Algebra 2

July 7, 2022

1 Končne grupe

1.1 Posledice Lagrangeeovega izreka

1. Navedi Lagrangeov izrek
2. Navedi vse majhne grupe do izomorfizma natančno do reda 8
3. POSLEDICA 1 - Kakšno je razmerje med redom grupe in redom njenih podgrup?
4. Za katere m velja $a^m = 1$? Dokaži ekvavilenco
5. Kaj velja za praštevilo p, če $a^p = 1$?
6. Kakšen je red slike homomorfizma?
7. Kdaj je red slike enak redu elementa
8. Kakšen je red odseka aN?
9. POSLEDICA 2 - Kakšni so redi elementov grupe? Dokaži
10. POSLEDICA 3 - Kaj velja za vsak element grupe reda n? Dokaži
11. POSLEDICA 4 - Navedi Fermatov mali izrek. Navedi še njegovo drugo obliko
    - Dokaz
12. POSLEDICA 5 - Kdaj je grupa ciklična? Kateri elementi jo generirajo?
13. - Dokaz

    POSLEDICA 6 - Čemu je ekvivalentno dejstvo, da ima ciklična grupa praštevilski red? Dokaz

1.2 Razredna formula

1. Definiraj kdaj sta elementa konjugirana
2. Kakšna relacija je konjugiranost? Dokaži
3. Definiraj konjugiranostni razred?
4. Čemu je enaka vsota redov konjugiranostnih razredov?
5. Kdaj ima konjugiranostni razred en sam element?
6. Definiraj centralizator elementa a
7. Kdaj je centralizator elementa enak celi grupi?
8. LEMA - V kakšnem razmerju je centralizator do grupe? Dokaži
9. LEMA - Navedi formulo, ki povezuje navedene pojme. Dokaži
10. Kaj velja za element iz centra grupe? (2 lastnosti)
11. Koliko je konjugiranostnih razredov z enim elementom?
12. Navedi razredno formulo

1.3 Cauchyjev izrek

1. Navedi Cauchyjev izrek
2. Dokaz
   - S katero metodo dokazujemo?
   - Dokaži če je red grupe enak p
   - Dokaži, če grupa ni Abelova in $n > p$
   - Dokaži, če je grupa Abelova in $n > p$
3. Navedi Cauchyjev izrek malo drugače. Dokaži ekvavilenco
4. Definiraj p-grupo
5. Za kakšne grupe ima ta definicija smisel?
6. Kaj je ekvivalentno temu, da je G p-grupa?

1.4 Delovanja grup

1. Definiraj delovanje grupe G na množici X
2. Definiraj orbito elementa x
3. Definiraj stabilizator elementa x
4. PRIMER 1 - Navedi delovanje s katerim grupa deluje sama na sebi
5. PRIMER 2 - Pokaži, da je konjungiranje delovanje
6. PRIMER 3 - Navedi delovanje s katerim grupa deluje na množici vseh odsekov podgrupe H
7. PRIMER 4 - Navedi delovanje s katerim grupa deluje na množici vseh podgrup
8. PRIMER 5 - Navedi delovanje s katerim grupa S_n deluje na množici vseh polinomov v n spremenljivkah
9. PRIMER 6 - Navedi delovanje s katerim grupa $GL_n(R)$ deluje na množici R^n
10. Kaj je trivialno delovanje?
11. V kakšnem razmerju je stabilizator z dano grupo?
12. Definiraj ekvavilenčno relacijo
13. Kaj so njeni ekvavilenčni razredi?
14. Navedi izrek o orbiti in stabilizatorju (formula). Navedi preslikavo, ki formulo dokazujemo
15. Navedi razredno formulo v skladu z novimi oznakami
16. Kaj velja za to formulo, če je G končna p-grupa?

