# Snop nalog iz Algebre 2

21. januar 2014

# Kazalo

# Poglavje 1

# Grupe

## 1.1 Permutacijske grupe

**1.** Naslednje permutacije zapiši kot produkt disjunktnih ciklov.

- $(2,4)(1,3,4)(2,4)(1,3,2,4)$
- $(2,3,5)(2,5,4,3)(1,3,2,4,5)$
- $(1,5)(3,6,4)(1,6,3,5,4)(1,2,5,6,3,4)(1,5,4,3,6,2)$
- $(1,3,2,7,5)(2,3)(4,6)(1,6,2,7,3,5)$
- $(1,8,7,5)(2,3,6,4)(1,8,6,7,5)(2,4)$
- $(1,2,3,8,7)(4,5,6,9)(1,3,5,9,8)(2,7)(1,7,8,4,6)(2,3,5,9)(1,8,7,5,3)(2,4,9)$
- $(1,10,6,5)(2,7,8)(3,9,4)(2,7,3,4)(5,8,9,10,6)(1,2,9,4,10,7,8,3,6)$

**2.** Pokaži, da lahko vsako permutacijo zapišemo kot produkt transpozicij.

**3.** Dokaži, da je red permutacije enak najmanjšemu skupnemu večkratniku dolžin njenih disjunktnih ciklov.

**4.** Bodi $q=(1,2,\ldots,m)$ cikel dolžine $m$. Dokaži, da je permutacija $q^n$ cikel dolžine $m$ natanko tedaj, ko sta $m$ in $n$ tuji števili. Še več, število ciklov permutacije $q^n$ je enako največjemu skupnemu delitelju števil $m$ in $n$.

**5.** Poišči vse elemente simetrične grupe $S_n$, katerih red je enak pribitemu praštevilu $p$.

**6.** Koliko elementov reda 6 in koliko elementov reda 12 vsebuje grupa $S_6$?

**7.** V grupi $S_n$ poišči vse permutacije, ki komutirajo s ciklom $\pi=(a_1,\ldots,a_n)$.

**8.** Dokaži, da za vsako permutacijo $\pi$ in transpozicijo $\tau$ velja $\operatorname{sgn}(\pi\tau)=-\operatorname{sgn}(\pi)$. Iz zapisa permutacije $\pi$ kot produkta transpozicij $\pi=\tau_1\tau_2\cdots\tau_k$ sklepaj $\operatorname{sgn}(\pi)=(-1)^k$. Izpelji, da za poljubni permutaciji $\pi_1$, $\pi_2$ velja $\operatorname{sgn}(\pi_1\pi_2)=\operatorname{sgn}(\pi_1)\operatorname{sgn}(\pi_2)$.

**9.** Dokaži, da je vsaka permutacija $\pi\in S_{10}$ reda 20 liha.

**10.** Pokaži, da lahko vsako sodo permutacijo zapišemo kot produkt 3-ciklov.

**11.** Permutaciji $p, q \in S_n$ sta konjugirani, če in samo če ju lahko zapišemo kot produkt enakega števila disjunktnih ciklov z enakim številom ciklov fiksnih dolžin.

**12.** Dokaži, da lahko grupo $S_n$ generiramo z množico permutacij $\{(1,2),(1,3),\ldots,(1,n)\}$. Od tod sklepaj, da lahko $S_n$ generiramo s permutacijama $(1,2)$ in $(1,2,\ldots,n)$.

**13.** Določi število elementov v vsakem konjugiranostnem razredu grupe $S_n$.

## 1.2 Binarne operacije

**14.** Naj bo $X$ neprazna množica. Pokaži, da je $(\mathscr{P}(X), \cap)$ komutativen monoid, ki ni grupa. Pokaži, da $(\mathscr{P}(X), \setminus)$ ni niti polgrupa.

**15.** Razišči lastnosti naslednjih operacij na $\mathbb{C}$ (komutativnost, asociativnost, obstoj leve/desne/dvostranske enote, levih/desnih/dvostranskih inverzov).

- $a \circ b = a^2 + b^2$
- $a \circ b = ab^2$
- $a \circ b = a + b + ab$
- $a \circ b = |a|b$

**16.** Naj bo $X$ množica izjavnih simbolov. Razišči lastnosti izjavnih veznikov $\wedge, \vee, \oplus, \uparrow, \downarrow$ kot binarnih operacij na množici $X$.

**17.** Preveri lastnosti operacije kompozitum na naslednjih množicah.

- $\{f : \mathbb{R} \to \mathbb{R}\}$
- $\{f$ konst.$\}$
- $\{f$ liha$\}$
- $\{f$ strogo monotona$\}$
- $\{f$ zvezna bijekcija$\}$

**18.** Poišči leve in desne enote $(\{f : \mathbb{R} \to [0,1]\}, \circ)$.

**19.** Na realnih številih je dana operacija $x \circ y = a + bx + cy + dxy$. Za katere $a, b, c, d \in \mathbb{R}$ je operacija asociativna/komutitvna/obstajajo leve ali desne enote/je $\mathbb{R}$ grupa?

**20.** Za vsako od spodnjih struktur navedi primer.

- Monoid, ki ni grupa.
- Polgrupa, ki ni monoid.
- Množica z binarno operacijo, ki ni asociativna.

**21.** Naj bo $U = \{\left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right] \mid n \in \mathbb{Z}\}$. Pokaži, da je $U$ grupa za matrično množenje.

**22.** Dani sta množici $A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}, a^2 + b^2 \neq 0\}$ in $B = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}, a^2 + b^2 + c^2 \neq 0\}$. Pokaži, da sta $A$ in $B$ grupi za operacijo množenja števil.

## 1.3 Zgledi grup

**23.** Sestavi tabelco množenja za vse grupe moči 1, 2, 3 in 4. Oceni število vseh (*bistveno različnih*) binarnih operacij/polgrup na množici moči $n$.

**24.** Razišči naslednje grupe.

- Trivialna grupa.
- Ciklična grupa $(\mathbb{Z}_n, +)$ ali $(\mathbb{Z}, +)$. Podgrupe ciklične grupe. Red elementa. Vloga ciklične grupe v abstraktni grupi.
- Direktni produkt in direktna vsota grup. $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$, čee $\gcd(n, m) = 1$. Kleinova četverka.
- Nalaganje cikličnih grup. Prüferjeva grupa praštevilskih kompleksnih korenov enote $\mathbb{Z}_{p^\infty} = \{z \in \mathbb{C} \mid z^{p^k} = 1 \text{ za nek } k \geq 0\}$. Glej tudi $p$-adična cela števila $\mathbb{Z}_p$.
- Racionalna števila $(\mathbb{Q}, +)$. Končno generirane podgrupe. Kvocient $(\mathbb{Q}/\mathbb{Z}, +)$ kot podgrupa $S^1$. Vložitev Pruferjeve grupe v $(\mathbb{Q}/\mathbb{Z}, +)$.
- Kvaternionska grupa $Q_8$.
- Prosta grupa. Konkatenacija besed.
- Matrične grupe: GL, SL, PSL, O, SO, U nad $\mathbb{C}$. PSL$(2,5)$ premika premice v ravnini.
- Grupe iz geometrije: diedrske grupe $D_{2n}$ kot simetrije pravilnih $n$-kotnikov, simetrična grupa kot popolna simetrija, alternirajoča grupa kot popolna toga (brez zrcaljenj) simetrija. Platonska telesa.

