UNIVERZA NA PRIMORSKEM
Fakulteta za matematiko, naravoslovje in informacijske tehnologije

Matematika – 1. stopnja

Luca Basiaco

p-Sylowke končnih simetričnih grup

Zaključna naloga

Koper, september 2012

Mentor: izr. prof. dr. István Kovács

Povzetek

Glavni in najbolj pomemben cilj zaključne naloge je konstruirati p-Slowke končnih simetričnih grup (kjer je p praštevilo) s pomočjo venčnih produktov. Soočili se bomo tudi z različnimi koncepti s področja permutacijskih grup, kot naprimer tranzitivnost, regularnost, semidirektni produkt, izreki Sylowa, itd.

Zaključna naloga je sestavljena iz petih poglavij. Prvo poglavje je namenjeno uvodu zaključne naloge, kjer preučujemo temeljne pojme teorije permutacijskih grup. V drugem in tretjem poglavju bomo analizirali semidirektni in venčni produkt. Četrto poglavje bo namenjeno konstrukciji p-Sylowk končnih simetricnih grup. V zadnjem poglavju pa bomo spoznali aplikacijo venčnega produkta na grafih. Dotaknili se bomo tako pomembnega koncepta algebraične teorije grafov.

Abstract

The main goal of the thesis is to construct Sylow p-subgroups of finite symmetric groups (where p is a prime number) with the aid of wreath products. Different concepts of permutation group theory, like transitivity, regularity, semidirect product, Sylow theorems, etc., will be of fundamental importance in the thesis.

The thesis is divided in five chapters. The first chapter starts with a short introduction, and then we review all the concepts of permutation group theory which will be used later. In the second and the third chapters we will focus on semidirect and wreath products, respectively. In the fourth chapter we will develop the construction of Sylow p-subgroups of finite symmetric groups. In the last chapter we also present an application of the wreath product construction in graph theory.

Math. Subj. Class. (2010): 20B30, 20B35, 20B25, 05E18.

Ključne besede: p-Sylowka, simetrična grupa, semidirektni produkt, venčni produkt, leksikografski produkt grafov.

Keywords: Sylow p-subgroup, symmetric group, semidirekt product, wreath product, lexicographic product of graphs.

Zahvala

Iskreno se zahvaljujem mentorju dr. Istvánu Kovácsu za pomoč in za nasvete, ki mi je nudil pri realizaciji zaključne naloge, ter za potrpežljivost.

Iskrena hvala tudi profesorici Elen Zrinski, ki mi je pomagala pri lektoriranju diplome.

Zaključno nalogo posvečam mojim nonam, Marii Basiaco in Gasparini Zahtila.

Kazalo

Slike

Tabele

Poglavje 1

Uvod

Leta 1872 je Ludwig Sylow odkril naslednjo zanimivo lastnost o končnih grupah: za vsako grupo G obstaja takšna podgrupa H, moči p^m (kjer je p praštevilo in m naravno število), tako, da $p^m \mid |G|$ in $p^{m+1} \nmid |G|$. Podgrupa H se imenuje *p-Sylowka* grupe G. Sylow je odkril veliko lastnosti glede teh podgrup. Imenujejo se izreki Sylowa in so ključnega pomena v teoriji končnih grup.

V splošnem, ko nekdo preučuje končno grupo G (ali razrede končnih grup), je bistvenega pomena obravnava Sylowe p-podgrupe. Ta je namreč eden od osrednjih problemov v algoritmični teoriji grup (glej [7]). Znano je, da lahko p-Sylowke permutacijskih grup najdemo v polinomskem času (glej [1]). V naši zaključni nalogi bomo obravnavali ta problem za poseben razred grup, imenovan *Simetrične grupe* S_n t.j. grupa vseh permutacij množice $\{1, 2, \ldots, n\}$. Naš glavni cilj bo rešiti naslednjo nalogo:

> Za vsako število $n > 1$ najdite generatorsko množico p-Sylowke končne simetrične grupe S_n.

Struktura p-Sylowk končnih simetričnih grup je prišla v javnost pred skoraj 100 leti. V obdobju od leta 1940 do leta 1950 je veliko matematikov z neposrednim pristopom obravnavalo te posebne grupe s pomočjo tako imenovanega *venčnega produkta* permutacijskih grup, glej [5, 6, 10].

V tretjem poglavju bomo predstavili operacijo venčnega produkta in s tem namenom bomo sledili knjigi [2]. Definirali bomo venčni produkt dveh grup kot poseben primer semidirektnega produkta (Poglavje 2). Obravnavana vsebina Poglavja 2 in 3 bo sledila vsebini [2, Poglavje 2.5] oziroma [2, Poglavje 2.6]. Rešili bomo določene zanimive naloge, ter ustvarili naše primere z namenom, da bi pojasnili teorijo.
Dodali bomo tudi opombo (Posledica 3.7), kjer obravnavamo generatorje venčnega produkta, ki pa niso bili eksplicitno omenjeni v [2]. V 4. Poglavju bomo aplicirali koncepte, ki smo jih razvili v 2. in 3. poglavju z namenom,

da bi zgradili generatorje p-Sylowk končnih simetričnih grup in tako dosegli glavni cilj zaključne naloge.

