16 Dodatek - Pomembni rezultati.

Grupa. Red grupe. Red elementa.

1. V grup je enota enolično določena edinstvena.
2. V grupi je inverz elementa enolično določen.
3. Če je $(G, \cdot)$ grupa, potem je $(a^{-1})^{-1} = a \ \ \forall a \in G$.
4. Če je $(G, \cdot)$ grupa, potem je $(ab)^{-1} = b^{-1}a^{-1} \ \ \forall a, b \in G$.
5. Če je $(G, \cdot)$ grupa in $ab = ac$, potem je $b = c$.
6. Če je $(G, \cdot)$ grupa in $ba = ca$, potem je $b = c$.
7. V končni grupi je red vsakega elementa končan in ne more biti večji od reda grupe.
8. V grupi je red elementa in njegovega inverza isti.

Podgrupe.

1. Če je H podgrupa grupe G potem
   (i) Je identiteta podgrupe H in grupe G ista.
   (ii) Je inverz elementa v podgrupi H glede na grupo H in G isti.
   (iii) Je red elementa v podgrupi H glede na grupo H in G isti.
2. Naj bo G grupa z binarno operacijo množenja. Podmnožica H grupe G je podgrupa grupe G če velja eden od naslednji ekvivalentnih pogojov:
   (a) $ab \in H$, $a^{-1} \in H \ \ \forall a, b \in H$
   (b) $ab^{-1} \in H \ \ \forall a, b \in H$
   Če je H končna je H podgrupa grupe G, če je $ab \in H \ \ \forall a, b \in H$.
3. Presek dveh podgrup grupe je tudi podgrupa grupe.

Ciklične grupe.

1. Vsaka ciklična grupa je abelska.
2. Če je a generator ciklične grupe G, potem je a^{-1} tudi generator grupe G.
3. Če končna grupa reda n vsebuje element reda n, potem je ta grupa ciklična.
4. Vsaka grupa praštevilskega reda je ciklična.
5. V vsaki grupi sestavljenega reda obstaja prava podgrupa.
6. Naj bo G ciklična grupa generirana z elementom $a \in G$ in naj bo $o(a) = n$. Za $m < n$, je element a^m generator grupe G če in samo če $\gcd(m, n) = 1$.
7. **(Fundamentalni izrek za ciklične grupe.)** Vsaka podgrupa ciklične grupe je ciklična. Poleg tega, če je $|\langle a \rangle| = n$, potem je red katerekoli podgrupe grupe $\langle a \rangle$ delitelj števila n. Za vsak pozitiven deljitelj k števila n, ima grupa $\langle a \rangle$ natanko eno podgrupo reda k - namreč $\langle a^{\frac{n}{k}} \rangle$.

8. Za vsak pozitiven delitelj k števila n, je množica $\langle n/k \rangle$ podgrupa grupe $\mathbb{Z}_n$ reda k. Poleg tega, te podgrupe so edine podgrupe grupe $\mathbb{Z}_n$.

9. Vsaka podgrupa ciklične grupe je ciklična.

10. Vsaka neskončna ciklična grupa ima natanko dva generatorja.

11. Vsaka prava podgrupa neskončne ciklične grupe je neskončna.

Permutacijske grupe.

1. Množica S_A vseh permutacij neprazne množice A je grupa glede na operacijo kompozicije funkcij.

2. Vsaka grupa je izomorfna neki permutacijski grupi (Cayley).

3. Vsaka permutacija se lahko napiše kot produkt transpozicij.

4. Množica vseh sodih permutacij končne množice je grupa glede na operacijo kompozicije funkcij.

5. Red permutacije končne množice zapisane kot produkt disjunktnih ciklov je najmanjši skupni večkratnik dolžine ciklov.

6. Če je π permutacija potem $\pi(a_1 a_2 ... a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)...\pi(a_k))$.

Homomorfizmi. Izomorfizmi.

1. Če je ϕ homomorfizem iz grupe G v grupo G' potem $\phi(e) = e'$.

2. Če je ϕ homomorfizem iz grupe G v grupo G' potem $\phi(a^{-1}) = [\phi(a)]^{-1} \ \forall a \in G$.

3. Če je ϕ izomomorfizem iz grupe G v grupo G' potem $\phi(a^n) = [\phi(a)]^n \ \forall a \in G$.

4. Naj bo $\phi : G \to G'$ izomomorfizem. Potem $G = \langle a \rangle$ če in samo če je $G' = \langle \phi(a) \rangle$.

5. Če je ϕ izomomorfizem iz grupe G v grupo G' potem $o(a) = o[\phi(a)] \ \forall a \in G$.