**25.** Bodi $G$ grupa in $S$ neka njena podmnožica. *Cayleyjev graf* $\mathrm{Cay}(G, S)$ grupe $G$ glede na $S$ je usmerjen graf s pobarvanimi povezavami (barve so označene z elementi množice $S$), katerega vozlišča so natanko elementi elementi grupe $G$, od vozlišča $x$ do vozlišča $y$ pa poteka povezava barve $s$, če in samo če velja $xs = y$ (torej: desno množenje z elementom $s$ pripelje $x$ do $y$).

- Nariši Cayleyjev graf ciklične grupe, produkta dveh cikličnih grup, kvaternionske grupe.
- Nariši Cayleyjev graf diederske grupe $D_{10}$ glede na množico $\{\tau, \rho\}$. V njem označi elemente podgrupe $K = \langle \rho \rangle$ grupe $D_{10}$. Pokaži, da je $K$ edinka v $D_{10}$. V Cayleyjevem grafu označi odseke $K$ v $D_{10}$. Kateri znani grupi je izomorfen kvocient $D_{10}/K$?
- Opiši Cayleyjev graf Pruferjeve grupe $\mathbb{Z}_{p^\infty}$ glede na množico $\{e^{2\pi i/p^k} \mid k \geq 0\}$.

## 1.4 Zgradba abstraktne grupe

**26.** Naj bo $G$ grupa, v kateri velja $x^2 = 1$ za vsak $x \in G$. Pokaži, da je $G$ komutativna. Navedi primer grupe $G$, v kateri velja $x^3 = 1$ za vsak $x \in G$, a $G$ ni komutativna.

**27.** Naj bo $G$ grupa sode moči. Pokaži, da v $G$ obstaja element reda 2.

**28.** Naj bosta $m$ in $n$ tuji števili in $G$ grupa moči $n$. Pokaži, da za vsak $y \in G$ obstaja natanko en tak $x \in G$, da je $x^m = y$.

**29.** Naj bosta $r$ in $s$ tuji števili in $x \in G$ element reda $rs$. Pokaži, da obstajata enolično določena elementa $y, z \in G$ redov $\text{red}(y) = r$ in $\text{red}(z) = s$, za katera velja $yz = zy = x$.

**30.** Razišči pomembne podmnožice grupe $G$. Kako so povezane z zgradbo grupe $G$? Kdaj so te podmnožice tudi podgrupe? Določi te podmnožice za primer $G = S_n$.

- Center $Z(G) = \{x \in G \mid [x, g] = 1 \forall g \in G\}$
- Izpeljana pogrupa $[G, G] = \{[x, y] \mid x, y \in G\}$
- Torzija $T(G) = \{x \in G \mid \text{red}(x) < \infty\}$
- Ciklična podgrupa $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$

**31.** Naj bo $G$ grupa in $H$ podgrupa praštevilskega indeksa. Pokaži, da je $H$ maksimalna podgrupa. Navedi primer grupe in njene maksimalne podgrupe, ki ni praštevilskega indeksa.

**32.** Naj bo $G$ grupa in $H, K$ podgrupi končnega indeksa v $G$. Pokaži, da drži ocena $|G : H \cap K| \leq |G : H||G : K|$. Kdaj velja enakost?

**33.** Naj bo $G$ grupa in $H, K$ njeni podgrupi. Pokaži, da je $H \cup K$ podgrupa grupe $G$, če in samo če je $H \subseteq K$ ali $K \subseteq H$. Pokaži, da je $HK$ podgrupa, če in samo če je $HK = KH$.

**34.** Dokaži, da grupi $(\mathbb{Q}, +)$ in $(\mathbb{Z}_{p^\infty}, \cdot)$ nista končno generirani.

**35.** Pokaži, da je vsaka neskončna končno (celo: števno) generirana grupa števna.

## 1.5 Podgrupe edinke, kvocienti in homomorfizmi

**36.** Naj bo $G$ grupa. Pokaži, da so podgrupe $Z(G)$, $[G, G]$, $\langle g \mid \text{red}(g) < \infty \rangle$ edinke v $G$. Kaj lahko poveš o pripadajočih kvocientnih grupah?

**37.** Naj bo $G$ grupa in $G/Z(G)$ ciklična grupa. Pokaži, da je $G$ abelova.

**38.** Sestavi homomorfizem iz grupe afinih transformacij v splošno linearno grupo. Kaj je njegovo jedro?

**39.** Poišči podgrupe edinke diedrske grupe $D_8$, kvaternionske grupe $Q_8$ in simetrične grupe $S_3$. Kaj so pripadajoči kvocienti?

**40.**

- Naj bo $G = (M_2(\mathbb{Z}), +)$ in $H = \{A \in G \mid \text{sled}(A) = 0\}$. Pokaži, da je $H \lhd G$ in $G/H \cong \mathbb{Z}$.
- Naj bo $G = \text{GL}_n(\mathbb{R})$ in $H = \text{SL}_n(\mathbb{R})$. Pokaži, da je $H \lhd G$ in $G/H \cong \mathbb{R}^*$.

**41.** Pokaži, da je vsaka podgrupa indeksa 2 edinka.

**42.** Naj bo $G$ grupa in $H, K$ podgrupi. Pokaži, da je $HK$ podgrupa v $G$, če je vsaj ena od podgrup $H, K$ edinka v $G$. Kadar sta edinki obe, je tudi $HK$ edinka.

**43.** Naj bo $G$ grupa in $H$ njena podgrupa edinka, katere moč je tuja njenemu indeksu. Dokaži, da je $H$ edina podgrupa grupe $G$ moči $|H|$.

**44.** Naj bo $G$ grupa, $H$ abelova grupa in $f: G \to H$ homomorfizem grup. Nadalje naj bo $N$ neka podgrupa grupe $G$, ki vsebuje jedro preslikave $f$. Pokaži, da je $N$ podgrupa edinka.

**45.** Poišči vse grupe, ki so izomorfne vsaki svoji netrivialni podgrupi.

**46.** Pokaži, da se da vsako končno grupo vložiti v alternirajočo grupo. Konkretno, vloži $V$ v $A_6$.

**47.** Navedi primer grupe $G$ v kateri najdeš podgrupi $H$ in $K$ z lastnostjo $H \lhd G$ in $K \lhd H$, toda $K \not\lhd G$.

**48.** Naj bo $G$ taka podgrupa simetrične grupe $S_n$, da vsebuje neko liho permutacijo. Pokaži, da obstaja v $G$ podgrupa edinka indeksa 2.

## 1.6 Rešljivost

**49.** Za vsako končno grupo $G$ obstaja zaporedje podgrup $1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 = G$ z enostavnimi kvocienti $G_i/G_{i+1}$. Takemu zaporedju pravimo *dekompozicijska vrsta*. Torej lahko vsako končno grupo sestavimo z zaporednimi razširitvami z enostavnimi grupami. Kadar lahko grupo $G$ sestavimo z zaporednimi razširitvami s cikličnimi grupami, je $G$ *policiklična*. Splošneje je poljubna grupa *rešljiva*, kadar ima vrsto $1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 = G$ z abelovimi faktorji.