Polek velike pomembnosti v teoriji grup, bo venčni produkt oz. njegova konstrukcija prikazana tudi v teoriji grafov. Močno je povezana s tako imenovanim *leksikografskim produktom* grafov. V zadnjem poglavju se bomo dotaknili te povezave in na kratko povzeli članek Sabidussija [9].

V ostalem delu uvoda se bomo seznanili z vsemi pojmi, ki jih bomo uporabili v glavni konstrukciji. Uporabili smo literaturo [2–4, 8].

1.1 Delovanje grupe

V tem podpoglavju bomo definirali delovanje grupe.

Definicija 1.1. Delovanje grupe G na neprazni množici X je preslikava $\mu : X \times G \to X$, ki zadošča naslednjim lastnostim, kjer z x^g označimo sliko $\mu((x, g))$ elementa $(x, g) \in X \times G$:

(i) $x^{1_G} = x$ za vsak $x \in X$, kjer je 1_G identiteta grupe G;

(ii) $x^{g_1 g_2} = (x^{g_1})^{g_2}$ za vsak $x \in X$ in vsak g_1, $g_2 \in G$.

Definicija 1.2. Slika delovanja grupe G na množici X je podgrupa v grupi $\mathrm{Sym}(X)$, ki jo sestavljajo permutacije π_g, $g \in G$, kjer je

$$\pi_g : x \mapsto x^g \quad \text{za vsak } x \in X.$$

Trditev 1.3. *Preslikava*

$$\pi : G \to \mathrm{Sym}(X)$$

$$\pi : g \mapsto \pi_g$$

je homomorfizem, kjer je π_g permutacija v grupi $\mathrm{Sym}(X)$*, ki je definirana v Definiciji 1.2.*

Dokaz. Naj bosta $g_1, g_2 \in G$. Permutacija $\pi(g_1)$ preslika element $\omega \in \Omega$ v element ω^{g_1}, ki ga permutacija $\pi(g_2)$ preslika v $(x^{g_1})^{g_2}$. Torej je

$$\pi(g_1)\pi(g_2) : x \mapsto (x^{g_1})^{g_2}.$$

Sedaj je, zaradi drugega aksioma v Definiciji 1.1, $(x^{g_1})^{g_2}$ enak $x^{g_1 g_2}$, ki pa je slika permutacije $\pi(g_1 g_2)$. Dobimo, da je $\pi(g_1)\pi(g_2) = \pi(g_1 g_2)$, torej, π je homomorfizem iz G v S_X. □

Definicija 1.4. Jedro delovanja G na X je edinka v G, ki je definirana takole:

$$\{g \in G : x^g = x \quad za\ vsak\ x \in X\}.$$

Pravimo, da je delovanje *zvesto*, če je njegovo jedro trivialno.

1.2 Regularnost in primitivnost

V tem podpoglavju se bomo osredotočili na dva osnovna pojma teorije permutacijskih grup: *regularnost* in *primitivnost*. Za množico X, nad katero deluje grupa G, bomo uporabili tudi izraz *G-prostor*.

Definicija 1.5. Grupa G deluje na množici X *tranzitivno* (oziroma je X tranzitiven G-prostor), če za vsak par elementov $x, y \in X$ obstaja element $g \in G$, da velja $x^g = y$.

Definicija 1.6. Grupa G deluje na množici X *polregularno* (oziroma je X polregularen G-prostor), če je G_x trivialen za vsak $x \in X$.

Primer 1.7. Naj bo $G = S_5$ in naj bo $X = \{1, 2, 3, 4, 5\}$. Grupa G ne deluje na množici X polregularno, saj obstaja permutacija, naprimer (1234), za katero velja $(1234) \in G_5$. To pomeni, da G_5 ne more biti trivialen. Delovanje je tranzitivno.

$\Diamond$

Definicija 1.8. Delovanje imenujemo *regularno*, če je hkrati tranzitivno in polregularno.

Definicija 1.9. Podmnožica B tranzitivnega G-prostora X je *blok*, če velja

$$B^g = B \text{ ali } B^g \cap B = \emptyset \text{ za vsak } g \in G.$$

če je B blok, potem vse podmnožice B^g za $g \in G$ tvorijo particijo množice X. To particijo imenujemo *sistem blokov*.

Opomba 1.10. Naj bo X tranzitiven G-prostor. Očitno je, da so množice v obliki $\{x\}$, kjer $x \in X$, in cela množica X vedno bloki. Te bloke imenujemo *trivialni bloki*.