6. Naj bo $\phi : G \to G'$ surjektivni homomorfizem. Potem je homomorfizem ϕ izomorfizem iz grupe G v grupo G' če in samo če $\ker(\phi) = \{e\}$.

7. Naj bo $\phi : G \to G'$ izomomorfizem. Potem je ϕ^{-1} izomomorfizem iz grupe G' v grupo G.

Odseki in Lagrangeov izrek.

1. Če je H podgrupa grupe G, potem sta vsaka dva desna (ali leva) odseka podgrupe H v grupi G enaka ali disjunktna.

2. Če je H podgrupa grupe G, potem obstaja bijektivna korespodenca med vsakima dvema desnima (ali levima) odsekoma podgrupe H v grupi G.

3. Če je H podgrupa grupe G, potem je unija vseh desnih (ali levih) odsekov podgrupe H v grupi G enaka grupi G.

4. Če je H podgrupa grupe G, potem desni (ali levi) odseki podgrupe H v grupi G porodio particijo grupe G.

5. **Lagrangeov izrek**. Red vsake podgrupe končne grupe deli red grupe.

6. Če je G končna grupa glede na operacijo množenja potem je $a^{|G|} = e \ \forall a \in G$.

Direktni produkt grup.

1. **(Direktni produkt grup).** Naj bodo $G_1, G_2, ..., G_n$ grupe. Za $(a_1, a_2, ..., a_n)$ in $(b_1, b_2, ..., b_n)$ v $\prod_{i=1}^{n} G_i$ definirajmo operacijo množenja po komponentah $(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n)$. Potem je $\prod_{i=1}^{n} G_i$ skupaj s to operacijo grupa, ki jo imenujemo direktni produkt grup G_i.
2. **(Red elementa v direktnem produktu).** $|(g_1, g_2, ..., g_n)| = \text{lcm}(|g_1|, |g_2|, ..., |g_n|)$
3. **(Kriterij, da je $G \times H$ ciklična).** Naj bosta G in H končni ciklični grupi. Potem je $G \times H$ ciklična, če in samo če sta $|G|$ in $|H|$ tuji števili.
4. **(Kriterij za $\mathbb{Z}_{n_1 n_2 ... n_k} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$).** Naj bo $m = n_1 n_2 ... n_k$. Potem sta grupi $\mathbb{Z}_m$ in $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$ izomorfni če in samo če so si števila n_1, n_2, ..., n_k v paroma tuja.
5. Spomnimo se $U(n) = \{k \in \mathbb{N} \mid k < n, \gcd(k, n) = 1\}$. Naj bosta s, t tuji naravni števili. Potem
$$U(st) \cong U(s) \times U(t).$$
Poleg tega, če je $U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}$ potem $U_s(st) \cong U(t)$ in $U_t(st) \cong U(s)$.

Podgrupe edinke. Kvocientne grupe.

1. **(Test za edinke.)** Podgrupa H grupe G je edinka v grupi G če in samo če $xHx^{-1} \subseteq H$ za vsak $x \in G$.

2. Podgrupa N grupe G glede na operacijo množenja je edinka v grupi G če in samo če $gNg^{-1} = N \ \forall g \in G$.

3. Podgrupa N grupe G je edinka v grupi G če in samo če je produkt dveh desnih odsek (podgrupe N v grupi G) spet desni odsek (podgrupe N v grupi G).

4. Produkt dveh edink grupe je tudi edinka grupe.

5. Presek dveh edinke grupe je tudi edinka grupe.

6. **(Kvocientne grupe.)** Naj bo G grupa in naj bo H edinka grupe G. Množica $G/H = \{aH \mid a \in G\}$ je grupa, glede na operacijo $(aH)(bH) = abH$, reda $[G : H]$.

7. Naj bo N edinka v grupi G glede na opearcijo množenja. Če je $\phi : G \to G/N$ definiran z $\phi(g) = Ng$, za $g \in G$, potem je ϕ surjektivni homomorfizem iz grupe G v grupo G/N. Jedro homomorfizma ϕ je N.

8. Če je ϕ surjektivni homomorfizem iz grupe G v grupo G', potem je $G/\ker(\phi) = G'$.

Homomorfizmi grup.

1. **(Lastnosti elementov glede na homomorfizem.)** Naj bo ϕ homomorfizem iz grupe G v grupo $\overline{G}$, in naj bo g element grupe G. Potem

   i. ϕ preslika identiteto grupe G v identiteto grupe $\overline{G}$.

   ii. $\phi(g^n) = (\phi(g))^n$ za vsak $n \in \mathbb{Z}$.

   iii. Če je $|g|$ končen, potem $|\phi(g)|$ deli $|g|$.

   iv. $\ker\phi$ je podgrupa grupe G.

   v. $\phi(a) = \phi(b)$ če in samo če $a\ker\phi = b\ker\phi$.

   vi. Če je $\phi(g) = g'$, potem je $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\ker\phi$.

