PREDAVANJA

Direktne vsote

Def: Grupa G je **notranji direktni produkt (DP)** svojih podgrup edink $N_1,\dots,N_s$, če velja:
(i) $G = N_1\cdots N_s$
(ii) $N_i \cap (N_1\cdots N_{i-1}\cdot N_{i+1}\cdots N_s) = \{1\}$ za $\forall i\in[s]$.

Trditev: Naj bodo $N_1,\dots,N_s \lhd G$, potem sta naslednji trditvi ekvivalentni:
(i) G je DP $N_1,\dots,N_s$
(ii) $\forall a\in G$ lahko na en sam način zapišemo kot $n_1n_2\cdots n_s$ za $n_i\in N_i$.

Def: **Komutator** elementov $a,b\in G$ je $[a,b] := aba^{-1}b^{-1}$.

Trditev: $M,N\lhd G \wedge M\cap N=\{1\} \implies \forall m\in M,\forall n\in N: mn=nm$.

Izrek: G DP $N_1,\dots,N_s \implies G\cong N_1\times\cdots\times N_s$.

Def: Naj bo G NDP $N_1,\dots,N_s$. Če je G aditivna (Abelova), namesto direktni produkt pravimo **direktna vsota (DV)** in pišemo $G = N_1\oplus\cdots\oplus N_s$.

Trditev: Naj bo G Abelova in $|G| = mn$ za $m\perp n$. Potem za $H := \{x\in G \mid mx=0\}$ in $K := \{x\in G\mid nx=0\}$ velja $G=H\oplus K$, $|H|=m$ in $|K|=n$.

Posledica: $m\perp n \implies \mathbb{Z}_{mn}\cong \mathbb{Z}_m\oplus\mathbb{Z}_n$.

Trditev: Naj bo G Abelova in $|G| = p_1^{k_1}\cdots p_s^{k_s}$ kjer p_i različna praštevila. Potem podgrupe $H_i = \{x\in G\mid p_i^{k_i}x=0\}$ za $i\in[s]$ zadoščajo $|H_i| = p_i^{k_i}$ in $G = H_1\oplus\cdots\oplus H_s$.

Def: Naj bo $p\in\mathbb{P}$ in G grupa reda p^k za $k\ge 0$. Potem je G **p-grupa**.

Trditev: Naj bo G Abelova netrivialna p-grupa. Potem je G ciklična $\iff$ ima samo eno podgrupo redo p.

Trditev: Naj bo G končna Abelova p-grupa in C ciklična podgrupa z največjim redom. Potem $\exists K\le G: G = C\oplus K$.

Izrek: **(osnovni izrek o končnih Abelovih grupah)** ∀ končna Abelova grupa G je DV cikličnih p-podgrup. Če je G DV $C_1,\cdots,C_n$ in hkrati DV $D_1,\cdots,D_{n'}$, potem je $n=n'$ in $\exists\sigma\in S_n\ \forall i\in[n]: C_i\cong D_{\sigma(i)}$.

Def: Naj bo G grupa, potem je $T(G) = \{g\in G\mid \mathrm{red}(g)<\infty\}$ **torzijska podgrupa** G. Če je $T(G)=\{0\}$, pravimo, da je G **brez torzije**.

Izrek: Naj bo G končno generirana Abelova grupa. Potem je $G\cong \mathbb{Z}^m\oplus K$, kjer je K končna Abelova grupa.

Trditev: Če je G končno generirana Abelova grupa brez torzije, potem je $G\cong\mathbb{Z}^n$, za nek $n\in\mathbb{N}$.

Trditev: ∀ končno generirana Abelova grupa je DV neke končno generirane Abelove grupe brez torzije in neke končne Abelove grupe.

Def: Naj bo K kolobar, $e\in K$ je **idempotent**, če $e^2=e$. Če zraven še $ae=ea$ za $\forall a\in K$, je **centralni idempotent**. Idempotenta e in f sta **ortogonalna**, če $ef=fe=0$.

Izrek: Naj bodo $I_1,\dots,I_s$ ideali kolobarja K, potem sta naslednji trditvi ekvivalentni:
(i) $K = I_1\oplus\cdots\oplus I_s$
(ii) ∃ paroma ortogonalni centralni idempotenti $e_1,\dots,e_s\in K$: $e_1+\cdots+e_s = 1\wedge\forall i\in[s]: I_i = e_iK$.

Izrek: $K = I_1\oplus\cdots\oplus I_s \implies K\cong I_1\times\cdots\times I_s$.

Delovanja grup

Izrek: **(Cayleyev izrek)** ∀ grupo lahko vložimo v neko simetrično grupo.

Def: Podgrupi simetrične grupe pravimo **permutacijska grupa.**

Posledica: ∀ končno grupo lahko vložimo v simetrično grupo S_n za nek $n\in\mathbb{N}$.

Def: Grupa G **deluje na množici** X, če $\exists\varphi: G\times X\to X$, $(g,x)\mapsto g\cdot x$, da velja:
(i) $\forall a,b\in G\ \forall x\in X: (ab)\cdot x = a\cdot(b\cdot x)$
(ii) $\forall x\in X: 1\cdot x = x$.
Preslikavi φ pravimo **delovanje grupe G na množici X**.