Primer 1.11. Dokažimo, da ima ciklična grupa $G = \langle(123456)\rangle$, kjer je $G \leqslant S_6$, natanko 5 netrivialnih blokov. Vemo, da $|B| \mid |G|$. Torej, bloki bodo moči ali 2 ali 3. Opazimo, da je množica $\{1, 4\}$ blok. Ostale bloke $\{2, 5\}$ in $\{3, 6\}$ dobimo z delovanjem grupe G na množici $\Omega = \{1, 2, 3, 4, 5, 6\}$. Isti postopek uporabimo za blok $\{1, 3, 5\}$ in tako dobimo $\{2, 4, 6\}$.

$\Diamond$

Definicija 1.12. Grupa G deluje na množici X *primitivno*, če je delovanje tranzitivno in ima G-prostor X samo trivialne bloke.

Trditev 1.13. (glej [2, Exercise 2.5.6]) *Naj bo K regularna podgrupa grupe* $\mathrm{Sym}(\Omega)$ *in naj bo C centralizator grupe K v* $\mathrm{Sym}(\Omega)$. *Potem je C regularna podgrupa izomorfna grupi K.*

Dokaz. Naj bo ω_0 točka v Ω. Potem definirajmo preslikavo f iz grupe K v množico Ω kot:

$$f:\ k \mapsto \omega_0^k. \tag{1.1}$$

Opazimo, da je f bikektivna.

Za vsak $x \in K$ definirajmo preslikavo $\bar{x}$ iz Ω v Ω kot:

$$\bar{x}:\ \omega \mapsto f(x^{-1}f^{-1}(\omega)).$$

Preslikava $\bar{x}$ je bijektivna in preslikava

$$\begin{aligned} \phi &: K \to \mathrm{Sym}(\Omega) \\ \phi &: x \mapsto \bar{x} \end{aligned}$$

je homomorfizem iz grupe K v grupo $\mathrm{Sym}(\Omega)$. Očitno je, da je preslikava $\psi:\ K \to K$, $k \mapsto x^{-1}k$ bijektivna. Sledi, da lahko $\bar{x}$ zapišemo kot kompozicijo treh bijektivnih preslikav: $\bar{x} = f \circ \psi \circ f^{-1}$ in se tako prepričamo, da je $\bar{x}$ tudi bijektivna.

Dokazati moramo nato, da velja, da za vsaka elementa $x, y \in K$ in vsak $\omega \in \Omega$:

$$\omega^{\overline{xy}} = \omega^{\bar{x}\cdot\bar{y}} \tag{1.2}$$

Levo stran lahko zapišemo kot $f((xy)^{-1}f^{-1}(\omega)) = f(y^{-1}x^{-1}f^{-1}(\omega))$. Desno stran pa lahko zapišemo kot

$$(\omega^{\bar{x}})^{\bar{y}} = f(y^{-1}f^{-1}(\omega^{\bar{x}})) = f(y^{-1}f^{-1}[f(x^{-1}f^{-1}(\omega))]) = f(y^{-1}x^{-1}f^{-1}(\omega)).$$

Sledi, da je enačba (1.2) dokazana.

Pomembno je opaziti, da, če je $x \in K$ in $\omega_0^{\bar{x}} = \omega_0$, potem je $x = 1_K$. Iz definicije (1.1) za f sledi, da je $f^{-1}(\omega_0) = 1_K$. Sledi, da je $\omega_0^{\bar{x}} = f(x^{-1}f^{-1}(\omega_0)) = f(x^{-1}1_K) = f(x^{-1}) = \omega_0^{x^{-1}}$. Torej, če velja, da $\omega_0^{\bar{x}} = \omega_0$, potem je $\omega_0^{x^{-1}} = \omega_0$ oziroma je $x = 1_K$.

Naj bo $\overline{K} = \phi(K)$. Ker vemo, da, če je $x \in K$ in $\omega_0^{\bar{x}} = \omega_0$, potem je $x = 1_K$, lahko trdimo, da je slika $\phi(K)$ izomorfna grupi K.

Dokažimo sedaj, da je grupa $\overline{K}$ regularna. Če ponovimo še enkrat, vemo, da če je $x \in K$ in $\omega_0^{\bar{x}} = \omega_0$, potem je $x = 1_K$. Sledi, da je stabilizator $\overline{K}_{\omega_0}$ trivialen. Po *lemi orbita-stabilizator* je

$$|\overline{K}| = |\omega_0^{\overline{K}}| \cdot |\overline{K}_{\omega_0}| = |\omega_0^{\overline{K}}|.$$

Ker je $\overline{K} \cong K$, potem je $|\overline{K}| = |K| = |\Omega|$, saj je K regularna. Dobimo, da je orbita $\omega_0^{\overline{K}} = \Omega$. Sledi, da je $\overline{K}$ tranzitivna moči $|\Omega|$. Opazimo tako, da je $\overline{K}$ regularna.