**50.** Končne enostavne grupe.

**51.** Bodi $n \geq 5$. V tej nalogi korakoma pokažeš, da je $A_n$ enostavna grupa.

- Pokaži, da lahko $A_n$ generiraš s 3-cikli.
- Pokaži, da za vsak 3-cikel $\pi$ obstaja element $\rho \in A_n$, da velja $\pi^\rho = (1,2,3)$. Sklepaj, da sta vsaka dva 3-cikla v $A_n$ konjugirana.
- Naj bo $n = 5$. Predpostavi, da je $N$ netrivialna edinka v $A_5$. Pokaži, da $N$ vsebuje 3-cikel, in sklepaj $N = A_5$.
- Naj bo $n > 5$. Predpostavi, da je $N$ netrivialna edinka v $A_n$. Pokaži, da obstaja element v $N$, ki fiksira vsaj $n-5$ točk.
- Sklepaj, da je $A_n$ enostavna.

S pomočjo dokazanega poišči vse podgrupe edinke simetrične grupe $S_n$.

**52.** Naj bo $F$ polje z več kot tremi elementi (končno ali neskončno) in $SL_2(F)$ grupa $2 \times 2$ matrik nad $F$ z determinanto 1. V tej nalogi korakoma pokažeš, da je kvocientna grupa $\mathrm{PSL}_2(F) = \mathrm{SL}_2(F)/\left\{ \left[\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right] \mid a^2 = 1 \right\}$ enostavna.

- Pokaži, da zadošča dokazati, da je vsaka podgrupa edinka v $\mathrm{SL}_2(F)$, ki vsebuje kakšno ne-skalarno matriko, nujno enaka $\mathrm{SL}_2(F)$.
- Privzemimo, da je $N$ podgrupa edinka v $\mathrm{SL}_2(F)$, ki vsebuje kakšno ne-skalarno matriko. Pokaži, da tedaj $N$ vsebuje matriko oblike $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ z $b \neq 0$.

  *Nasvet: za dano matriko $A$ izračunaj $XAX^{-1}$, kjer je $X = \left[\begin{smallmatrix} 1 & e \\ 0 & 1 \end{smallmatrix}\right]$ in $e \in F$.*

- Označimo
$$L=\left\{\begin{bmatrix}1 & 0\\ c & 1\end{bmatrix} \mid a\in F\right\} \quad \text{in} \quad U=\left\{\begin{bmatrix}1 & b\\ 0 & 1\end{bmatrix} \mid b\in F\right\}.$$
Pokaži, da sta $L$ in $U$ podgrupi v $\mathrm{SL}_2(F)$.
- Pokaži $LN = NL = \mathrm{SL}_2(F)$.
- Pokaži $L \leq N$.
- Pokaži $U \leq N$.
- Pokaži $N = \mathrm{SL}_2(F)$.

**53.** Pokaži, da je končna grupa rešljiva, če in samo če je policiklična.

**54.** Poišči dekompozicijo abelove grupe $\mathbb{Z}_{10} \times \mathbb{Z}_{100} \times \mathbb{Z}_{15} \times \mathbb{Z}_{12}$. Poišči vrsto, ki opazi njeno policikličnost.

**55.** Poišči vse abelove grupe moči 81.

**56.** Za dano grupo $G$ definiramo $[G,G] = \langle [x,y] \mid x,y \in G\rangle$, to je *izpeljana podgrupa* grupe $G$. Pokaži, da je $[G,G]$ edinka v $G$ in da je kvocient $G/[G,G]$ abelova grupa.

**57.** Naj bo $G$ grupa in $N$ njena podgrupa edinka. Pokaži, da je kvocient $G/N$ abelova grupa, če in samo če je $N \geq [G,G]$.

**58.** Za dano grupo $G$ induktivno definiramo zaporedje podgrup $G^{(1)} = G$ in $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$. Pokaži, da je grupa $G$ rešljiva, če in samo če za nek $n$ velja $G^{(n)} = 1$. Torej obstaja kanoničen način za preverjanje rešljivosti.

**59.** Za vsako od spodnjih grup določi najmanjši $k$, pri katerem je $k$-ta izpeljana podgrupa trivialna.

- $\mathbb{Z}$
- $S_3$ in $S_4$
- $D_{2n}$
- $\{\left[\begin{smallmatrix} a & b\\ 0 & d\end{smallmatrix}\right] \mid a,d \in F^*, b \in F\}$

**60.** Pokaži, da simetrična grupa $S_n$ ni rešljiva za $n \geq 5$.

**61.** Pokaži, da je podgrupa rešljive grupe sama rešljiva. Pokaži, da je kvocient rešljive grupe sam rešljiv. Pokaži, da je razširitev rešljive grupe z rešljivo grupo sama rešljiva.

**62.** Pokaži, da je center vsake končne $p$-grupe netrivialen. S pomočjo tega pokaži, da je vsaka končna $p$-grupa rešljiva.

**63.** Poišči podatek o številu grup moči $2^n$ za $n \leq 10$ in o številu grup moči največ 2013. Kako bi jih sam preštel?

**64.** Pokaži, da je vsaka grupa moči $pq$, kjer sta $p$ in $q$ praštevili, rešljiva.

**65.** Pokaži, da je vsaka grupa moči $pqr$, kjer so $p, q, r$ praštevila, rešljiva.

**66.**

- Pokaži, da je vsaka grupa moči 585 rešljiva.
- Pokaži, da je vsaka grupa moči 80 rešljiva.
- Pokaži, da je vsaka grupa moči 36 rešljiva.