Def: Naj G deluje na X. **Orbita** elementa $x\in X$ je $G\cdot x := \{a\cdot x\mid a\in G\}$, **stabilizator** elementa x pa je $G_x := \{g\in G\mid g\cdot x = x\}$. **Množica fiksnih točk** $g\in G$ je $X^g := \{x\in X\mid g\cdot x = x\} = \mathrm{fix}(g)$, **fiksne točke/invariante delovanja** pa je množica $X^G := \bigcap_{g\in G} X^g = \mathrm{fix}(G)$.

Trditev: Naj G deluje na X, potem je $x\sim y \iff \exists a\in G: a\cdot x = y$ ekvivalenčna relacija, $[x] = G\cdot x$ in $G_x\le G$.

Def: Kvocientno množico $X/G = \{G\cdot x\mid x\in X\}$ imenujemo **prostor orbit**. Če je $|X/G|=1$, je delovanje **tranzitivno**.

Def: Naj bo G grupa in $x\in G$. Potem je njegov **konjugiranostni razred** $\mathrm{Raz}(x) := \{axa^{-1}\mid a\in G\}$, **centralizator** pa $C(x) := \{g\in G\mid xg = gx\}$.

Izrek: **(izrek o orbiti in stabilizatorju)** Naj G deluje na X. Potem za $\forall x\in X$ velja $|G\cdot x| = [G:G_x]$ in če G končna $|G| = |G\cdot x|\cdot|G_x|$.

Izrek: Naj G deluje netrivialno na končni X, potem $\exists x_1,\dots,x_m\in X\setminus X^G$, da je $|X| = |X^G| + \sum_{j=1}^m [G:G_{x_j}]$.

Posledica: Naj končna p-grupa G deluje na končni X. Potem $p\mid |X|-|X^G|$.

Izrek: **(Burnsideova lema)** Naj končna grupa G deluje na končni X, potem $|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|$.

Razredna formula in Cauchyjev izrek

Izrek: **(razredna formula)** Naj bo G končna grupa. Če G ni Abelova, potem $\exists x_1,\dots,x_m\in G\setminus Z(G)$, da je $|G| = |Z(G)| + \sum_{j=1}^m [G:C(x_j)]$.

Posledica: ∀ končna netrivialna p-grupa ima netrivialen center.

Posledica: $|G| = p^2$ za $p\in\mathbb{P}\implies G$ Abelova.

Izrek: **(Cauchyjev izrek)** Naj bo G končna grupa. Če praštevilo $p\mid |G|$, potem G vsebuje element reda p.

Posledica: Končna grupa je p-grupa $\iff$ red vsakega elementa je potenca p.

Izreki Sylowa

Def: Naj bo $H\le G$, množici $N(H) := \{a\in G\mid aHa^{-1} = H\}$ pravimo **normalizator** H.

Def: $H\le G$ je **p-podgrupa Sylowa**, če je $|H| = p^k\wedge p^{k+1}\nmid |G|$. Z n_p ozn. $\#p$-podgrup Sylowa grupe G.

Izrek: **(izreki Sylowa)** Naj praštevilo p deli red končne grupe G:
(a) $p^k \mid |G| \implies G$ vsebuje vsaj eno p-podgrupo reda p^k.
(b) $\forall p$-podgrupa G je vsebovani v kaki p-podgrupi Sylowa.
(c) $\forall p$-podgrupi Sylowa sta konjugirani.
(d) $\#p$-podgrup Sylowa grupe G deli $|G|$.
(e) $\#p$-podgrup Sylowa grupe G je $pm+1$ za nek $m\ge0$.

Posledica: $|G| = p^kt\wedge p\nmid t\implies n_p\mid t$.

Posledica: Naj bo S p-podgrupa Sylowa v G, potem $S\lhd G\iff n_p = 1$.

Končne enostavne grupe

Def: Grupa G je **enostavna**, če sta njeni edini podgrupi edinki $\{1\}$ in G.

Def: Naj bo G končna netrivialna grupa in podgrupe $M_i\le G$ take, da velja: $\{1\} = M_s\subseteq M_{s-1}\subseteq\cdots\subseteq M_0 = G$, $M_{i+1}\lhd M_i$ in M_i/M_{i+1} enostavne za $i=0,1,\dots,s-1$. Takemu zaporedju pravimo **kompozicijska vrsta** grupe G.

Izrek: **(Jordan-Hölderjev izrek)** Če sta $M_0,\dots,M_s$ in $N_0,\dots,N_t$ kompozicijski vrsti G, potem $t=s$ in $\exists\sigma\in S_t: N_i/N_{i+1}\cong M_{\sigma(i)}/M_{\sigma(i+1)}$.

Izrek: A_n je enostavna za $n\ge5$.

Izrek: **(klasifikacija končnih enostavnih grup)** Če je G lkončna enostavna grupa, potem sodi v eno izmed naslednjih družin:
(i) $\mathbb{Z}_p$, $p\in\mathbb{P}$
(ii) A_n, $n\ge5$
(iii) grupe Liejevega tipa
(iv) 26 Sporadičnih grup.

Rešljive grupe

Def: Grupa G je **rešljiva**, če $\exists N_0,\dots,N_m\lhd G$, da velja $\{1\} = N_0\subseteq N_1\subseteq\cdots\subseteq N_m = G$ in N_{i+1}/N_i je Abelova za $i=0,1,\dots,m-1$.

Def: Naj bo G grupa, z G' ozn. podgrupo generirano z vsemi komutatorji iz G in ji pravimo **komutatorska podgrupa**.

Trditev: $N\lhd G\implies N'\lhd G$.