Dokažimo sedaj, da velja $\overline{K} \leq C$. Naj bo $\omega \in \Omega$. Potem velja, da $\omega = \omega_0^k$ za nek $k \in K$. Sledi, da za vsaka elementa $x \in K$ in $\bar{y} \in \overline{K}$:

$$\begin{aligned} \omega^{x\bar{y}} &= f(y^{-1}f^{-1}(\omega_0^{kx})) = f(y^{-1}kx) = \omega_0^{y^{-1}kx}, \\ \omega^{\bar{y}x} &= [f(y^{-1}f^{-1}(\omega_0^k))]^x = (f(y^{-1}k))^x = \omega_0^{y^{-1}kx}. \end{aligned}$$

V naslednjem koraku bomo dokazali, da je $\overline{K} = C$.

Kot prva stvar, dokažimo, da je C polregularna. Naj bo $c \in C_{\omega_0}$ in naj bo $\omega \in \Omega$. Obstaja potem takšen $x \in K$, da velja $\omega = \omega_0^k$. če nadaljujemo je $\omega^c = \omega_0^{kc} = \omega_0^{ck} = \omega_0^k = \omega$. Ker je bil ω poljuben element v Ω, $\omega^c = \omega$ za vsak $\omega \in \Omega$, potem je $c = 1_K$ in stabilizator C_{ω_0} je trivialen. To pomeni, da je C polregularna grupa.

Sedaj imamo enakost:

$$|C| = |\omega_0^C| \cdot |C_{\omega_0}| \leq |\omega_0^C| = |\Omega| = |\overline{K}|.$$

Dokazali smo, da je $\overline{K} \leq C$, sedaj pa lahko trdimo, da je $\overline{K} = C$. □

1.3 Izreki Sylowa

Navedimo izreke Sylowa brez dokaza.

Izrek 1.14 (1. izrek Sylowa)**.** *Naj bo G končna grupa, $|G| = p^n m$, kjer je p praštevilo, $n, m \in \mathbb{N}$ in $p \nmid m$. Potem v grupi G obstaja podgrupa H moči p^i za vsak $i = 0, 1, 2, 3, \ldots, n$.*

Definicija 1.15. Naj bo G končna grupa, $|G| = p^n m$, kjer je p praštevilo, $n, m \in \mathbb{N}$ in $p \nmid m$. Podgrupa grupe G moči p^n je Sylowa p-podgrupa grupe G oziroma p-Sylowka.

Izrek 1.16 (2. izrek Sylowa)**.** *Naj bo G končna grupa, $|G| = p^n m$, kjer je p praštevilo, $n, m \in \mathbb{N}$ in $p \nmid m$. Naj bosta P_1 in P_2 podgrupi grupe G moči p^n (torej p-Sylowki). Potem obstaja $g \in G$, za katerega velja*

$$P_2 = g^{-1}P_1 g$$

Izrek 1.17 (3. izrek Sylowa)**.** *Naj bo G končna grupa, $|G| = p^n m$, kjer je p praštevilo, $n, m \in \mathbb{N}$ in $p \nmid m$. Naj bo l število vseh p-Sylowk grupe G. Potem $l \equiv 1 (mod\ p)$ in $l \mid |G|$.*

Poglavje 2

Semidirektni produkti

V tem poglavju bomo vpeljali koncept semidireknega produkta, ki bo bistvenega pomena v naslednjem poglavju. Obravnavana vsebina sledi poglavju [2, Section 2.5].

Definicija 2.1. Naj bosta H in K grupi in naj delovanje grupe H na grupi K ohranja strukturo grupe K. Z drugimi besedami, za vsak $x \in H$ je preslikava $u \mapsto u^x$ avtomorfizem grupe K. Naj bo

$$G = \{(u, x) |\ u \in K, x \in H\}.$$

Definiramo produkt $\circ$ za množico G takole:

$$(u, x) \circ (v, y) = (uv^{x^{-1}}, xy)$$

za vsak $(u, x), (v, y) \in G$.

Trditev 2.2. *$(G, \circ)$ je grupa.*

Dokaz. Očitno je, da je produkt $\circ$ zaprta operacija. Kot opazimo v Definiciji 2.1 je $uv^{x^{-1}} \in K$ in $xy \in H$. Preverimo asociativnost.

$$\begin{aligned} ((u, x) \circ (v, y)) \circ (w, z) &= (uv^{x^{-1}}, xy) \circ (w, z) \\ &= (uv^{x^{-1}} w^{(xy)^{-1}}, xyz) \end{aligned}$$

za vsak $(u, x), (v, y), (w, z) \in G$.

$$\begin{aligned} (u, x) \circ ((v, y) \circ (w, z)) &= (u, x) \circ (vw^{y^{-1}}, yz) \\ &= (u(vw^{y^{-1}})^{x^{-1}}, xyz) \\ &= (uv^{x^{-1}} w^{(xy)^{-1}}, xyz) \end{aligned}$$

za vsak $(u, x), (v, y), (w, z) \in G$.