**67.** Pokaži, da je vsaka grupa moči $p^2$ abelova.

**68.** Pokaži, da je vsaka grupa moči 77 ciklična.

**69.** Poišči $p$-podgrupo Sylowa grupe $\mathrm{GL}_n(\mathbb{Z}_p)$.

**70.** Poišči vse podgrupe Sylowa v $A_5$.

**71.** Pokaži, da grupe $Q_8$ ni mogoče vložiti v $S_5$.

**72.** Pokaži, da je vsaka grupa moči $< 60$ rešljiva.

## 1.7 Delovanja

**73.** Razišči naslednja delovanja.

- Simetrična grupa $S_n$ deluje na množici $\{1, 2, \ldots, n\}$.
- Simetrična grupa $S_4$ deluje na vozliščih/licih/povezvah tetraedra. Alternirajoča grupa $A_5$ deluje na vozliščih/licih/povezavah ikozaedra. Simetrična grupa geometrijskega objekta deluje na njem.
- Simetrična grupa $S_n$ deluje na množici polinomov $\mathbb{C}[x_1, x_2, \ldots, x_n]$.
- $\mathrm{GL}_n(\mathbb{R}), \mathrm{SL}_n(\mathbb{R}), \mathrm{O}_n(\mathbb{R})$ deluje na vektorskem prostoru $\mathbb{R}^n$. Orbite delovanja $\mathrm{O}_2(\mathbb{R})$ na $\mathbb{R}^2$. Stabilizator vektorja pri delovanju $\mathrm{GL}_n(\mathbb{R})$. Delovanje $\mathrm{GL}_n(\mathbb{R})$ na podprostorih $\mathbb{R}^n$. Delovanje $\mathrm{PSL}_2(p)$ na premicah ravnine $\mathbb{Z}_p^2$.
- Grupa afinih transformacij prostora $\mathrm{AGL}_n(\mathbb{R}) = \{T_{A,b} \colon x \mapsto Ax + b \mid A \in \mathrm{GL}_n(\mathbb{R}), b \in \mathbb{R}^n\}$. Translacije kot jedro homomorfizma $\mathrm{AGL}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$. Evklidska grupa.
- Kvaternionska grupa deluje na $\mathbb{R}^3$.
- Tri delovanja grupe $\mathbb{R}$ na torusu $S^1 \times S^1$. Prvo $t : (e^{ix}, e^{iy}) \mapsto (e^{i(x+t)}, e^{iy})$, drugo $t : (e^{ix}, e^{iy}) \mapsto (e^{i(x+t)}, e^{i(y+t)})$, tretje $t : (e^{ix}, e^{iy}) \mapsto (e^{i(x+t)}, e^{i(y+t\sqrt{2})})$. Orbite delovanj.
- Trivialno delovanje grupe $G$ na kateri koli množici $X$.
- Delovanje grupe $G$ na sebi z levim množenjem.
- Delovanje grupe $G$ na pripadajočem Cayleyjevem grafu.
- Delovanje grupe $G$ na sebi s konjugiranjem.
- Delovanje grupe $G$ na odsekih podgrupe $H$.

- Delovanje grupe $G$ na množici vseh $p$-podgrup Sylowa s konjugiranjem.

**74.** Naj bo $G$ končna enostavna grupa in $H$ neka njena prava podgrupa indeksa $n$. Pokaži, da moč grupe $G$ deli $n!$.

**75.** Naj bo $G$ grupa moči $p^n r$, kjer je $p$ praštevilo, $n \geq 1$, $r \geq 2$, $p$ ne deli $r$ in $p^n$ ne deli $(r-1)!$. Pokaži, $G$ ni enostavna.

# Poglavje 2

# Kolobarji

## 2.1 Zgledi kolobarjev

**76.** Razišči naslednje kolobarje.

- 0.
- Številski kolobarji. $\mathbb{Z}, 2\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ in še kaj. Ne-primer: $\mathbb{N}, 2\mathbb{Z}+1$.
- Ostanki $\mathbb{Z}_n$. Ta je obseg, čee je $n$ praštevilo. Delitelji niča v $\mathbb{Z}_n$.
- Gaussova števila $\mathbb{Z}[i]$. Eisensteinova števila $\mathbb{Z}[e^{2\pi i/3}]$. Kummerjev kolobar $\mathbb{Z}[\zeta]$. Nariši elemente Kummerjevega kolobarja za $\zeta \in \{e^{2\pi i/k} \mid k \in \{2,3,4,5\}\}$ in premisli, kako se množijo in seštevajo.
- Polinomi $R[X]$. Razcepnost nad $\mathbb{Z}_p[X]$. Potenčne vrste $R[[X]]$.
- Zvezne realne funkcije glede na kompozitum. Integrabilne zvezne s kompaktno podporo glede na konvolutivno množenje (ni enote).
- Matrike $\mathrm{M}_n(F)$. Matrike nad kolobarjem (npr. matrike nad matrikami). Delitelji niča, nilpotenti, idempotenti (Jordanova kanonična forma, minimalni polinom). Podgrupa obrnljivih matrik $\mathrm{GL}_n(F)$. Podkolobar zgornje trikotnih matrik. Matrike z ničelnim stolpcem ali vrstico. Matrike z eno samo neničelno vrstico ali stolpcem.
- Direktni produkti kolobarjev. Končni enostavni kolobarji so izomorfni $\mathrm{M}_n(F)$ za končno polje $F$.
- Abelova grupa s trivialnim množenjem. Endomorfizmi abelove grupe. Konkretno za $\mathbb{Z}_n$, $\mathbb{Z}$, proste abelove grupe, $\mathbb{Q}$.
- Grupa enot kolobarja.
- Potenčna množica $\mathscr{P}(X)$. Boolov kolobar (vsi elementi so idempotenti).

**77.** Naj bo $G$ grupa in $R$ komutativen kolobar. Na množico $RG = \{\sum_{i=1}^{n} r_i g_i \mid n \in \mathbb{N}_0,\ r_i \in R,\ g_i \in G\}$ vseh končnih kombinacij elementov grupe $G$ s koeficienti v kolobarju $R$ vpeljemo operaciji seštevanja in množenja po predpisu

$$(\textstyle\sum_{i=1}^{n} r_i g_i) + (\sum_{j=1}^{m} s_j h_j) := \sum_{i=1}^{n} r_i g_i + \sum_{j=1}^{m} s_j h_j$$
$$(\textstyle\sum_{i=1}^{n} r_i g_i) \cdot (\sum_{j=1}^{m} s_j h_j) := \sum_{i,j} (r_i s_j)(g_i h_j).$$

Dobljeni kolobar je *grupni kolobar* grupe $G$ s koeficienti v $R$.

- Pokaži, da je $RG$ zares kolobar.
- Ko je $R$ polje, je $RG$ vektorski prostor.
- Posebni primer sta Kummerjev kolobar $\mathbb{Z}[\zeta]$ in Laurentovi polinomi $\mathbb{C}[\mathbb{Z}]$.

**78.** Pozitivna realna števila $\mathbb{R}_+$ opremimo z operacijama $x \oplus y = xy$ in $x \otimes y = x^{\log y}$. Pokaži, da je $(\mathbb{R}_+, \oplus, \otimes)$ komutativen kolobar.

**79.** Naj bo $M$ množica vseh naravnih števil, ki se dajo zapisati kot produkt samih različnih praštevil (pazi: število 1 pripada $M$, ker ga lahko zapišemo kot prazen produkt). Uvedimo v $M$ dve operaciji: $a \oplus b$ naj bo število, ki ga dobimo, če v produktu $ab$ izpustimo vse prafaktorje, ki nastopajo dvakrat; $a \otimes b = \gcd\{a, b\}$. Pokaži, da je $(M, \oplus, \otimes)$ komutativen kolobar.

**80.** Pokaži, da Pruferjeve grupe ni mogoče opremiti z množenjem, s katerim bi postala kolobar z enoto.

**81.** Naj bo $K$ kolobar števil $\{a+bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ za običajno seštevanje in množenje. Definirajmo normo $N(a+bi\sqrt{5}) = a^2+5b^2$. Najprej pokaži, da velja $N(xy) = N(x)N(y)$ za vsaka $x, y \in K$, nato pa s pomočjo tega poišči vse obrnljive elemente kolobarja $K$.

## 2.2 Zgradba abstraktnega kolobarja

**82.** Pokaži, da je v komutativnem kolobarju vsota dveh nilpotentov zopet nilpotent.

**83.** Pokaži, da je kolobar $R$ komutativen, če in samo če za vsaka $a, b \in R$ velja $(a+b)^2 = a^2+2ab+b^2$.

**84.** Pokaži, da je vsak Boolov kolobar komutativen karakteristike 2.

**85.** Naj bo $R$ kolobar, v katerem za vsak element $x$ velja $x^3 = x$. Pokaži, da je $R$ komutativen.

**86.** Pokaži, da je v vsakem komutativnem kolobarju $R$ vsota obrnljivega elementa in nilpotenta obrnljiv element. Poišči primer nekomutativnega kolobarja, ko to ne velja.