1.5 Izreki Sylowa

1. Definiraj normalizator
2. Navedi tri trditve, ki veljajo za normalizator
3. Definiraj p-podgrupo
4. Definiraj p-podgrupo Sylowa
5. (definiraj najprej red grupe G) Kakšen red imajo p-podgrupe?
6. (definiraj najprej red grupe G) Kakšen red imajo p-podgrupe Sylowa?
7. Za kakšno grupo G veljajo izreki Sylowa?

8. IZREK 1 - Kdaj G vsebuje p-podgrupo reda p^l?
    - S katero metodo dokazujemo ta izrek?
    - Dokaži, če p ne deli reda centra grupe
    - Dokaži, če p deli red centra grupe
9. IZREK 2 - V kakšnem razmerju so p-podgrupe in p-podgrupe Sylowa?
    - Definiraj množico vseh odsekov
    - Definiraj delovanje
    - Definiraj množico Z
    - Pokaži, da Z ni prazna
    - Pokaži, da je H podgrupa
10. IZREK 3 - Iz dane p-podgrupe pridobi novo p-podgrupo. Zakaj to velja?
11. POSLEDICA - Kdaj je p-podgrupa Sylowa podgrupa edinka?
12. IZREK 4 - Kaj velja za število vseh p-podgrup?
    - Definiraj množico vseh p-podgrup Sylowa
    - Definiraj delovanje na tej množici
    - Kaj je orbita?
    - Kaj je stabilizator?
    - Po lemi o orbiti in stabilizatorju privedi dokaz do konca
13. IZREK 5 - Kakšne oblike je število vseh p-podgrup?
    - Definiraj množico vseh p-podgrup
    - Definiraj delovanje na njej
    - Definiraj podmnožico podgrup Sylowa W
    - Kateri element je zagotovo vsebovan v W?
    - Pokaži, da je to edini element, ki je vseboven v W
    - Izpelji koliko je število p-podgrup Sylowa

1.6 Končne Abelove grupe

1. Naštej vse končne abelova grupe
2. LEMA 1 - Navedi lemo, s katero grupo razdelimo na dve podgrupi
3. Dokaz
    - kaj moraš dokazat?
    - uporabi Lagrangeevo posledico

- uporabi tujust elementov
- pokaži, da je vsota direktna

4. Iz leme izpelji izomorfizem med cimličnimi grupami
5. LEMA 2 - Posploši prvo lemo na splošnejše rede grupe G. Dokaz
6. LEMA 3 - Kdaj je p-grupa ciklična? (ekvavilenca)
7. Dokaz
    - (=¿) če je G ciklična
    - (¡=) če je red(G) = p
    - (¡=) Kaj lahko poveš o edini podgrupi s p elementi?
    - (¡=) formalno zapiši kaj je ta podgrupa
    - (¡=) uporabi izrek o izomorfizmu in definiraj preslikavo
    - (¡=) kaj velja za sliko endomorfizma?
    - (¡=) kaj zato vemo o kvocientni grupi?
    - (¡=) kaj so elementi kvocientne grupe?
    - (¡=) kako lahko torej razpišemo G?
    - (¡=) pokaži, da je G ciklična
8. LEMA 4 - Kako podgrupo dopolnimo do grupe? Kakšna mora biti podgrupa, da to sploh lahko storimo?
9. Dokaz
    - kako dopolnimo, če je G ciklična?
    - če G ni ciklična, kaj je IP.?
    - Kaj nam o G in C pove lema 3?
    - Kaj velja za
10. Navedi osnovni izrek o končnih abelovih grupah
11. Kaj so ciklične grupe?
12. Kako izberemo podgrupe, če je G netrivialna?
13. Dokaži osnovni izrek
14. Navedi ekvivalentno formulacijo izreka
15. Kdaj so si direktne vsote ekvavilentne?
16. IZREK - Klasifikacija končnih Abelovih grup
17. Dokaz
18. Navedi osnovni izrek o končno generiranih abelovih grupahni

