpha)\mathcal{O}$, where the minimal polynomial p of α splits into irreducible factors mod $\mathfrak{p}\mathcal{O}$

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

Also have $f_i = \deg(p_i)$.

By definition of $\mathcal{F}$, note that for a number field K (i.e. $\mathcal{R} = \mathbb{Z}$) it is sufficient if $\mathfrak{p} = (p) \not| ([\mathcal{O} : \mathbb{Z}[\alpha]])$.

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

"Zerlegungsgruppe" $G_\mathfrak{B} := \{\sigma \in G \mid \sigma\mathfrak{B} = \mathfrak{B}\}$ with fixed field $Z_\mathfrak{B} = L^{G_\mathfrak{B}}$

"Trägheitsgruppe" $I_\mathfrak{B} := \ker(\phi)$ with fixed field $T_\mathfrak{B} = L^{I_\mathfrak{B}}$

where

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

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:

$$\mathfrak{p} \quad \underset{1}{\overset{1}{\subseteq}} \quad \mathfrak{B}_Z := \mathfrak{B} \cap Z_{\mathfrak{B}} \quad \underset{1}{\overset{f}{\subseteq}} \quad \mathfrak{B}_T := \mathfrak{B} \cap T_{\mathfrak{B}} \quad \underset{e}{\overset{1}{\subseteq}} \quad \mathfrak{B}$$

where the "Verzweigungsindizes" are written over the corresponding ideal decompositions and the "Trägheitsindizes" are written below, respectivly.

14.7 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

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

Then for odd a, n have

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

15 Elliptic Curves

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

15.1 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

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

for $a_1, ..., a_6 \in K$ 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.

15.2 Picard group structure

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

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

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

$$\bar{\sigma} : \mathrm{Pic}^0(E) \to E, \quad \overline{D} \mapsto \sigma(D)$$

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

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

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 ϕ 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, $\mathrm{Cl}(K[E])$ is generated by $\mathrm{im}\phi$. Note that $\langle x-\lambda, y-\mu\rangle\langle x-\lambda, y+\mu\rangle =$

$\langle x - \lambda \rangle$ is principal, so imϕ is inversion-closed. Lastly show that imϕ 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. □

15.3 Isogenies

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

Proof If ψ is a morphism, then

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

is a ring homomorphism. In particular, ψ^* is also a group isomorphism between the class groups. Now have $\psi = \phi^{-1} \circ \psi^* \circ \phi$ for the ϕ from 15.2.

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 ψ_* between the Picard groups. □

15.4 Nonconstant isogenies are surjective

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

Proof The image of ϕ is closed in the Zariski-topology, so either ϕ surjective or ϕ has finite image as E_2 is an irreducible 1-dimensional variety. However, the kernel of ϕ is the fiber $\phi^{-1}(\mathcal{O})$ which does not contain E_1 by assumption. Thus $\phi^{-1}(\mathcal{O})$ is a proper subvariety of E_1 and hence 0-dimensional. Thus $\ker \phi$ is finite, so ϕ cannot have finite image.

16 Computational Algebraic Number theory and Cryptanalysis

16.1 Primality test

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

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

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

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

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 bee 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

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

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

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

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

$$\left(\frac{a}{p_i}\right) = -1 \ \Leftrightarrow\ 2\text{ord}[a]_{p_i} \not| \ p_i - 1 \ \Leftrightarrow\ 2^{r+2} d_i \not| \ p_i - 1 \ \Leftrightarrow\ 2^{r+2} \not| \ p_i - 1 \ \Leftrightarrow\ b_i \perp 2$$

This yields

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

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

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

so

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

and at last we get

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

□

16.2 Hidden Subgroup Problem

Given a group G together with a group homomorphism $f : G \to X$ 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 ζ, 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 $k \in \{0, ..., N-1\}, f(x_0) \in X$ is equal to

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

$$= \frac{1}{N^2} \left| \sum_{l=0}^{M} \zeta^{kbl} \right|^2 = \frac{1}{N^2} \left| \frac{1 - \zeta^{kb(M+1)}}{1 - \zeta^{kb}} \right|^2 = \frac{1}{N^2} \left| \frac{\sin(2\pi \frac{kb(M+1)}{N})}{\sin(2\pi \frac{kb}{N})} \right|^2$$

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

As b is odd, have $\overline{b} \in \mathbb{Z}_N^*$ and so there are at least b different $k \in \{0, ..., N-1\}$ such that $|kb \mod N| \leq \frac{b}{2}$. For such a k, have that $\delta_k := \frac{kb}{N} - \lfloor \frac{kb}{N} \rceil$ is at most $\frac{b}{2N}$ in absolute value. Thus

$$\sin\left(2\pi \frac{kb}{N}\right) = \sin(2\pi\delta_k) \leq |\delta_k|$$

and $\delta_k(M+1)$ is at most $\frac{N}{b} \frac{b}{2N} = \frac{1}{2}$ in absolute value, so (sin is convex in $[0, \frac{1}{2}]$)

$$\sin\left(2\pi \frac{kb(M+1)}{N}\right) = \sin(2\pi\delta_k(M+1)) \geq |\delta_k|(M+1) \sin\left(\frac{1}{2}\right) \geq \frac{|\delta_k|(M+1)}{3}$$

It follows that

$$\frac{1}{N^2} \left| \frac{\sin(2\pi \frac{kb(M+1)}{N})}{\sin(2\pi \frac{kb}{N})} \right|^2 \geq \frac{1}{N^2} \left(\frac{|\delta_k|(M+1)}{3} \frac{1}{|\delta_k|} \right)^2 = \frac{(M+1)^2}{9N^2} \geq \frac{1}{9b^2} \left(1 - \frac{2b}{N} + \frac{b^2}{N^2} \right)$$

As f takes different values on different cosets, we have b different values of the form $f(x_0)$. For each of them, the above applies, so the probability that we measure any value where the first component is a fixed $k \in \{0, ..., N-1\}$ with $|\delta_k| \leq \frac{b}{2N}$ is at least

$$b \cdot \frac{1 - \epsilon}{9b^2} = \frac{1 - \epsilon}{9b}$$

where $\epsilon = 1 - \frac{2b}{N} + \frac{b^2}{N^2}$.

As there are at least b such k, the probability that we measure a value whose first component satisfies $|\delta_k| \leq \frac{b}{2N}$ is at least

$$b \cdot \frac{1-\epsilon}{9b} = \frac{1-\epsilon}{9}$$

If N is sufficiently large - say $N \geq b^2$ - then $\epsilon \in \Theta(\frac{1}{b})$, hence we can find a k with $|\delta_k| \leq \frac{b}{2N}$ in polynomial time. Using continued fractions, we can extract b from this.

17 Algorithms

17.1 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), ..., (X_n, k_m) 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 λ is the positive root of the branching vector polynomial equation (there exactly one, as the $m-1, ..., 0$-th derivates 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)

17.2 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.