**87.** Naj bo $G$ končna grupa in $F$ poljubno polje. Pokaži, da ima grupni kolobar $FG$ veliko netrivialnih deliteljev niča.

**88.** † Naj bo $G$ grupa brez elementov končnega reda in $F$ poljubno polje. Ali ima grupni kolobar $FG$ kakšen netrivialen delitelj niča?

## 2.3 Ideali, kvocienti in homomorfizmi

**89.** Poišči vse unitalne kolobarje, v katerih je vsaka aditivna podgrupa ideal.

**90.** Pokaži, da je vsak ideal v $\mathbb{Z}$ generiran z enim elementom. Poišči kolobar in ideal, ki ga ni mogoče generirati z enim elementom.

**91.** Pokaži, da je $\langle 2, X \rangle$ maksimalen ideal v $\mathbb{Z}[X]$. Določi kvocientni kolobar.

**92.** Množico $\{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \text{ liho }\}$ opremimo z običajnima operacijama seštevanja in množenja. Pokaži, da dobimo kolobar, v katerem je $(2)$ maksimalen ideal.

**93.** Pokaži, da je vsak komutativen kolobar z enico, v katerem je vsak pravi ideal praideal, nujno obseg.

**94.** Pokaži, da množica matrik $\{\left[\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right] \mid a, b, c \in R\}$ tvori podkolobar v $\mathrm{M}_n(R)$. Pokaži, da je $\{\left[\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right] \mid a, b \in R\}$ njegov ideal. Poišči kvocienti kolobar.

**95.** Pokaži, da je vsak ideal kolobarja $\mathrm{M}_n(R)$ oblike $\mathrm{M}_n(I)$ za nek ideal $I$ kolobarja $R$.

**96.** Pokaži, da grupni kolobar $F[G]$, kjer je $G$ končna grupa, nikoli ni enostaven.

**97.** Poišči obsege ulomkov naslednjih kolobarjev.

- $\mathbb{Z}$, $2\mathbb{Z}$
- $F$, $F[X]$, $F[[X]]$
- $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$

## 2.4 Polinomi

**98.** Koliko je nerazcepnih kvadratnih polinomov v $\mathbb{Z}_p[X]$?

**99.** Pokaži, da je Kummerjev kolobar $\mathbb{Z}[\zeta]$, določen s polinomom $p_\zeta(X)$, izomorfen kvocientnemu kolobarju $\mathbb{Z}[X]/\langle p_\zeta(X)\rangle$.

**100.** Pokaži, da je Kummerjev kolobar $F[\zeta]$ polje, če in samo če je $p_\zeta$ nerazcepen polinom.

**101.** Pokaži, da je kolobar $\mathbb{R}[X]/(X^2-2x+2)$ izomorfen $\mathbb{C}$.

**102.** Naj bo $R$ komutativen kolobar. Poišči obrnljive elemente kolobarja $R[X]$.

**103.** Poišči vse elemente $a \in \mathbb{Z}_3$, za katere je $\mathbb{Z}_3[X]/(X^3+X^2+aX+1)$ obseg.

**104.** Pokaži, da so praideali v $\mathbb{Z}[X]$ oblike: $\langle 0\rangle$, $\langle f\rangle$ ($f$ je nerazcepen v $\mathbb{Z}[X]$), $\langle p\rangle$ ($p$ je praštevilo), $\langle p, f\rangle$ ($p$ je praštevilo, $f$ je nerazcepen mod $p$). Nariši sliko.

**105.** Kateri kvocientni kolobarji $\mathbb{Z}[\sqrt{3}]$ so polja?

**106.** Algoritem deljenja. Izvedi ga na paru polinomov $X^5+2X^4-X+1$ in $X^2+X$ v $\mathbb{C}[X]$ in $\mathbb{Z}_4[X]$. V obeh primerih poišči njun največji skupni delitelj.

**107.** Naj bo $I=(x+2y-1)$ v $\mathbb{R}[x,y]$. Ali je $I$ praideal? Ali je $I$ maksimalni ideal?

**108.** Preverjanje nerazcepnosti v $\mathbb{Z}[X]$.

- Eisensteinov kriterij. Obstaja praštevilo $p$, ki ne deli $a_n$, deli vse ostale koeficiente in $p^2$ ne deli $a_0$.
- Racionalne ničle. Če je $p/q$ ničla, potem $p$ deli $a_0$ in $q$ deli $a_n$.

- Spremeni koeficiente v $\mathbb{Z}/p\mathbb{Z}$. Če je polinom v sliki nerazcepen, je tudi v originalu. (Obratno ni res, glej $X^4+1$, ki je razcepen mod $p$ za vsa praštevila, ampak nerazcepen nad $\mathbb{Z}$ (Eisenstein na $X+1$).)

**109.** Ali je polinom $X^4-15X^3+7$ razcepen nad $\mathbb{Q}$?

**110.** Naj bo $p$ praštevilo in $n \geq 2$. Pokaži, da je $X^n+pX+p^2$ nerazcepen v $\mathbb{Z}[X]$.

**111.** Naj bo $p$ praštevilo. Pokaži, da je polinom $\sum_{i=0}^{p-1} X^i \in \mathbb{Q}[X]$ nerazcepen.

**112.** Poišči kakšen polinom v $\mathbb{Z}[X]$, ki se mod 2 reducira v $X$ in mod 3 v $-X^3+X+1$. Nato upoštevaj še, da se mod 5 reducira v polinom $X^4+3X^3+X^2+X+1$.

**113.** Dokaži Wilsonov izrek: Naravno število $n$ je praštevilo, čee je $(n-1)! \equiv -1 \bmod n$.

**114.** Nekomutativni polinomi. $F\langle X,Y\rangle$. Komutator $[X,Y]=XY-YX$. Kvocient $F\langle X,Y\rangle/([X,Y]) \cong F[X,Y]$.

**115.** Simetrična grupa $S_n$ deluje na kolobarju $\mathbb{C}[X_1,X_2,\cdots,X_n]$ po predpisu $\pi(P(X_1,\ldots,X_n))=P(X_{\pi(1)},\ldots,X_{\pi(n)})$. Poišči algebraično neodvisne generatorje množice fiksnih točk tega delovanja.

## 2.5 Gaussova cela števila

**116.** Dokaži, da je kolobar Gaussovih celih števil glavni kolobar.

**117.** Poišči obrnljive elemente v $\mathbb{Z}[i]$.

**118.** V tej nalogi raziščeš Gaussova praštevila.

- Konjugat nerazcepnega števila je nerazcepno število.
- Nerazcepno Gaussovo število je praštevilo ali pa je kvadrat njegove norme praštevilo.
- 2 je razcepno število.
- Praštevila, kongruentna 3 mod 4, so nerazcepna Gaussova števila.
- Nerazcepna Gaussova praštevila so natanko praštevila, kongruentna 3 mod 4.