2 Deljivost v komutativnih kolobarjih

2.1 Glavni ideali

1. Definiraj glavni ideal
2. Razloži vsebovanost elementa a in ideala (a)
3. Kako je generiran glavni ideal?
4. Kdaj je ideal glavni?
5. Definiraj desni ideal generiran z a. Kako ga označimo?
6. Definiraj levi ideal generiran z a. Kako ga označimo?
7. Kakšne oblike elementi so v dvostranskem idealu generiranem z a? Kako ga označimo?
8. S kakšnimi kolobarji se ukvarjamo mi?
9. Katera dva ideala sta vedno glavna? S čem sta generirana?
10. Kdaj je (a)=K? Zakaj?
11. Kdaj sta to edina ideala? Kaj iz tega sledi?
12. Kaj so glavni ideali celih števil? S čem je generiran? Kaj zato velja?
13. Kaj so glavni ideali kolobarja F[X]? S čem so generirani? Kaj velja za glavne ideali F[X]?
14. Definiraj končno generiran ideal
15. Kaj vse vsebuje končno generiran glavni ideal?
16. Elementi kakšne oblike so v končno generiranem idealu?
17. Kako je končno generiran ideal povezan z glavnimi ideali?
18. Kaj vsebuje ideal (4, 6) kolobarja celih števil? Čemu je enak?
19. Kaj vsebuje ideal (2, X) kolobarja F[X]? Ali je glavni?

2.2 Deljivost in nerazcepnost

1. Definiraj, da b deli a. Kakšen mora biti kolobar? Kako označimo?
2. Poimenuj a in b
3. Definiraj deljivost z glavnimi deali
4. Dokaži ekvavilenco definicij deljivosti

5. Definiraj kdaj sta elementa asociirana
6. Kaj velja za deliteje asociiranih elementov. Katere elemente asociirana elementa delita?
7. Natanko kdaj sta si elementa celega kolobarja asociirana?
    - dokaz (=¿)
    - dokaz (¡=)
8. Kaj so asociirani elementi v kolobarju celih števil?
9. Kaj so asociirani elementi v F[X]?
10. Definiraj največji skupni delitelj elementov a in b. V kakšnem kolobarju je definiran?
11. Definiraj kdaj sta elementa tuja
12. Kaj je z enoličnostjo in obstojem največjega skupnega delitelja?
13. Kaj velja za različne največje skupne delitelje?
14. Kako dosežemo enoličnost v Z?
15. Kako dosežemo enoličnost v F[X]?
16. TRDITEV - Kdaj obstaja največji skupni delitelj kolobarja? Kakšne oblike je? Kakšen mora biti kolobar?
    - dokaži, da obstaja skupni delitelj in njegovo obliko
    - dokaži, da je največji
17. Definiraj nerazcepen element v kakem kolobarju ga definiramo?
18. Definiraj razcepen element
19. Kaj so nerazcepni elementi kolobarja celih števil?
20. Najdi nek nerazcepen element v Z[X]. Zakaj ta element ni nerazcepen v Q[X]?
21. Kaj so obrnljivi elementi v Z[i]? Najdi nek razcepen in nek nerazcepen element v tem kolobarju in razloži zakaj je razcepen oz. nerazcepen
22. TRDITEV - Kdaj je element celega kolobarja nerazcepen (ekvavilenca)? Dokaži