2. **(Lastnosti podgrupe glede na homomorfizem.)** Naj bo ϕ homomorfizem iz grupe G v grupo $\overline{G}$, in naj bo H podgrupa grupe G. Potem

   i. $\phi(H) = \{\phi(h) \mid h \in H\}$ je podgrupa grupe $\overline{G}$.

   ii. Če je H ciklična, potem je $\phi(H)$ ciklična.

   iii. Če je H, abelska potem je $\phi(H)$ abelska.

   iv. Če je H edinka v G, potem je $\phi(H)$ edinka v $\phi(G)$.

   v. Če je $|\ker\phi| = n$, potem je ϕ n-na-1 preslikava iz G na $\phi(G)$ (ϕ je n-na-1 surjekcija).

   vi. Če je $|H| = n$, potem $|\phi(H)|$ deli n.

   vii. Če je $\overline{K}$ podgrupa grupe $\overline{G}$, potem je $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ podgrupa grupe G.

   viii. Če je $\overline{K}$ edinka grupe $\overline{G}$, potem je $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ edinka grupe G.

   ix. Če je ϕ surjekcija in $\ker\phi = \{e\}$, potem je ϕ izomorfizem iz G v $\overline{G}$

3. **(Jedro homomorfizma je edinka.)** Naj bo ϕ homomorfizem iz grupe G v grupo $\overline{G}$. Potem je $\ker\phi$ edinka grupe G.

4. **(Prvi izrek o izomorfizmu.)** Naj bo ϕ homomorfizem grupa iz grupe G v grupo $\overline{G}$. Potem je preslikava iz grupe $G/\ker\phi$ v grupo $\phi(G)$, podana z $g\ker\phi \to \phi(g)$, izomorfizam. Torej $G/\ker\phi \cong \phi(G)$.

5. Naj bo ϕ homomorfizem iz končne grupe G v grupo $\overline{G}$. Potem $|\phi(G)|$ deli $|G|$ in $|\overline{G}|$.

Delovanje grupe na množici.

1. Naj G deluje na množici X. Za poljuben element $x \in X$ je stabilizator G_x elementa x podgrupa grupe G.

2. Naj bo X G-množica. Za vsak $g \in G$, je funkcija $\sigma_g : X \to X$ definirana z $\sigma_g(x) = gx$ za $x \in X$, permutacija množice X. Tudi, preslikava $\phi : G \to S_X$ definirana z $\phi(g) = \sigma_g$ je homomorfizem z lastnostjo, da je $\phi(g)(x) = gx$.

3. Naj bo X G-množica in naj bosta $x \in X$, $g \in G$ poljubna elementa. Potem je $G_{gx} = gG_xg^{-1}$. Še več, če je H neka neprazna množica, potem je $G_{gH} = gG_Hg^{-1}$.

4. Naj bo X G-množica in naj bosta $x \in X$, $g \in G$ poljubna elementa. Če je $gx = y$ in $T = \{t \in G \mid tx = y\}$, potem je $T = gG_x$.

5. **(Orbita-stabilizator izrek.)** Naj bo X G-množica in naj bo $x \in X$. Potem je $|Gx| = [G : G_x]$. Če je G končna, potem je $|Gx|$ deljitelj od $|G|$. Poleg tega

$$|G| = |Gx| \cdot |G_x|.$$

6. Množica orbit pri delovanju grupe G na množici X predstavlja razbitje (oz. particijo) množice X (različne orbite so disjunktne).

Izreki Sylowa.

1. **(Cauchijev izrek.)** Naj bo G končna grupa in naj p deli $|G|$, kje je p praštevilo. Potem obstaja element $a \in G$ $(a \neq e)$ t.d. $a^p = e$ (obstaja element reda p).

2. Naj bo G končna abelska grupa. Če m deli red grupe G, potem obstaja $H \leq G$ reda m.

3. **(prvi izrek Sylowa)** Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem za vsak i $(1 \leq i \leq k)$ velja, da ima G najmanj edno podgrupo reda p^i.

4. **(drugi izrek Sylowa)** Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem sta vsaki dve podgrupi reda p^k konjugirani.

5. **(tretji izrek Sylowa)** Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem je število podgrup reda p^k oblike $1 + mp$, kjer je m neko ne-negativno celo število. Velja tudi, da $1 + mp$ deli $|G|$.