**119.** † Ali za kakšen par različnih praštevil $p,q$ število $(p^q-1)/(p-1)$ deli $(q^p-1)/(q-1)$?

# Nasveti

**1.**

- $(2,4)(1,3,4)(2,4)(1,3,2,4) = (1,2,3,4)$
- $(2,3,5)(2,5,4,3)(1,3,2,4,5) = (1,3,5)(2,4)$
- $(1,5)(3,6,4)(1,6,3,5,4)(1,2,5,6,3,4)(1,5,4,3,6,2) = (1,5,6)(2,4)$
- $(1,3,2,7,5)(2,3)(4,6)(1,6,2,7,3,5) = (1,7)(2,3,5,6,4)$
- $(1,8,7,5)(2,3,6,4)(1,8,6,7,5)(2,4) = (1,6,2,3,7)(5,8)$
- $(1,2,3,8,7)(4,5,6,9)(1,3,5,9,8)(2,7)(1,7,8,4,6)(2,3,5,9)(1,8,7,5,3)(2,4,9) = (1,7,3,5,8)(6,9)$
- $(1,10,6,5)(2,7,8)(3,9,4)(2,7,3,4)(5,8,9,10,6)(1,2,9,4,10,7,8,3,6) = (2,6,3,7,4,10,5)$

**2.** Pokaži, da velja $(a_1, a_2, \ldots, a_n) = (a_1, a_2)(a_1, a_3)\cdots(a_1 a_n)$.

**3.** Disjunktni cikli komutirajo.

**4.** Opazuj orbito točke 1 oziroma orbite točk $\lambda d + 1$ za $\lambda \in \mathbb{N}$.

**5.** Permutacijo razbijemo na disjunktne cikle. Vsak od teh mora biti reda $p$.

**6.** Disjunktni cikli.

**7.** Naj permutacija $\theta$ komutira s $\pi$. Če je $q(a_1) = a_\ell$, tedaj velja $\theta(a_k) = a_{\ell+k-1}$. Od tod sledi $q = p^m$.

**8.** Štej inverzije.

**9.** Permutacijo $\pi$ zapišemo kot produkt disjunktnih ciklov. Ta zapis mora vsebovati natanko en cikel reda 5, 4 in 1.

**10.** Opazuj cikle lihe dolžine. Vsakega lahko zapišeš kot produkt dveh ciklov lihe dolžine z natanko enim skupnim simbolom.

**11.** Ugotovi, kaj je konjugacija v $S_n$. Po tem lahko za dani permutaciji eksplicitno podaš element, ki konjugira prvo permutacijo v drugo.

**12.** Pokaži $(a,b) = (a,1)(1,b)(1,a)$. Nato opazuj konjugiranja.

**13.** Disjunktni cikli.

**14.** Poišči množico, ki nima inverza.

**20.** $(\mathbb{N}_0,+)$, $(\mathbb{N},+)$, $(\mathbb{R}^3,\times)$.

**21.** Računaj.

**22.** Rečunaj.

**23.** Število vseh binarnih sistemov je $n^{n^2}$. Izomorfizem je permutacija, zato je število bistveno različnih binarnih operacij vsaj $n^{n^2-n}$. Isto oceno lahko uporabimo za zgornjo mejo za število polgrup in latinskih kvadratov. Za spodnjo mejo za število polgrup opazujemo pri pribitem $m$ operacije na množici $\mathbb{Z}_n$ z lastnostjo $i \circ j = 0$ za $i < m$ ali $j < m$. Za to operacijo velja asociativnost, vseh teh operacij pa je vsaj $m^{(n-m)^2}$. (Tu bi morali še, kot prej, deliti z $n!$, a kot prej to ne vpliva na red rezultata.) Postavimo $m \approx n^{1-\frac{1}{2}\varepsilon}$ in dobimo spodnjo mejo $n^{(1-\varepsilon)n^2}$. Mimogrede, število vseh grup je navzgor omejeno s funkcijo

$$n^{\frac{2}{27}\mu(n)^2+O(\mu(n)^{\frac{5}{3}})},$$

kjer je $\mu(n)$ najvišji eksponent, ki se pojavi v praštevilski faktorizaciji števila $n$.

**25.** Obišči Povezave na spletni učilnici. Pri drugem delu je kvocient izomorfen $\mathbb{Z}_2$.

**26.** Velja $xy = x^{-1}y^{-1} = (yx)^{-1} = yx$. Opazuj zgornje trikotne matrike reda 3 z enicami po diagonali.

**27.** Privzemi, da takega elementa ni. Grupa $G\backslash\{1\}$ razpade na kose $\{x,x^{-1}\}$ za $x \in G$.

**28.** Razširjeni Evklidov algoritem.

**29.** Razširjeni Evklidov algoritem.

**30.** Primer grupe, ko torzija ni podgrupa, je neskončna diedrska grupa.

**31.** Lagrangeov izrek. Za primer opazuj $A_5$ in podgrupo $\langle(1,2,3),(1,2)(4,5)\rangle$.

**32.** Velja $|G : H \cap K| = |G : H||H : H \cap K| \leq |G : H||G : K|$. Enakost velja, če in samo če je $G = HK$.

**33.** Izberi elementa $a \in H\backslash K$ in $b \in K\backslash H$ ter si oglej njun produkt.

**34.** Obe grupi predstavi kot neskončno unijo nekih njenih podgrup. V končno generirani grupi ni neskončnih naraščajočih verig podgrup.

**35.** Števna unija števnih množic je števna.

**36.** Računaj. $G/[G,G]$ je največji abelov kvocient $G$. Kvocient po podgrupi, generirani s torzijo, je brez torzije.

**37.** Računaj komutator.

**39.** V $D_8$ najdemo trivialni edinki, center moči 2, dve Kleinovi četverki in eno ciklično podgrupo edinko moči 4. V $Q_8$ je vsaka podgrupa edinka. Poleg trivialnih podgrup imamo center moči 2 in tri ciklične podgrupe edinke moči 4. V $S_3$ so podgrupe edinke le trivialni in $A_3$.

**40.** Po sledi sestavi homomorfizem z jedrom $H$.

**41.** Opazuj leve in desne odseke po tej podgrupi.

**42.** Računaj.

**43.** Opazuj naravni epimorfizem $G \to G/H$.

**44.** Korespondenčni izrek.

**45.** Opazuj ciklične podgrupe.

**46.** Najprej vloži v simetrično grupo.

**47.** Išči v simetrični grupi.

**48.** Po predznaku sestavi homomorfizem.

**50.** Obišči Povezave na spletni učilnici.

**51.**

- Dovolj je dokazati, da je lahko vsak produkt dveh transpozicij zapišeš kot produkt 3-ciklov. Obravnavaj dve možnosti: bodisi transpoziciji premakneta skupno točko bodisi ne.
- Gotovo obstaja $\rho' \in S_n$, da velja $\pi^{\rho'} = (1,2,3)$. Če je $\rho' \in A_n$, konec. Sicer opazuj $(4,5)\rho'$.
- Vzemi poljubno netrivialno permutacijo $\sigma \in N$ in jo zapiši kot disjunkten produkt ciklov. Loči 3 možnosti. Izberi 3-cikel $\delta$ in opazuj $[\delta,\sigma] = \delta^{-1}(\delta^{\sigma})$.
- Vzemi poljubno netrivialno permutacijo $\sigma \in N$. Izberi 3-cikel $\delta$ in opazuj $[\delta,\sigma] = \delta^{-1}(\delta^{\sigma})$. Ob ustrezni izbiri $\delta$ je $[\delta,\sigma]$ permuacija v $N$, ki premika največ 5 točk.
- Element iz prejšnje točke je v podgrupi, izomorfni $A_5$. Po predprejšnji točki zato $N$ vsebuje vse elemente te podgrupe. V posebnem vsebuje vsaj en 3-cikel. Zaključi.