2.3 Evklidski kolobarji

1. Navedi izrek o deljenju za polinome
2. Dokaz
   - Dokaži, če je deljenec ničeln. Kaj vzamemo za $q(x)$ in kaj za $r(x)$?
   - S katero metodo dokazujemo?
   - Kaj vzamemo za $q(x)$ in kaj za $r(x)$ pri $st(f(x)) = 0$?
   - Dokaži za $m- > m+1$
3. Definiraj evklidski kolobar
4. Naštej tri osnovne evklidske kolobarje
5. Najdi enega, ki ni evklidski
6. Za vsakega od njih najdi preslikavo δ $(Z,\, F[X])$
7. Katera algebraična struktura je vedno evklidski kolobar? Kaj je njena preslikava δ?
8. IZREK - Kakšni so ideali evklidskega kolobarja? Dokaži
9. POSLEDICA - Navedi ekvavilence temu, da je p nerazcepen. Pri kakšnih pogojih to velja? Dokaži
10. POSLEDICA - Kaj Zagotovo obstaja v evklidskem kolobarju?
11. POSLEDICA - Zaradi katere se vpelje praelement. Dokaži
12. Definiraj praelement
13. Kaj velja za praelemente? (Od sošolca zapiski)
14. Kaj velja za praelemente v Evklidskih kolobarjih? Dokaži (Od sošolca zapiski)
15. LEMA - Kdaj lahko tvorimo zaporedje elementov, katerih ideali so strogo naraščajoči?
16. Navedi dve definiciji Noetherskega kolobarja
17. Navedi Hilertov izrek o bazi
18. Naštej tri kolobarje, ki so Noetherski
19. Navedi nek kolobar, ki ni Noetherski
20. LEMA - Kateri kolobarji so vedno Noetherski? Dokaži
21. Kaj povesta zadnji dve lemi?

22. Kaj so ideali Noetherskega kolobarja?
23. Definiraj kolobar z enolično faktorizacijo
24. Kaj pomeni "do asociiranosti natančno"?
25. Kateri kolobarji imajo enolično faktorizacijo?
26. Povzemi kaj velja za evklidske kolobarje
27. Navedi osnovni izrek aritmetike za evklidske kolobarje

2.4 Nerazcepni polinomi

1. Kdaj je kolobar polinomov evklidski?
2. Kakšni so ideali kolobarja polinomov? Kakšne oblike so? Kaj jih generira?
3. Definiraj največji skupni delitelj polinomov. Ali obstaja? Kakšne oblike je? Kdaj je enoličen?
4. Kaj so obrnljivi elementi v kolobarju polinomov?
5. Kateri elementi kolobarja polinomov so nerazcepni?
6. Čemu je nerazcepnost polinomov ekvavilentna?
7. Kako lahko zapišemo nekonstantne polinome?
8. Kateri polinomi so nerazepni?
9. Kaj pravi osnovni izrek algebre v C?
10. Kateri polinomi so nerazcepni v C?
11. Kako lahko zapišemo nekonstantne polinome v C?
12. Kateri polinomi so nerazcepni v R?
13. Kako lahko zapišemo nekonstantne polinome v R?
14. TRDITEV - Kdaj ima polinom ničlo a? (kaj ga mora deliti?) Dokaži
15. POSLEDICA - Kdaj so polinomi katere stopnje nerazcepni?
16. Kaj NE vpliva na nerazcepnost polinomov?
17. Definiraj primitiven polinom na dva načina
18. LEMA - Kaj je produkt primitivnih polinomov?
    - S katero tehniko dokazujemo?
    - Definiraj ideal v katerem je produkt polinomov

- Kaj pa sledi za ta ideal, ker sta $f(x)$ in $g(x)$ primitivna?
- Definiraj odseka
- Koliko je produkt teh odsekov?
- Kaj iz tega sledi za kvocientni kolobar?
- Privedi do protislovja z zadnjo točko

19. IZREK - Kako je z nerazcepnostjo polinomov v $Z[X]$ in $Q[X]$?
    - Kaj moramo dokazati?
    - Zapiši enakost
    - Vpelji največje skupne delitelje in zapiši enakost
    - Uporabi lemo
    - Izpelji do konca
20. Ime leme, ki sledi iz leme in izreka
21. Kaj pravi Eisensteinov kriterij?
    - S katero tehniko dokazujemo?
    - Kaj sledi iz izreka?
    - Kaj velja za konstanten člen?
    - Kaj velja za vodilni člen?
    - Kaj velja za koeficiente enega od faktorjev (polinomov)?
    - Razpiši koeficient začetnega polinoma
    - Privedi do protislovja
22. Katera znana polinomska funkcija je nerazcepna?
23. Definiraj množico primitivnih korenov
24. Definiraj ciklonomične polinome