Trditev: Naj bo $N\lhd G$. Potem je G/N Abelova $\iff G'\subseteq N$.

Izrek: Naj bo G grupa. Ozn. $G^{(0)} = G$ in induktivno $G^{(i+1)} := (G^{(i)})'$ za $i\ge0$. G je rešljiva $\iff \exists m\in\mathbb{N}: G^{(m)} = \{1\}$.

Posledica: Podgrupa rešljive grupe je rešljiva.

Posledica: Naj bo $N\lhd G$. G je rešljiva $\iff N$ in G/N sta rešljivi.

Izrek: **(Feit-Thompsonov izrek)** ∀ grupe lihe moči so rešljive.

Kolobarji polinomov

Trditev: Naj bo F polje, potem je $F[x]$ brez deliteljev niča.

Izrek: **(osnovni izrek o deljenju)** Za poljubna $f(x),g(x)\in F[x]$, kjer $g(x)\ne0$ in F polje, ∃ enolična $k(x),r(x)$, da velja $f(x) = k(x)\cdot g(x)+r(x)$, $\deg(r)<\deg(g)$.

Posledica: ∀ ideal v kolobarju $F[x]$, kjer F polje je glavni ideal.

Trditev: Naj bo F polje in $f(x)\in F[x]$. Potem je $a\in F$ ničla $f(x)\iff (x-a)\mid f(x)$.

Posledica: Naj bo F polje in $p(x)\ne 0\in F[x]$. Potem je v F kvečjemu $\deg(p)$ ničel $p(x)$.

Def: Naj bo F polje, $p(x)\in F[x]$, $\deg(p)>0$. Pravimo, da je $p(x)$ **nerazcepen nad** F, če iz $p(x) = g(x)\cdot h(x)$ za $g(x),h(x)\in F[x]$ sledi, da je eden od g,h konstanten.

Trditev: Naj bo F polje, $p(x)\in F[x]$, $\deg(p)>0$:
(i) $\deg(p)=1\implies p(x)$ nerazcepen
(ii) $\deg(p)\ge2$ in $p(x)$ nerazcepen $\implies$ nima ničle v F
(iii) $\deg(p)\in\{2,3\}\implies (p(x)$ nerazcepen $\iff$ nima ničle v F.

Def: $p(x) = a_nx^n+\cdots+a_0\in\mathbb{Z}[x]$ je **primitiven**, če so $a_0,\dots,a_n$ tuja.

Izrek: **(Gaussova lema)** Produkt primitivnih polinomov je primitiven polinom.

Izrek: Naj bo $f(x)\in\mathbb{Z}[x]$ tak, da ga ne moremo zapisati kot produkt dveh nekonstantnih polinomov v $\mathbb{Z}[x]$, potem je $f(x)$ nerazcepen nad $\mathbb{Q}[x]$.

Izrek: **(Eisensteinov kriterij)** Naj bo $f(x) = a_nx^n+\cdots+a_0$ in $\exists p\in\mathbb{P}$, da $p\mid a_i$ za $i<n$, $p\nmid a_n,a_0^2$. Potem je $f(x)$ nerazcepen nad $\mathbb{Q}[x]$.

Razširitve polj

Def: Naj bosta K,F polji in $F\subseteq K$, potem je K **razširitev** polja F, ozn. K/F.

Def: Naj bo K/F razširitev, potem je $a\in K$ **algebraičen** nad F, če $\exists p(x)\in F[x]: p(a)=0$. Če je $p(x)$ moničen in minimalne stopnje, pravimo da je $m_a(x) := p(x)$ **minimalni polinom** za a nad F in a stopnje algebraičnosti $\deg(m_a(x))$ nad F. Sicer je **transcendentalen** nad F. V primeru $F=\mathbb{Q}$ in $K=\mathbb{C}$, pravimo da je a **algebraično/transcen-**

dentalno število.
Izrek: π je transcendentalno nad $\mathbb{Q}$.
Izrek: Naj bo $a \in K$ algebraičen nad F in $p(x) \neq 0 \in F[x] : p(a) = 0$ moničen. Naslednje trditve so ekvivalentne:
(i) $p(x)$ *minimalen polinom za* a
(ii) $p(x)$ *nerazcepen*
(iii) $\forall q(x) \in F[x] : q(a) = 0 \implies p(x)|q(x)$

Končne razširitve

Def: Razširitev K/F je **končna**, če je K končno razsežen vektorski prostor nad F in pišemo $[K : F] := \dim_F(K)$.
Izrek: Naj bosta razširitvi L/K in K/F končni, potem:$[L : F] = [L : K] \cdot [K : F]$.
Posledica: Naj bo K/F končna razširitev in L podpolje K, ki vsebuje F, potem $[L : F]$ deli $[K : F]$.
Def: Razširitev K/F je **algebraična**, če je $\forall a \in K$ algebraičen nad F, sicer je **transcendentalna**.
Trditev: Vsaka končna razširitev je algebraična.
Def: Razširitev K/F je **enostavna/primitivna**, če $\exists a \in K : K = F(a)$. Elementu a pravimo **primitivni element** K.
Izrek: Naj bo K/F razširitev in $a \in K$ algebraičen nad F stopnje n. Potem je $F(a) = F[a] = \{\alpha_0 + \alpha_1 a + \cdots + \alpha_{n-1}a^{n-1} \mid \alpha_i \in F\}$ končna razširitev F in $[F(a) : F] = n$.
Izrek: Naj bo K/F razširitev in $a_1, \ldots, a_n \in K$ algebraični nad F. Potem je $F(a_1, \ldots, a_n) = F[a_1, \ldots, a_n]$ končna razširitev F.
Posledica: Naj bo K/F razširitev in $L = \{a \in K \mid a$ algebraičen nad $F\}$. L je podpolje K.