Edine edinke v $S_n$ so 1, $A_n$ in $S_n$ (za edinko $N$ opazuj $N \cap A_n$).

**52.**

- Korespondenčni izrek.
- Če je ne, imajo vse matrike v $N$ na mestu $1-2$ element 0. Ker je $N$ edinka v $\mathrm{SL}_2(F)$, konjugiraš poljubno matriko v $N$ in sklepaš, da mora imeti 0 na mestu $2-1$. Torej je vsaka matrika v $N$ diagonalna. Ko tako matriko zopet konjugiraš, vidiš, da mora biti skalarna.
- Računaj.
- Ker je $N$ edinka, velja $LN = NL$. Vzemi matriko $A$ iz druge točke in opazuj, kaj pomeni množenje z leve in desne z elementi iz $L$. Sklepaj, da $LN$ vsebuje $L$ in $U$, in je zato enaka $\mathrm{SL}_2(F)$.
- Izberi $a \neq -1,0,1$ v $F$ in si oglej matriko $A = \left[\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right]$. Upoštevaj $\mathrm{SL}_2(F) = LN$ in zapiši $A = XY$, kjer je $X \in L$ in $Y \in N$. Potem izračunaj komutator $[Z,Y]$ za poljuben $Z \in L$ in zaključi $L \leq N$.
- Ker $L \leq N$ in ker lahko konjugiramo $L$ do $U$, je res tudi $U \leq N$.

- Podgrupi $L$ in $U$ generirata ves $\mathrm{SL}_2(F)$.

**53.** Opazuj najdaljšo vrsto, ki opazi rešljivost dane grupe.

**54.** Korakoma po direktnih faktorjih abelove grupe. Ciklično grupo, katere moč je potenca praštevila, dekomponiramo takole: $1 \lhd \langle 5 \rangle \lhd \mathbb{Z}_{25}$.

**55.** $\mathbb{Z}_3 \oplus \mathbb{Z}_{27}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_9 \oplus \mathbb{Z}_9$, $\mathbb{Z}_{81}$.

**56.** Za poljubne $x, y, z \in G$ velja $[x,y]^z = [x^z, y^z] \in [G,G]$, zato je $[G,G]$ res edinka v $G$. V kvocientu velja $[x[G,G], y[G,G]] = [x,y][G,G] = 1[G,G]$, zato je $G/[G,G]$ res abelova grupa.

**57.** Za poljubna $x, y \in G$ velja $[xN, yN] = [x,y]N$. Torej je $G/N$ abelova, če in samo če za vse $x, y \in G$ velja $[x,y] \in N$, kar je enakovredno $[G,G] \leq N$.

**58.** Če je grupa $G$ rešljiva, ima vrsto $1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 = G$ z abelovimi faktorji. Torej za vsak $i$ velja $G_i^{(2)} \leq G_{i+1}$. Od tod sledi $1 = G_n \geq G_{n-1}^{(2)} \geq (G_{n-2}^{(2)})^{(2)} = G_{n-2}^{(3)} \geq \cdots \geq G_1^{(n)}$. Obratno, če za nek $n$ velja $G^{(n)} = 1$, potem ravno izpeljana vrsta opazi rešljivost grupe $G$, saj so vsi kvocienti $G_1^{(k)}/G_1^{(k+1)}$ abelovi.

**59.**

- $\mathbb{Z}$ je abelova grupa, zato je $\mathbb{Z}^{(2)} = 1$.
- Izpeljana vrsta $S_3$ je enaka $1 \lhd A_3 \lhd S_3$. Izpeljana vrsta $S_4$ je enaka $1 \lhd \{(), (12)(34), (13)(24), (14)(23)\} \lhd A_4 \lhd S_4$.
- Pokaži $D_{2n}^{(2)} = \langle \rho^2 \rangle$. Slednja grupa je abelova.
- Izračunaj komutator poljubnih dveh takih matrik. Potem si oglej kvocient po osumljeni podgrupi.

**60.** Dokaži $[S_n, S_n] = A_n$ (predznak je homomorfizem) in $[A_n, A_n] = A_n$ (enostavnost $A_n$).

**61.** Uporabi karakterizacijo rešljivosti z izpeljanimi podgrupami. Za rešljivo grupo $G$ in njeno podgrupo $H$ velja $H^{(i)} \leq G^{(i)}$, za njeno edinko $N$ pa $(G/N)^{(i)} = G^{(i)}N/N$. Kadar je $G$ razširitev rešljive grupe $N$ z rešljivo grupo $Q$, velja $G^{(i)} \leq N$ za dovolj velik $i$.

**62.** Naj grupa deluje na sebi s konjugiranjem. Oglej si razredno enačbo in obravnavaj deljivost s $p$. Za rešljivost uporabi prejšnjo nalogo in indukcijo.

**63.**

| | |
|---|---|
| $2^1$ | 1 |
| $2^2$ | 2 |
| $2^3$ | 5 |
| $2^4$ | 14 |
| $2^5$ | 51 |
| $2^6$ | 267 |
| $2^7$ | 2328 |
| $2^8$ | 56092 |
| $2^9$ | 10494213 |
| $2^{10}$ | 49487365422 |

Število grup moči največ 2013 je 49910529547.

**64.** Naj bo $S$ $q$-podgrupa Sylowa. Število vseh $q$-Sylowk je delitelj $p$, ki je 1 mod $q$, torej obstaja ena sama podgrupa Sylowa. Tako je $S$ edinka v $G$ moči $q$, torej $S \cong \mathbb{Z}_q$. Hkrati je $|G/S| = p$, torej je $G/S \cong \mathbb{Z}_p$. Torej je $G$ razširitev rešljive grupe z rešljivo.

**65.** Če je $p = q < r$, si oglej $p$-Sylowke in preštej elemente reda 3 v $G$. Če je $p < q = r$, si oglej $q$-Sylowko. Če je $p < q < r$, si oglej $r$-Sylowke in preštej elemente reda $r$ v $G$, nato si oglej še $q$-Sylowke in preštej elemente reda $q$ v $G$.

**66.**

- Najprej v $G$ poišči podgrupi Sylowa za praštevili 5 in 13. Obe sta edinki in skupaj tvorita rešljivo podgrupo edinko moči 65. Kvocient je moči 9, torej rešljiv.
- Uporabi izreke Sylowa, da dokažeš, da v grupi obstaja podgrupa edinka moči 16.
- Uporabi izreke Sylowa. Potem opazuj delovanje grupe $G$ na odsekih 3-Sylowke.

**67.** Glej $G/Z(G)$.

**68.** Obe Sylowki sta edinki.

**69.** Najprej izračunaj moč $\mathrm{GL}_n(\mathbb{Z}_p)$. Nato si oglej zgornje trikotne matrike z enicami po diagonali.