3 Ničle polinomov in razširitve polj

3.1 Algebraični in transcedentni elementi

1. Zakaj vpeljujemo nova polja?
2. Naštej 7 primerov polj
3. Navedi en algebraičen in en transcedentni element
4. Kaj je razlika med transcedentnim in algebraičnim elementom?
5. Definiraj algebraičen element

6. Definiraj transcedentni element
7. Definiraj minimalni polinom algebraičnega elementa a
8. Definiraj stopnjo algebraičnosti
9. Dokaži obstoj minimalnega polinoma algebraičnega elementa a
10. Dokaži enoličnost minimalnega polinoma algebraičnega elementa a
11. Navedi ekvavilence temu, da je $p(x)$ minimalni polinom algebraičnega elementa a
    - 1. ekvavilenca
    - 2. ekvavilenca
    - 3. ekvavilenca
12. Kateri elementi so algebraični stopnje 1? Kaj je njihov minimalni polinom?
13. Pokaži, da je vsako kompleksno število algebraično nad realnimi števili. Kaj je njegova stopnja algebraičnosti?
14. Najdi transcedentni element v polju racionalnih funkcij. Zakaj ni algebraičen?
15. Kdaj algebraičnim oz. transcedentnim elementom pravimo števila?
16. Definiraj algebraično število
17. Kako iz polinoma v $Q[X]$ dobimo polinom v $Z[X]$?
18. Ali je i algebraičen? Če ja, katere stopnje in katerega polinoma?
19. Ali je praštevilo p algebraično število? Če ja, katere stopnje in katerega polinoma?
20. Kakšna je množica algebraičnih števil? Zakaj?
21. Kakšna je množica transcedentnih števil?

3.2 Končne razširitve

1. Kako lahko obravnavamo razširitev E polja F? Pokaži zakaj
2. Definiraj končno razširitev E polja F
3. Definiraj stopnjo razširitve. Kako jo označimo?
4. Kako označujemo stopnjo razširitve v linearni algebri?
5. Navedi primer končne razširitve. Kaj je baza razširitve kot vektorskega prostora? Kolikšna je stopnja razširitve?

6. Navedi primer, ki ni končna razširitev Q. Zakaj ni?
7. IZREK - O "tranzitivnosti" končnih razširitev. Dokaži
   - Definiraj baze
   - Pokaži, da je "baza" E nad F ogrodje
   - Pokaži, da je "baza" E nad F linearno neodvisna
8. POSLEDICA - Kdaj $[L : F]$ deli $[E : F]$. Dokaži
9. Definiraj algebraično razširitev
10. Definiraj transcedentno razširitev
11. TRDITEV - Katere razširitve so algebraične? Dokaži
12. Ali velja obrat trditve?
13. Kaj označuje $F[A]$?
14. Kaj označuje $F(A)$?
15. Kako pišemo ti dve množici, če je A končna?
16. Eksplicitno zapiši ti dve množici v primeru, ko $A = a$
17. Kako imenujemo $F(A)$?
18. Definiraj enostavno razširitev polja. Kako imenujemo element a?
19. PRIMER - Kakšne oblike so elementi $f(i)$ za $f(x) \in Q[X]$? Zakaj?
20. Čemu je enak $R[X]$? Kaj zato velja?
21. IZREK - V skladu z novo vpeljanimi oznakami povej kaj velja za algenraičen element stopnje n a
   - Pokaži, da je $F[A]$ polje (vsebovanost inverznih elementov)
   - Dokaži enakost $F[A]$ in množice, ki si jo definirala (vzami nek element iz $F[A]$ in pošiči njegovo stopnjo)
   - Pokaži stopnjo algebraičnosti (poišči bazo)
22. PRIMER - Poišči bazo $Q(n - rootp)$
23. PRIMER - Kaj je $Q(\sqrt{2})$
24. PRIMER - Kaj je $Q(tretjikoreniz2)$
25. OPOMBA - Poišči epimorfizem kolobarjev $F[X] \to F[a]$
   - Poišči izomorfizem, če je a algebraičen
   - Poišči izomorfizem, če je a transcedenten