Preverimo sedaj, da obstaja nevtralni element. Privzemimo, da je ta $(1_K, 1_H)$, kjer sta 1_K in 1_H nevtralna elementa v K oziroma H. Velja, da za vsak $(v, y) \in G$:

$$(1_K, 1_H) \circ (v, y) = (1_K v^{1_H}, 1_H y) = (v, y),$$

in

$$(v, y) \circ (1_K, 1_H) = (v 1_K^{y^{-1}}, y 1_H) = (v, y).$$

Torej je res $(1_K, 1_H)$ nevtralni element. Preveriti moramo še obstoj inverznega elementa za vsak $(u, x) \in G$.

$$\begin{aligned} (1_K, 1_H) &= (u, x) \circ (o, p) \\ &= (o, p) \circ (u, x) \\ &= (o u^{p^{-1}}, px) \end{aligned}$$

Opazimo, da je $p = x^{-1}$ in, da je $o = (u^x)^{-1}$. Sledi, da je $(u, x)^{-1} = ((u^x)^{-1}, x^{-1})$, za vsak $(u, x) \in G$. □

Definicija 2.3. Grupa $(G, \circ)$ je *semidirektni (poldirektni) produkt* grupe K z grupo H. Notacija je $K \rtimes H$.

Opomba 2.4. Očitno je, da velja $|K \rtimes H| = |K||H|$. Semidiretni produkt je implicitno odvisen od delovanja grupe H na grupi K. V posebnem primeru, ko avtomorfizem zadošča $u^x = u$ za vsak element $x \in H$, dobimo, da je $K \rtimes H$ enak navadnemu direktnemu produktu $K \times H$.

Trditev 2.5. *Naj bosta* $H^* = \{(1_K, x) \mid x \in H\}$ *in* $K^* = \{(u, 1_H) \mid u \in K\}$ *podgrupi v* G*, izomorfni grupi* H *oziroma grupi* K*. Potem je* $G = K^* H^*$ *in* $K^* \cap H^* = \{(1_K, 1_H)\}$.

Dokaz. Pokazati moramo najprej, da je $(u, v) = (u, 1_H) \circ (1_K, v)$ za vsak $(u, 1_H) \in K^*, (1_K, v) \in H^*$. Opazimo, da je $(u, 1_H) \circ (1_K, v) = (u 1_K^{1_H}, v) = (u, v)$.
Pokazati moramo nato, da je $K^* \cap H^* = \{(1_K, 1_H)\}$. Edini element v grupi G, ki obstaja hkrati in v grupi H^* in v grupi K^*, je element $(1_K, 1_H)$. □

Trditev 2.6. K^* *je edinka v* $(G, \circ)$.

Dokaz. Dokazati moramo, da velja naslednje:

$$K^* = g^{-1} K^* g$$

za vsak $g \in G$, oziroma

$$(i, j)^{-1} \circ (u, 1_H) \circ (i, j) \in K^*$$

za vsak $(i,j) \in G$ in za vsak $(u,1_H) \in K^*$.
Opazimo, da je

$$\begin{aligned}(i,j)^{-1} \circ (u,1_H) \circ (i,j) &= ((i^j)^{-1}, j^{-1}) \circ (ui, j) \\ &= ((i^j)^{-1}(ui)^j, 1_H) \\ &= ((i^j)^{-1}u^j i^j, 1_H).\end{aligned}$$

Sledi, da je $K^* \triangleleft G$. □

Opomba 2.7. Način delovanja grupe H^* na grupi K^* s konjugiranjem se izraža kot v prvotnem delovanju grupe H na grupi K (glej Definicijo 2.1). Namreč

$$\begin{aligned}(1_K,x)^{-1} \circ (u,1_H) \circ (1_K,x) &= (1_K, x^{-1}) \circ (u,x) \\ &= (u^x, 1_H)\end{aligned}$$

za vsak $x \in H$ in $u \in K$.