Konstrukcije z ravnilom in šestilom

Def: Naj bo $\mathcal{P} \subseteq \mathbb{R}^2$. Točka $T = (a,b) \in \mathbb{R}^2$ je **konstruktibilna iz $\mathcal{P}$**, če jo lahko skonstruiramo v s končnim številom operacij, kjer smemo: **(i)** narisati premico med točkama iz $\mathcal{P}$, **(ii)** narisati krožnico z središčem v točki iz $\mathcal{P}$ in točka iz $\mathcal{P}$ leži na krožnici, in je Z presek premic/krožnic. Za $\mathcal{P} = \{(0,0),(1,0)\}$ pravimo da je (a,b) **kosntruktibilna točka** in a,b **konstruktibilni števili**.
Izrek: Naj bo $\mathcal{P} \subseteq \mathbb{R}^2$ in $F \leq \mathbb{R}$ tako polje, da $\mathcal{P} \subseteq F \times F$. Če je $(a,b) \in \mathbb{R}^2$ konstruktibilna iz $\mathcal{P}$, potem sta a in b algebraični nad F stopnje 2^k za $k \geq 0$.
Posledica: Podvojitev (volumna) kocke je nemogoča samo z ravnilom in šestilom.
Posledica: Trisekcija kota $60°$ je nemogoča samo z ravnilom in šestilom.
Posledica: Konstrukcija kvadrata s površino danega kroga je nemogoča samo z ravnilom in šestilom.
Posledica: Množica konstruktibilnih števil je podpolje v $\mathbb{R}$.

Razpadna polja

Trditev: Naj bo K/F razširitev in $a \in K$: $\exists f(x) \in F[x] : f(a) = 0 \iff \exists g(x) \in K[x] : f(x) = (x - a) \cdot g(x)$.
Def: Če je $a \in K$ ničla $f(x) \in F[x]$ in $\exists h(x) \in K[x] : f(x) = (x - a)^k \cdot h(x) \wedge h(a) \neq 0$, je a **ničla večkratnosti k** za $f(x)$.
Izrek: Polinom $f(x) \in F[x]$ stopnje n ima največ n ničel, če je štejemo večkratnost ničel, v katerikoli razširitvi $K \supseteq F$.
Izrek: Naj bo $f(x) \in F[x] : \deg(f) > 0$, potem $\exists$ razširitev F, v kateri ima $f(x)$ ničlo.
Izrek: Naj bo $f(x) \in F[x] : \deg(f) = n > 0$, z vodilnim koeficientom c, potem $\exists$ razširitev F, ki vsebuje take $a_1, \ldots, a_n$, da $f(x) = c(x - a_1) \ldots (x - a_n)$.
Def: Naj bo K/F razširitev in $f(x) \in F[x]$. Pravimo da $f(x)$ **razpade** nad K, če je enak produktu linearnih polinomov v $K[x]$. Če $\nexists$ pravo podpolje K, v katerem $f(x)$ razpade, pravimo da je K **razpadno polje** $f(x)$ nad F.
Trditev: Naj bo $p(x) \in F[x]$ nerazcepen in a ničla $p(x)$ v neki razširitvi K/F. Če je $\varphi : F \to F'$ izomorfizem polj in a' ničla $p_\varphi(x)$ v neki razširitvi K'/F', potem $\exists$ enoličen izomorfizem $\Phi : F(a) \to F'(a')$, ki zadošča $\Phi(a) = a'$.
Izrek: Naj bo $f(x) \in F[x] : \deg(f) > 0$ in K razpadno polje $f(x)$ nad F. Če je $\varphi : F \to F'$ izomorfizem polj in K' razpadno polje $f_\varphi(x)$ nad F', potem lahko φ razširimo na izomorfizem med K in K'.
Posledica: Naj bo $f(x) \in F[x] : \deg(f) > 0$, potem je njegovo razpadno polje nad F eno samo do izomorfizma natančno.
Def: Razširitev K/F je **normalna**, če za $\forall p(x) \in K[x]$ velja: $\forall$ ničle $p(x)$ so v K ali nobena ničla $p(x)$ ni v K.
Izrek: Naj bo K/F končna razširitev, potem je K/F normalna $\iff$ K je razpadno polje nekega polinom iz $F[x]$.

Algebraično zaprtje polja

Def: Pravimo da je polje A **algebraično zaprto**, če za $\forall f(x) \in A[x]$ $\deg(f) > 0 \implies \exists a \in A : f(a) = 0$. Polje $\overline{A}$ je **algebraično zaprtje** A, če je algebraično zaprto in algebraična razširitev A.
Trditev: Naj bo K razširitev L in L algebraična razširitev F. Če je $a \in K$ algebraičen nad L, potem je algebraičen tudi nad F.
Izrek: Naj bo F podpolje algebraično zaprtega polja A. Potem je $\overline{F} = \{a \in A \mid a$ algebraičen nad $F\}$ algebraično zaprtje F.
Posledica: Polje $\forall$ algebraičnih števil je algebraično zaprtje $\mathbb{Q}$.