26. Kaj velja za stopnjo algebraičonsti polja, L, ki vsebuje F?

27. IZREK - Razširi prejšni izrek na višje dimenzije

   - Kaj sledi iz indukcijske predpostavke?
   - Kako iz tega dobiš končno razširitev polja F z n algebraičnimi elementi?
   - Zakaj je kolobar $F[a_1, ...a_n]$ polje?

28. Opiši polje $Q(\sqrt{2}, \sqrt{3})$. Kolikšna je njegova stopnja algebraičnosti nad poljem Q?

29. Navedi izrek o primitivnem elementu

30. PRIMER - Čemu je enak $Q(\sqrt{2}, \sqrt{3})$?

31. POSLEDICA - Algebraično opiši množico vseh elementov iz E, ki so algebraični nad F. Dokaži

32. Navedi primer podpolja algebraičnih števil

33. Navedi primer polja algebraičnih števil nad nekim poljem, ki je algebraična razširitev, a ni končna

3.3 Konstrukcije z ravnilom in šestilom

1. Poimenuj tri probleme antične grčije

2. Opiši podvojitev kocke in formaliziraj

3. Opiši trisekcijo kota in formaliziraj

4. Opiši kvadraturo kvadrata in formaliziraj

5. Kako iz dane množice točk konstruiramo novo točko z ravnilom in šestilom?

6. Definiraj konstruktabilne točke

7. Kaj je največja množica konstruktabilnih točk?

8. Definiraj konstruktabilna števila

9. Zapiši lemo, s katero izpeljemo glavni izrek tega poglavja. Dokaži (razdeli na tri dele)

10. Navedi glavni izrek tega poglavja. Koliko je stopnja algebraičnosti komponent v izreku?

11. Razloži zakaj ni možno - podvojitev kocke

12. Razloži zakaj ni možno - trisekcija kota

13. Razloži zakaj ni možno - kvadratura kroga

3.4 Kratnost ničle polinoma

1. TRDITEV - Natanko kdaj ima polinom ničlo $a \in E$? Pazi od kod jemlješ polinome!
2. Definiraj enostavno ničlo
3. Definiraj k-kratno ničlo
4. PRIMER - Najdi in kategoriziraj ničle $x^4 - 2x^3 + 2x - 1$
5. Kako pridemo do polinoma brez ničel v E?
6. Koliko ničel ima f?
7. Pokaži, da f nima drugih ničel kot teh, ki jih dobimo v razcepu
8. Kolikšne stopnje je f?
9. TRDITEV - Največ koliko ničel ima neničeln polinom?
10. PRIMER - Dan imaš polinom $f(x) = x^6 - 3x^4 + 4$ Najdi število ničel in polinom brez ničel v Q, R in C
11. Kdaj so ničle polinomov enostavne?
12. Definiraj odvod polinoma
13. Kolikšne stopnje je odvod polinoma? Kdaj ta enačba velja? Zakaj drugače ne velja?
14. IZREK - Kdaj so vse ničle polinoma enostavne? Dokaži
15. Definiraj seperabilen polinom
16. Definiraj seperabilno razširitev
17. Definiraj perfektno polje
18. Navedi primera perfektnih polj
19. Navedi primer polja, ki ni perfektno. Koliko je njegova karakteristika?