Trditev 2.8. *Naj bo G grupa, $K, H \leq G$, $K \triangleleft G$, $G = KH$ in $K \cap H = \{1_G\}$, kjer je 1_G nevtralni element grupe G. Potem je $G \cong K \rtimes H$, kjer H deluje na grupi K s konjugiranjem.*

Dokaz. Najprej moramo dokazati, da obstaja homomorfizem iz grupe $K \rtimes H$ v grupo G. Torej, veljati mora $f(ab) = f(a)f(b)$, za vsak $a, b \in K \rtimes H$. V našem primeru naj bo $f((u,x)) = ux$, za vsak $(u,x) \in K \rtimes H$.

$$\begin{aligned}f((u,x)(v,y)) &= f((uv^{x^{-1}}, xy)) \\ &= uv^{x^{-1}}xy \\ &= uxvx^{-1}xy \\ &= uxvy,\end{aligned}$$

$$f((u,x))f((v,y)) = uxvy,$$

za vsak $(u,x),(v,y) \in K \rtimes H$.
Dokažimo sedaj, da je homomorfizem f bijektivna funkcija iz grupe $K \rtimes H$ v grupo G. Najprej pokažimo, da je homomorfizem f injektivni. Veljati mora, da za vsak $(a,b),(c,d) \in K \rtimes H$: $f((a,b)) = f((c,d)) \Rightarrow (a,b) = (c,d)$.

Predpostavimo, da je $f((a,b)) = f((c,d))$. Od tod je $ab = cd$. Dobimo tako element $x = c^{-1}a = db^{-1}$, za katerega velja, da $x \in K \cap H$. To je res, ker sta $a, c \in K$ in $b, d \in H$. Z uporabo predpostavke $K \cap H = \{1_G\}$ dobimo, da je $x = 1_G$, tj. $(a,b) = (c,d)$.
Preslikava f je surjektivna, saj $f((u,x)) = ux$. Namreč, iz Trditve 2.8 opazimo, da je $G = KH$, za vsak $(u,x) \in K \rtimes H$. □

Opomba 2.9. Grupo G imenujemo *razpadna razširitev* grupe K z grupo H.

Poglavje 3

Venčni produkti

V tem poglavju bomo vpeljali koncept venčnega produkta, ki bo bistvenega pomena za konstrukcijo p-Sylowke končnih simetričnih grup v naslednjem poglavju. Obravnavana vsebina sledi poglavju [2, Section 2.6].

Naj bosta X in Y neprazni množici. S $\mathrm{Fun}(\Gamma, K)$ bomo označili množico vseh funkcij iz X v Y.

Trditev 3.1. *Naj bo Γ neprazna množica in naj bo K grupa. Potem je $\mathrm{Fun}(\Gamma, K)$ grupa s sledečo operacijo:*

$$(fg)(\gamma) = f(\gamma)g(\gamma)$$

za vsak $f, g \in \mathrm{Fun}(\Gamma, K)$ in $\gamma \in \Gamma$.

Dokaz. Očitno je, da je $\mathrm{Fun}(\Gamma, K)$ neprazna in da je zaprta za zgoraj navedeno operacijo. Preverimo asociativnost. Velja namreč, da je

$$(f(\gamma)g(\gamma))h(\gamma) \quad = \quad f(\gamma)(g(\gamma)h(\gamma))$$

za vsak $f, g, h \in \mathrm{Fun}(\Gamma, K)$ in za vsak $\gamma \in \Gamma$, saj je K grupa. Preverimo obstoj nevtralnega elementa. Veljati mora namreč, da za vsak $f \in \mathrm{Fun}(\Gamma, K)$ $fe = ef = f$, kjer je e nevtralni element.

$$\begin{aligned} f(\gamma) &= ef(\gamma) \\ &= fe(\gamma) \\ &= f(\gamma)e(\gamma) \end{aligned}$$

za vsak $f \in \mathrm{Fun}(\Gamma, K), \gamma \in \Gamma$. Opazimo, da je $1_K = e(\gamma)$, za vsak $\gamma \in \Gamma$. Dokazati moramo še, da za vsako funkcijo $f \in \mathrm{Fun}(\Gamma, K)$ obstaja $f^{-1} \in \mathrm{Fun}(\Gamma, K)$.

$$\begin{aligned} e(\gamma) &= gf(\gamma) = fg(\gamma) \\ 1_K &= g(\gamma)f(\gamma) = f(\gamma)g(\gamma) \end{aligned}$$

za vsak $\gamma \in \Gamma$, $f \in \mathrm{Fun}(\Gamma, K)$. Ker vemo, da je K grupa, opazimo, da je $g = f^{-1}$. □

Trditev 3.2. *Naj bo K grupa in Γ končna množica moči m, $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$. Potem je grupa $\mathrm{Fun}(\Gamma, K)$ izomorfna direktnemu produktu K^m z izomorfizmom $f \mapsto (f(\gamma_1), \ldots, f(\gamma_m))$.*

Dokaz. Najprej preverimo, da je preslikava $\mu : f \mapsto (f(\gamma_1), \ldots, f(\gamma_m))$ homomorfizem. Veljati mora, da $\mu(fg) = \mu(f)\mu(g)$, za vsak $f, g \in \mathrm{Fun}(\Gamma, K)$.