Končna polja

Trditev: Naj bo K končno polje in $char(K) = p$, potem je $|K| = p^n$ za nek $n \in \mathbb{N}$.
Trditev: Naj bo K polje in $|K| = p^n$, potem je K razpadno polje polinoma $f(x) = x^{p^n} - x$ nad $\mathbb{Z}_p$.
Trditev: Naj bo R komutativen kolobar in $char(R) = p \in \mathbb{P}$, potem je $\varphi : R \to R$, $\varphi(x) = x^p$ endomorfizem R.
Trditev: Razpadno polje $\mathbb{F}_{p^n}$ polinoma $f(x) = x^{p^n} - x$ nad $\mathbb{Z}_p$ ima p^n elementov.
Izrek: Za $\forall p \in \mathbb{P}$ in $\forall n \in \mathbb{N}$ $\exists$ polje s p^n elementi, ki je do izomorfizma natančno enolično določeno, ozn. s $\mathbb{F}_{p^n}$ ali $GF(p^n)$, ki ga imenujemo **Galoisovo polje** reda p^n.
Izrek: (Wedderburnov izrek) $\forall$ končen obseg je polje.
Trditev: Multiplikativna grupa končnega polja je ciklična.

Separabilne razširitve

Def: $f(x) \in F[x]$ je **separabilen** če so njegove ničle v poljubni razširitvi F enostavne. Algebraična razširitev K/F je **separabilna**, če je za $\forall a \in K$ $m_a(x)$ separabilen. Če je vsaka končna razširitev F separabilna, je F **perfektno**.
Def: Naj bo K/F razširitev polj, in L podpolje K, ki vsebuje F. Potem je L **vmesno** polje.
Izrek: Naj bo F polje in $char(F) = 0$ ter $p(x) \in F[x]$ nerazcepen. Potem so ničle $p(x)$ v poljubni razširitvi K/F enostavne.
Posledica: F polje, $char(F) = 0 \implies \forall$ algebraična razširitev F je separabilna.
Izrek: (primitivni element) $\forall$ končna razširitev polja s karakteristiko 0 je enostavna.
Trditev: Končna polja so perfektna.
Def: Normalnim separabilnim razširitvam pravimo **Galoisove razširitve**.
Trditev: Naj bodo $F \subseteq L \subseteq K$ polja:
(i) K/F končna $\implies K/L$ končna
(ii) K/F normalna $\implies K/L$ normalna
(iii) K/F separabilna $\implies K/L$ separabilna.

Galoisova grupa razširitve

Def: Naj bo K/F razširitev in $\alpha : K \to K$ avtomorfizem. Pravimo da je α F-**avtomorfizem**, če $\alpha|_F = \mathrm{id}_F$. Množico $\forall$ F-avtomorfizmov polja K imenujemo **Galoisova grupa** razširitve K/F, ozn. $\mathrm{Gal}(K/F) = \mathrm{Aut}(K/F)$.
Izrek: Naj bo F polje, $char(F) = 0$, $f(x) \in F[x] : \deg(f) > 0$ in K razpadno polje $f(x)$ nad F. Če je $\varphi : F \to F'$ izomorfizem polj in K' razpadno polje $f_\varphi(x)$ nad F', potem $\exists$ natanko $[K : F]$ izomorfizmov med K in K', ki razširjajo φ.
Trditev: Naj bo $\sigma \in \mathrm{Aut}(K/F)$, $f(x) \in F[x]$, $a \in K : a$ ničla $f(x) \implies \sigma(a)$ ničla $f(x)$.
Def: Naj bo K/F končna razširitev, $char(F) = 0$ in $H \leq \mathrm{Aut}(K/F)$. Vmesnemu polju $K^H := \{x \in K \mid \forall \sigma \in H : \sigma(x) = x\}$, pravimo **fiksno polje** od H.
Trditev: Naj bo K/F končna razširitev, $char(F) = 0$, $H \leq \mathrm{Aut}(K/F)$ in $a \in K$, ter $\{a_1, \ldots, a_m\} = \{\sigma(a) \mid \sigma \in H\}$. Potem je $p(x) = (x - a_1) \cdots (x - a_m)$ minimalni polinom a nad K^H.
Trditev: Naj bo K/F končna razširitev, $char(F) = 0$ in $H \leq \mathrm{Aut}(K/F)$. Potem $|H| = [K : K^H]$ in $[K : F] = |H| \cdot [K^H : F]$.
Izrek: Naj bo K/F končna razširitev in $char(F) = 0$. Naslednje trditve so ekvivalentne:
(i) $|\mathrm{Aut}(K/F)| = [K : F]$
(ii) $K^{\mathrm{Aut}(K/F)} = F$
(iii) K/F je normalna oz. $\forall$ nerazcepen polinom iz $F[x]$ z ničlo v K, razpade nad K
(iv) K je razpadno polje nekega nerazcepnega polinoma iz $F[x]$
(v) K je razpadno polje nekega polinoma iz $F[x]$.
Def: Končna razširitev K/F, $char(F) = 0$, je **Galoisova**, če zadošča pogojem (i)-(v) prejšnjega izreka. V tem primeru grupi $\mathrm{Aut}(K/F) =: \mathrm{Gal}(K/F)$ pravimo **Galoisova grupa** od K nad F. Če je K razpadno polje polinoma $f(x) \in F[x]$, ji pravimo tudi Galoisova grupa od $f(x)$ nad F.
Izrek: (fundamentalni izrek Galoisove teorije) Naj bo K Galoisova razširitev F, $char(F) = 0$. Naj bo $\mathcal{I}$ množica $\forall$ vmesnih polj med F in K, ter $\mathcal{G}$ množica $\forall$ podgrup $G := \mathrm{Aut}(K/F)$. Potem:
(a) $\alpha : \mathcal{G} \to \mathcal{I}$, $\alpha(H) = K^H$ je bijekcija in njen inverz je $\beta : \mathcal{I} \to \mathcal{G}$, $\beta(L) = \mathrm{Gal}(K/L)$.
(b) Če H sovpada z L, t.j. $H = \mathrm{Gal}(K/L)$ oz. $L = K^H$, potem je $|H| = [K : L]$ in $[G : H] = [L : F]$.
(c) Če H in H' sovpadata z L in L', potem $H \subseteq H' \iff L \supseteq L'$.
(d) Če H sovpada z L, potem je H podgruga edinka v $G \iff L$ je Galoisova razširitev F. V tem primeru je $G/H \cong \mathrm{Gal}(L/F)$.