Grupa automorfizmov.

1. **(G/Z izrek)** Naj bo G grupa in naj bo $Z(G)$ center grupe G. Če je $G/Z(G)$ ciklična grupa, potem je G abelska.

2. Naj bo f automorfizem grupe G. Če je H podgrupa grupe G, potem je $f(H)$ tudi podgrupa grupe G.

3. Naj bo f automorfizem grupe G. Če je N edinka grupe G, potem je $f(N)$ tudi edinka grupe G.

4. Za abelske grupe je edini notranji automorfizem identična preslikava, medtem ko za neabelske grupe obstaja netrivialen notranji automorfizem.

5. Množica $\mathrm{Inn}(G)$ vseh notranjih automorfizmov grupe G je edinka grupe $\mathrm{Aut}(G)$ (vseh automorfizmov grupe G).

6. Za vsako grupo G je $G/Z(G)$ izomorfna z $\mathrm{Inn}(G)$ (kjer je $Z(G)$ center grupe G).

Osnovni izrek o končnih Abelskih grupah.

1. **(Osnovni izrek o končnih Abelskih grupah.)** Vsaka končna abelska grupa je direktni produkt cikličnih grup, katerih red je praštevilska potenca. Število cikličnih grup v produktu in njihov red sta enolično določena.

Ker je vsaka ciklična grupa reda n izomorfna grupi $\mathbb{Z}_n$, osnovni izrek o končnih Abelskih grupah torej pove, da je vsaka končna abelska grupa G izomorfna grupi oblike

$$\mathbb{Z}_{{p_1}^{n_1}} \times \mathbb{Z}_{{p_2}^{n_2}} \times ... \times \mathbb{Z}_{{p_k}^{n_k}}$$

kjer so p_i praštevila (ki niso nujno različna), in kjer so števila ${p_1}^{n_1}$, ${p_2}^{n_2}$, ..., ${p_k}^{n_k}$ $(n_i \in \mathbb{N})$ enolično določena z grupo G.

Center. Normalizator elementa.

1. Relacija konjugiranosti na grupi je ekvivalenčna relacija na grupi G in pripadajoči ekvivalenčni razredi porode particijo grupe G v medsebojno disjunktne ekvivalenčne razrede, ki jih imenujemo razredi konjugiranosti.
2. Normalizator $N(a)$ elementa a v grupi G je podgrupa grupe G.
3. Če je G končna grupa, potem je $|G| = \sum_a \frac{|G|}{|N(a)|}$, kjer vsota teče po elementih a, ki so predstavniki razredov konjugiranosti.
4. Center grupe G je edinka v grupi G.
5. Število razredov konjugiranosti ne-abelskih grup reda p^3, kje je p praštevilo, je $p^2 + p - 1$.
6. Če je G končna grupa, potem je $|G| = |Z| + \sum_{a \notin Z} \frac{|G|}{|N(a)|}$, kjer vsota teče po elementih a, ki so predstavniki razredov konjugiranosti, ki vsebujejo več kot en element.
7. Naj bo G grupa in naj bo $Z(G)$ center grupe G. Če je $G/Z(G)$ ciklična grupa, potem je G abelska.

Ostalo.

1. Končna grupa G je p-grupa če in samo če je $|G|$ enak potenci števila p.
2. Relacija konjugiranosti na množici vseh nepraznih podmnožic grupe je ekvivalenčna relacija.
3. Relacija konjugiranosti na množici vseh podgrup grupe je tudi ekvivalenčna relacija.
7. Naj bo G grupa. Za poljubno neprazno podmnožico S grupe G, je normalizator $N(S)$ množice S podgrupa grupe G.
8. Če je G končna grupa in $S \subseteq G$ $(S \neq \emptyset)$ potem je $|C(S)| = \frac{|G|}{|N(S)|}$.
9. Naj bosta H in K dve (ne nujno različni) podgrupi končne grupe G. Za $x, y \in G$ sta dvojna odseka HxK in HyK bodisi enaka, bodisi disjunktna.
10. Naj bosta H in K dve (ne nujno različni) podgrupi končne grupe G. Za $x \in G$ je $|HxK| = \frac{|H|\,|K|}{|(x^{-1}Hx) \cap K|}$.
11. **(Frobenius).** Če sta H in K dve (ne nujno različni) podgrupi končne grupe G, potem je $|G| = \sum \frac{|H|\,|K|}{|(x^{-1}Hx) \cap K|}$ kjer vsota (na desni strani) teče po elementih x, ki so predstavniki dvojnih odsekov HyK.