$$\begin{aligned} \mu(fg) &= ((fg)(\gamma_1), \ldots, (fg)(\gamma_m)) \\ &= (f(\gamma_1)g(\gamma_1), \ldots, f(\gamma_m)g(\gamma_m)) \end{aligned}$$

$$\begin{aligned} \mu(f)\mu(g) &= (f(\gamma_1), \ldots, f(\gamma_m))(g(\gamma_1), \ldots, g(\gamma_m)) \\ &= (f(\gamma_1)g(\gamma_1), \ldots, f(\gamma_m)g(\gamma_m)) \end{aligned}$$

za vsak $f, g \in \mathrm{Fun}(\Gamma, K)$. Preverimo še bijektivnost oziroma injektivnost in surjektivnost. Naj bodo $\mu(f) = \mu(g)$, za nek $f, g \in \mathrm{Fun}(\Gamma, K)$. Preveriti moramo, da je $f = g$.

$$\begin{aligned} \mu(f) &= \mu(g) \\ \mu(f)\mu(g^{-1}) &= \mu(e) \\ \mu(fg^{-1}) &= \mu(e) \\ fg^{-1} &= e \\ f &= g, \end{aligned}$$

kjer je e nevtralni element grupe $\mathrm{Fun}(\Gamma, K)$. Opazimo, da za vsak element od K^m obstaja element v $\mathrm{Fun}(\Gamma, K)$. Velja surjektivnost in tako bijektivnost. □

Trditev 3.3. *Naj bosta K, H grupi in naj H deluje na neprazni množici Γ. Potem H deluje na grupi $\mathrm{Fun}(\Gamma, K)$ takole:*

$$f^x(\gamma) = f(\gamma^{x^{-1}}) \quad \text{za vsak } f \in \mathrm{Fun}(\Gamma, K), \gamma \in \Gamma \text{ in } x \in H. \tag{3.1}$$

Dokaz. Preveriti moramo aksioma (i) in (ii) v Definiciji 1.1.

(i): $f^{1_H}(\gamma) = f(\gamma^{1_H}) = f(\gamma)$ za vsak $f \in \mathrm{Fun}\,(\Gamma, K)$ in $\gamma \in \Gamma$,

(ii): $f^{h_1h_2}(\gamma) = f(\gamma^{(h_1h_2)^{-1}}) = f(\gamma^{(h_2^{-1}h_1^{-1})}) = f((\gamma^{h_2^{-1}})^{h_1^{-1}}) = f^{h_1}(\gamma^{h_2^{-1}}) = (f^{h_1})^{h_2}(\gamma)$ za vsak $f \in \mathrm{Fun}(\Gamma, K), \gamma \in \Gamma$ in vsaka $h_1, h_2 \in H$.

□

Očitno je, da je zgornje delovanje grupe H na grupi $\mathrm{Fun}(\Gamma, K)$ ohranja strukturo grupe $\mathrm{Fun}(\Gamma, K)$. Sedaj lahko vpeljemo najbolj pomembno definicijo zaključne naloge.

Definicija 3.4. Naj bosta K, H grupi in naj H deluje na neprazni množici Γ. *Venčni produkt* grupe K z grupo H, z oznako $K \text{ wr}_\Gamma H$, je semidirektni produkt

$$K \text{ wr}_\Gamma H = \text{Fun}(\Gamma, K) \rtimes H,$$

definiran z delovanjem (3.1).

Po Trditvi 2.5 lahko definiramo grupi:

$$H^* = \{(e, x) | x \in H\} \text{ in } \text{Fun}(\Gamma, K)^* = \{(f, 1_H) | f \in \text{Fun}(K, \Gamma)\}.$$

Podgrupo $\text{Fun}(\Gamma, K)^*$ imenujemo *bazna grupa* venčnega produkta $K \text{ wr}_\Gamma H$. Označimo jo tudi z B.

Opomba 3.5. Pomembno je opaziti naslednje. Če je Γ končna množica, $\Gamma = \{1, \ldots, m\}$, potem po Trditvi 3.2 bazno grupo B venčnega produkta grupe K z grupo H identificiramo z direktnim produktom $K \times \ldots \times K$ (m krat). Delovanje grupe H nad B ustreza permutaciji komponent:

$$(u_1, \ldots, u_m)^x = (u_{1'}, \ldots, u_{m'}) \text{ kjer } x = \begin{pmatrix} 1 & \ldots & m \\ 1' & \ldots & m' \end{pmatrix},$$

za vsak $(u_1, \ldots, u_m) \in B$ in $x \in H$.