Rešljivost polinomskih enačb

Def: Naj bo F polje, $f(x) \in F[x]$ je **rešljiv z radikali** nad F, če $\exists a_1, \ldots, a_m$ v neki razširitvi F, da velja:
(i) $f(x)$ razpade nad $F(a_1, \ldots, a_m)$
(ii) $\exists n_i \in \mathbb{N}$ za $i = 2, \ldots, m$ da $a_1^{n_1} \in F \wedge a_i^{n_i} \in F(a_1, \ldots, a_{i-1})$ za $i = 2, \ldots, m$.
Trditev: Naj bo F podpolje $\mathbb{C}$ in $\alpha \in F$, $n \in \mathbb{N}$. Potem je Galoisova grupa polinoma $x^n - \alpha$ rešljiva nad F.
Izrek: Naj bo F podpolje $\mathbb{C}$ in $f(x) \in F[x]$. Če je $f(x) \in F[x]$ rešljiv z radikali nad F, potem je Galoisova grupa od $f(x)$ nad F rešljiva. (Velja tudi obrat)
Trditev: Nerazcepen kvintični polinom $p(x) \in \mathbb{Q}[x]$ z natanko 3 ni-

člami ni rešljiv z radikali nad $\mathbb{Q}$.
Izrek: (Abel-Ruffinijev izrek) $\exists$ kvintični polinom v $\mathbb{Q}[x]$, ki ni rešljiv z radikali nad $\mathbb{Q}$.
Izrek: (fundamentalni izrek algebre) $\mathbb{C}$ je algebraično zaprto.

VAJE

Grupe

Def: S_n označuje simetrično grupo množice $[n]$. $\pi \in S_n$ je soda, če je produkt sodo mnogo transpozicij, ozn. $\mathrm{sgn}(\pi) = 1$, sicer je liha in $\mathrm{sgn}(\pi) = -1$.
Trditev: $(a_1 a_2 \dots a_k) = (a_1 a_k) \cdots (a_1 a_2)$.
Trditev: Naj bo $\sigma \in S_n$. Potem $\sigma \cdot (a_1 \cdots a_k) \cdot \sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_k))$.
Def: $\pi,\sigma \in S_n$ imata **enako zgradbo disjunktnih ciklov**, če sta oba produkt disjunktnih ciklov dolžin $k_1, \dots, k_s$. Permutaciji sta **konjugirani**, če $\exists \tau \in S_n : \pi = \tau\sigma\tau^{-1}$.
Trditev: Permutaciji sta konjugirani $\iff$ imata enako zgradbo disjunktnih ciklov.
Trditev: Transpozicije $(i \quad i+1)$ generirajo S_n in $(i\ j) = (i\ i+1)(i+1\ i+2) \cdots (j-1\ j) \cdots (i+1\ i+2)(i\ i+1)$.
Def: **Diedrska grupa** je $D_{2n} := \{1, r, \dots, r^{n-1}, z, rz, \dots, r^{n-1}z\}$, kjer $r^n = 1$, $z^2 = 1$ in $r^k z = z r^{n-k}$, r-rotacija, z-zrcaljenje čez os simetrije v pravilnem n-kotniku.
Trditev: $H \cup K \leq G$, potem $K \subseteq H$ ali $H \subseteq K$.
Trditev: $H_1 \leq G_1$ in $H_2 \leq G_2 \implies H_1 \times H_2 \leq G_1 \times G_2$. Obrat ne velja - diagonalna grupa.
Def: $GL_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$ je **glavna linearna grupa**, $SL_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$ pa **specialna linearna grupa**, ki je podgrupa edinka v $GL_n(\mathbb{R})$.
Trditev: $H,K \leq G$ končni, potem $|HK| = \frac{|H|\cdot|K|}{|H \cap K|}$.
Trditev: $\mathbb{Z}_n$ ima (eno samo) podgrupo reda $k \iff k \mid n$.
Trditev: Podgruda ciklične grupe je ciklična.
Trditev: G neskončna $\implies$ G ima neskončno podgrup.
Trditev: Naj bo $k \in \mathbb{Z}_n$, red(k)= $\frac{n}{\mathrm{gcd(k,n)}}$.
Trditev: $m \perp n \implies \mathbb{Z}_{\gtrdot} \times \mathbb{Z}_n$ ciklična.
Def: $U_n := \{A \in M_n(\mathbb{C}) \mid \overline{A^T} A = I\}$ je **unitarna grupa**, $SU_n := \{A \in U_n \mid \det(A) = 1\}$ pa **specialna unitarna grupa**.
Def: $\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\}$
Def: Podgrupa $N \leq G$ je **edinka**, če $\forall \varphi \in \mathrm{Inn}(G) : \varphi(N) = N$. N je **karakteristična**, če za $\forall \varphi \in \mathrm{Aut}(G) : \varphi(N) \subseteq N$.
Trditev: $Z(G)$ je karakteristična.
Trditev: $H \overset{\text{kar.}}{\leq} K$ in $K \overset{\text{kar.}}{\leq} G \implies H \overset{\text{kar.}}{\leq} G$.