**71.** Opazuj 2-Sylowke v $S_5$.

**72.** Za moč 36 opazuj delovanje grupe na odsekih 3-podgrupe Sylowa.

**74.** Opazuj delovanje $G$ na odsekih po $H$.

**75.** Opazuj delovanje $G$ na odsekih $p$-podgrupe Sylowa $S$ v $G$. Jedro delovanja je zaradi pogojev prava edinka.

**80.** Enota 1 je gotovo končnega aditivnega reda, recimo $r$, zato za vsak element kolobarja velja $rx = (r1)x = 0$, kar je nemogoče.

**81.** Obrnljiv element mora imeti normo $\pm 1$.

**82.** Binomski izrek.

**84.** Velja $2a = a + a = (a+a)^2 = 4a^2 = 4a$, zato je $2a = 0$. Nadalje je $(a+b) = (a+b)^2 = a + b + ab + ba$, zato je $ab + ba = 0$.

**85.** Najprej pokaži $3x^2 = 3x$. Potem opazuj komutativen podkolobar $\{3x \mid x \in R\}$ kolobarja $R$. Nato manipuliraj.

**86.** Najprej je produkt obrnljivega elementa in nilpotenta zopet nilpotent (ker smo v komutativnem!), zato je dovolj dokazati, da je $1+n$ obrnljiv element za nilpotent $n$. Razstavi $1 = 1 - (-n)^k$. Za primer išči v $2 \times 2$ matrikah.

**87.** Za $g \in G$ z lastnostjo $g^r = 1$ razstavi $0 = 1 - g^r$.

**89.** Karakteristika.

**90.** Evklidov algoritem. Za primer opazuj $F[X, Y]$ in ideal $\langle X, Y \rangle$.

**91.** Kvocient je izomorfen $(\mathbb{Z}[X]/\langle X\rangle)/(\langle X,2\rangle/\langle X\rangle)=\mathbb{Z}_2$.

**93.** Za element $x$ opazuj $(x^2)$.

**94.** Kvocient je izomorfen $R$, izomorfizem izhaja iz $\left[\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right] \mapsto c$.

**95.** Jasno je $\mathrm{M}_n(I)$ ideal v $\mathrm{M}_n(R)$. Obratno, naj bo $J$ ideal v $\mathrm{M}_n(R)$. Naj bo $I=\{a_{11} \mid [a_{ij}] \in J\}$. Tedaj je $I$ ideal v $R$. Pokažimo, da velja $J=\mathrm{M}_n(I)$. Za poljubno matriko $A \in \mathrm{M}_n(R)$ velja $E_{ij}AE_{kl}=a_{jk}E_{il}$. Če je torej $A \in J$ velja $a_{ij}E_{11} \in J$. Zato je $J \subseteq \mathrm{M}_n(I)$. Obratno, naj bo $x \in I$ in $y \in J$ matrika z $y_{11}=x$. Velja $xE_{ij}=E_{i1}yE_{1j} \in J$. Tako vsebovanost $[a_{ij}] \in \mathrm{M}_n(I)$ implicira $[a_{ij}]=\sum a_{ij}E_{ij} \in J$.

**96.** Opazuj $\sum_{g\in G} g$.

**97.** $\mathbb{Q}$, $\mathbb{Q}$, $F$, $F(X)$, $F((X))$ (Laurentove vrste), $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$. Pri zadnjih dveh racionaliziraj.

**98.** $\binom{p}{2}$.

**99.** Izomorfizem je induciran z naravno preslikavo $X \mapsto \zeta$.

**100.** Evklidov algoritem.

**101.** $X^2-2x+2=(X-1)^2+1$.

**102.** Uporabi dejstvo, da je vsota obrnljivega elementa in nilpotenta spet obrnljiv element. Dokazuj z indukcijo na stopnjo polinoma.

**103.** Obseg bo, če in samo če bo polinom nerazcepen, kar se zgodi, če in samo če nima ničle.

**104.** Naj bo $P$ praideal in $p$ polinom najmanjše stopnje v $P$. Če $p \notin \mathbb{Z}$, potem je $p$ nerazepen in $\langle p\rangle$ je praideal v $\mathbb{Z}[X]$, celo maksimalen. Če je $p \in \mathbb{Z}$, potem si oglej $\mathbb{Z}[X]/\langle p\rangle$ in sliko $P$ v tem kvocientnem kolobarju. Za sliko glej Povezave na spletni učilnici.

**105.** Iščeš maksimalne ideale v $\mathbb{Z}[X]/\langle X^2-3\rangle$.

**107.** Najprej določi kvocientni kolobar.

**108.** Dokaz Eisensteinovega kriterija: Reduciraj mod $p$. Vsak od faktorjev mora imeti vse člene razen vodilnega deljive s $p$, kar je v protislovju s pogojem, da $p^2$ ne deli prostega člena.

**109.** Ne. Reduciraj koeficiente na $\mathbb{Z}_2$.

**110.** S protislovjem. Primerjaj koeficiente.

**111.** Eisenstein na $P(X+1)$.

**112.** Kitajski izrek o ostankih, rešitev iščemo napeto na 2 in 3 (v obliki $x=\alpha 2+\beta 3$). Mod 6 dobimo polinom $2X^3+0X^2+1X+4$. Mod 30 dobimo polinom $X^4+8X^3+6X^2+1X+16$.

**113.** Fermatova kongruenca. Oglej si polinom $\prod_{i=1}^{p-1}(X-i)=X^{p-1}-1$ v $\mathbb{Z}_p[X]$. Obratno, naj bo $n=rs$. Potem $r$ deli $(n-1)!$, zato ne more deliti $(n-1)!+1$.

**115.** Opazuj polinome $s_k=\sum_{A\subseteq\{1,\ldots,n\},|A|=k}\prod_{i\in A}X_i$.

**116.** Oponašamo dokaz za polinomski kolobar. Izberi ideal $I$ in v njem število $z$ z najmanjšo neničelno normo. Za poljubno drugo število $w \in I$ najdemo $v \in \mathbb{Z}[i]$, da je $|v - w/z| < 1$. Torej je $vz - w = 0$ po minimalnosti. Sledi $I = \langle z \rangle$.

**117.** Norma obrnljivega elementa je 1.

**118.** Če je število asociirano realnemu številu, je asociirano naravnemu in je zato nerazcepno v $\mathbb{Z}$, torej praštevilo. V nasprotnem razccepimo kvadrat njegove norme v $\mathbb{Z}$; ta razcep velja tudi v Gaussovih številih. Sledi, da je kvadrat norme praštevilo. Velja $2 = (1+i)(1-i) = i(1-i)^2$, asociirano je kvadratu. Praštevilo, kongruentno 3 mod 4, razcepimo na $p = z\bar{z}$ za $z \in \mathbb{Z}[i]$ (namreč: če nek nerazcepen $z$ deli $p$, potem tudi $\bar{z}$ deli $p$, in torej $z\bar{z}$ deli $p$ (ker $z$ ni celo število), zato je $p = z\bar{z} \cdot w$ za nek $w$, kar implicira, da celo število $z\bar{z}$ deli $p$), in si ogledamo kongruenco mod 4. Obratno, naj bo $p$ praštevilo oblike $4n+1$. Uporabi Wilsonov izrek, da dokažeš, da $p$ deli $((\frac{p-1}{2})!)^2 + 1$. Slednje razcepi in sklepaj, da $p$ deli oba faktorja. Odštej.