Homomorfizmi

Trditev: $\varphi : G \to H$ homomorfizem, $a \in G \implies \mathrm{red}(\varphi(a)) \mid \mathrm{red}(a)$. Če φ vložitev, velja enakost.
Def: Kolobar K je enostaven, če sta edina ideala $\emptyset$ in K.
Trditev: D obseg $\implies M_n(D)$ enostaven.
Trditev: Center enostavnega kolobarja je polje.
Trditev: K_1,K_2 kolobarja, potem je $\forall$ ideal v $K_1 \times K_2$ oblike $I_1 \times I_2$, kjer I_1 ideal K_1 in I_2 ideal K_2.
Trditev: I,J ideala komutativnega kolobarja in $I + J = K$, potem $IJ = I \cap J$.
Izrek: (kitajski izrek o ostankih) Naj bodo $n_1, \dots, n_s$ tuja cela števila. Za poljubne $a_1 \dots, a_s \in \mathbb{Z}$ $\exists a \in \mathbb{Z}$, da je $\forall i \in [s] : a \equiv_{n_i} a_i$ in če $b \equiv_{n_i} a_i$ za nek i, potem $n_1 \cdots n_s \mid a - b$.

Direktne vsote

Trditev: G p-grupa, H q-grupa, $p \neq q : G,H$ ciklični $\iff G \oplus H$ ciklična.
Trditev: Končna Abelova grupa G je ciklična, če za $\forall p \in \mathbb{P} : p \mid |G| \implies G$ vsebuje natanko $p-1$ elementov reda p.
Trditev: Naj bo G končna Abelova grupa, potem $\forall m : m \mid |G| \implies G$ vsebuje podgrupo reda m.

Delovanja grup

Trditev: Naj bo $\sigma \in A_n$ in $C(\sigma)$ centralizator σ v S_n, potem:
(i) $C(\sigma) \subseteq A_n \implies \mathrm{Raz}(\sigma)$ v S_n razpade na 2 enako velika dela v A_n
(ii) $C(\sigma) \nsubseteq A_n \implies \mathrm{Raz}(\sigma)$ v S_n sovpada z $\mathrm{Raz}(\sigma)$ v A_n.
Trditev: $H \leq G \implies N(H)/C(H) \cong K \leq \mathrm{Aut}(H)$.
Trditev: Naj bo G končna in $H < G$, $[G : H] = m : |G| \nmid m! \implies G$ ni enostavna.
Trditev: Naj bo $|G| = 2m$, m liho. Potem ima G podgrupo indeksa 2 in ni enostavna.

Komutatorske in rešljive grupe

Def: Naj bo $A,B \leq G$, potem je $[A,B] := \{aba^{-1}b^{-1} \mid a \in A, b \in B\}$. Z G' ozn. **komutatorsko podgrupo** $[G,G]$.
Trditev: $G' \triangleleft G$ in G/G' Abelova.
Trditev: $H < G : H \triangleleft G \iff [H,G] < H$.
Trditev: $H \triangleleft G$ in G/H Abelova $\implies G' \leq H$.
Trditev: $|G| = p^k \implies G$ je rešljiva.

Polinomi

Trditev: Polje F končno $\iff p(x) \neq q(x) \in F[x]$, ki imata enako polinomsko funkcijo.
Trditev: Naj bo F polje in $p(x) \in F[x]$ v n različnih elementih doseže enako vrednost, potem $\deg(p(x)) \geq n$.
Trditev: $f(x) = x^n + 1$ nerazcepen nad $\mathbb{Q} \iff n = 2^k, k \geq 1$.
Trditev: Naj bodo $a_0, \dots, a_n \in \mathbb{Z}$ in $p \in \mathbb{P} : p \nmid a_n$. Če $a_n x^n + \cdots a_0$ nerazcepen nad $\mathbb{Q}$, potem je nerazcepen nad $\mathbb{Z}_p$.
Trditev: a,b,c liha $\implies ax^4 + bx + c$ nerazcepen nad $\mathbb{Q}$.
Trditev: Naj bodo $a_1, \dots, a_n \in \mathbb{Z}$ različna, potem sta $(x - a_1) \cdots (x - a_n) - 1$ in $(x - a_1)^2 \cdots (x - a_n)^2 + 1$ nerazcepna nad $\mathbb{Q}$.
Trditev: $x^p - x + 1$ je nerazcepen in separabilen nad $\mathbb{Z}_p$.

Razširitve polj

Trditev: Naj bo $[E : F] = p \in \mathbb{P}$, potem je $\forall a \in E \backslash F$ algebraičen stopnje p nad F.
Trditev: a,b algebraična nad F in $[F(a) : F] \perp [F(b) : F] \implies [F(a,b) : F] = [F(a) : F] \cdot [F(b) : F]$.
Trditev: $F(a^k, a^l) = F(a^d)$ za $d = \gcd(k,l)$.
Trditev: $a_1, \dots, a_n$ algebraični nad F, potem $[F(a_1, \dots, a_n) : F] \leq [F(a_1) : F] \cdots [F(a_n) : F]$.
Trditev: F polje in $f(x) \in F[x]$. Ničle $f(x)$ so v poljubni razširitvi F enostavne $\iff f(x)$ in $f'(x)$ tuja.
Trditev: Naj bo E/F razširitev in $char(F) = 0$, $a \in E$ je k-kratna ničla $f(x) \in F[x] \iff f(a) = f'(a) = \cdots = f^{(k)}(a) = 0$ in $f^{(k+1)}(a) \neq 0$.
Trditev: Naj bo $char(K) = 2$ in $M = K(x^2, y^2)$, potem M nima primitivnega elementa.

Razpadna polja

Trditev: Naj bo E/F razpadno polje polinoma $f(x) \in F[x]$, $\deg(f) = n$. Potem:
(i) $[E : F] \leq n!$
(ii) $f(x)$ nerazcepen $\implies n \mid [E : F]$
(ii) $E = F(a_1, \dots, a_k)$, a_i ničle in $k \leq n$.

Trditev: Naj bo F polje in $a_1, \dots, a_n \in F$, potem $\exists f(x) \in F[x] : f(a_1) = \cdots = f(a_n) = 1$.
Trditev: F je algebraično zaprto $\iff \nexists$ prava končna razširitev F.
Trditev: Naj bo $[L : K] = 2$, potem je L/K normalna.
Trditev: Naj bo $f(x) = x^4 + bx^2 + c \in \mathbb{Q}[x]$ in naj bo $G = \mathrm{Gal}_{\mathbb{Q}}(f(x))$. Potem je $G \leq D_8$. Naj bodo $\pm\alpha, \pm\beta$ ničle $f(x)$. Če $\alpha\beta$ ali $\alpha^2 \in \mathbb{Q}$, potem je $G \leq K_4$. Če $\sqrt{c(b^2 - 4c)} \in \mathbb{Q}$, potem $G \leq C_4$.
Trditev: Naj bo $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ nerazcepen in $D = ((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))^2$ diskriminanta. Če $\sqrt{D} \in \mathbb{Q}$ potem $G \cong \mathbb{Z}_3$, sicer $G \cong S_3$.
Trditev: Naj bo $f(x) \in \mathbb{Q}[x]$ nerazcepen stopnje 5 z natanko 3 realnimi ničlami, potem $\mathrm{Gal}_{\mathbb{Q}}(f(x)) \cong S_5$.
Def: Naj bo $p(x) \in \mathbb{Q}[x]$ in $\deg(p) = n$, kjer $\alpha_1, \dots, \alpha_n$ ničle $p(x)$. Potem je njegova **diskriminanta** $D_f := \prod_{i,j \in [n] \wedge i<j} (\alpha_i - \alpha_j)^2$.
Trditev: Naj bo $p(x) = ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$. Potem je $D_p = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2$.
Izrek: (Cardanova formula) Naj bo $p(x) = ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$, $a \neq 0$ nerazcepen. Naj bo $p(x) = 0$, potem z $x = t - \frac{b}{3a}$ dobimo $t^3 + pt + q = 0$, kjer $p = \frac{3ac - b^2}{3a}, q = \frac{2b^3 - 9abc + 27a^2d}{27a^3}$. Naredimo substitucijo $t = u + v$ in dobimo $u^3 + v^3 + (3uv + p)(u + v) = 0$. Izberemo $uv = -\frac{p}{3}$ in dobimo $u^3 + v^3 + q = 0$. Potem sta u^3, v^3 ničle $y^2 + qy - \frac{p^3}{27} = 0$. Naj bo $\Delta = (\frac{q}{2})^2 + (\frac{p}{3})^3$ in $u = \sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}}$, $v = \sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}$. Potem so ničle $t^3 + pt + q = 0$ enake $t_1 = u + v$, $t_2 = \omega u + \omega^2 v$ in $t_3 = \omega^2 u + \omega v$. Ničle $p(x)$ pa $x_i = t_i - \frac{b}{3a}$, kjer $\omega = e^{2\pi i/3}$.
Izrek: (Galoisova grupa polinomov 4. stopnje) Naj bo $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}[x]$ nerazcepen. Nastavimo $t = x + \frac{a_3}{4}$ v $f(x)$ in dobimo $g(t) = t^4 + pt^2 + qt + r \in \mathbb{Q}[x]$. Naj bodo $\alpha_1, \dots, \alpha_4$ ničle $g(x)$, $\Theta_1 := (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$, $\Theta_2 := (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$ in $\Theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$, potem je $R(x) := (x - \Theta_1)(x - \Theta_2)(x - \Theta_3) = x^3 - px^2 - 4rx + (4pr - q^2)$ **kubična rezindenta** in $D_g = D_R$. Velja $\mathrm{Gal}_{\mathbb{Q}}(f(x)) = \begin{cases} A_4\ ;\ \sqrt{D_R} \in \mathbb{Q} \\ S_4\ ;\ \sqrt{D_R} \notin \mathbb{Q} \end{cases}$.
Trditev: Naj bo $p \in \mathbb{P}$, $p > 2$, potem je $\mathrm{Gal}_{\mathbb{Q}}(x^p - 1) \cong C_{p-1}$.