Posledica 3.6. *Če je Γ končna množica, $\Gamma = \{1, \ldots, m\}$ in obstaja $K \text{ wr}_\Gamma H$, potem je*

$$|K \text{ wr}_\Gamma H| = |K|^m \cdot |H|.$$

Dokaz. Po Definiciji 3.4 je $|K \text{ wr}_\Gamma H| = |\text{Fun}(\Gamma, K) \rtimes H|$. Zaradi Opombe 2.4 sklepamo, da je $|\text{Fun}(\Gamma, K) \rtimes H| = |\text{Fun}(\Gamma, K)| \cdot |H|$. Iz Trditve 3.2 sklepamo, da je $|\text{Fun}(\Gamma, K)| \cdot |H| = |K|^m \cdot |H|$. □

Posledica 3.7. *Če elementi $h_1, \ldots, h_r$ generirajo grupo H ter elementi $k_1, \ldots, k_s$ generirajo grupo K, H deluje na množici Γ tranzitivno in obstaja $K \text{ wr}_\Gamma H$, potem elementi*

$$(e, h_1), \ldots, (e, h_r), (f_1, 1_H), \ldots, (f_s, 1_H)$$

generirajo $K \text{ wr}_\Gamma H$. Funkcija f_i ($i \in \{1, \ldots, s\}$) je definirana na sledečem načinu; $f_i(\gamma) = k_i$ za $\gamma = \gamma_0$, sicer $f_i(\gamma) = 1_K$ za nek fiksiran element $\gamma_0 \in \Gamma$.

Pojasnimo zgornjo posledico v naslednjem primeru.

Primer 3.8. Naj bo $K = C_5$ in naj bo $H = \langle (a\,b\,c\,d\,e) \rangle$, ki deluje na $\Gamma = \{a, b, c, d, e\}$.

- Koliko je $|K \text{ wr}_\Gamma H|$?
- Poiščite generatorje grupe $K \text{ wr}_\Gamma H$.

Za lažje razumevanje snovi bomo v nadaljevanju z V označili venčni produkt $K \text{ wr}_\Gamma H$.

S pomočjo Posledice 3.6 izračunamo moč $|V|$:

$$|V| = |K \text{ wr}_\Gamma H| = |K|^{|\Gamma|} \cdot |H| = 5^5 \cdot 5 = 15625.$$

Generatorje bomo našli z uporabo Posledice 3.7. Opaziti moramo najprej, da permutacija $(a\,b\,c\,d\,e)$ generira grupo H. Očitno pa je tudi, da element $(1\,2\,3\,4\,5)$ generira grupo K. Zavedati se moramo nato, da H deluje na Γ tranzitivno. S pomočjo Posledice 3.7 dobimo dva generatorja za V, in sicer

$$\begin{aligned} v_1 &= (e, (a\,b\,c\,d\,e)), \\ v_2 &= (f, 1_H), \end{aligned}$$

kjer je e nevtralni element grupe $\text{Fun}(\Gamma, K)$, in je f definiran na sledeči način; $f(a) = f(b) = f(c) = f(d) = id$ in $f(e) = (12345)$.

$\Diamond$

V posebnem primeru, ko prva komponenta K venčnega produkta $K \text{ wr}_\Gamma H$ deluje na neki množici Δ, lahko definiramo delovanje grupe $K \text{ wr}_\Gamma H$ na množici $\Delta \times \Gamma$ takole:

$$(\delta, \gamma)^{(f,h)} = (\delta^{f(\gamma)}, \gamma^h) \tag{3.2}$$

za vsak par $(\delta, \gamma) \in \Delta \times \Gamma$ in za vsak element $(f, h) \in K \text{ wr}_\Gamma H$.

Da se prepričamo, da (3.2) res definira delovanje, moramo preveriti aksioma v Definiciji 1.1. Nevtralni element v $G = K \text{ wr}_\Gamma H$ je $1_G = (e, 1_H)$, kjer je e nevtralni element grupe $\text{Fun}(\Gamma, K)$, torej, $e(\gamma) = 1_K$ za vsak $\gamma \in \Gamma$.

Preverimo (i) aksiom:

$$(\delta, \gamma)^{1_G} = (\delta, \gamma)^{(e,1_H)} = (\delta^{e(\gamma)}, \gamma^{1_H}) = (\delta^{1_K}, \gamma) = (\delta, \gamma).$$

Sedaj preverimo (ii) aksiom:

$$\Big((\delta, \gamma)^{(f,h)}\Big)^{(g,k)} = \Big(\delta^{f(\gamma)}, \gamma^h\Big)^{(g,k)} = \Big((\delta^{f(\gamma)})^{g(\gamma^h)}, (\gamma^h)^k\Big) = \Big(\delta^{f(\gamma)g(\gamma^h)}, \gamma^{hk}\Big).$$

Vemo, da je po (3.1) $g(\gamma^h) = g^{h^{-1}}(\gamma)$, torej

$$\Big(\delta^{f(\gamma)g(\gamma^h)}, \gamma^{hk}\Big) = \Big(\delta^{f(\gamma)g^{h^{-1}}(\gamma)}, \gamma^{hk}\Big) = \Big(\delta^{fg^{h^{-1}}(\gamma)}, \gamma^{hk}\Big) = (\delta, \gamma)^{(fg^{h^{-1}}, hk)}.$$

Po Definiciji 2.1 pa je $(fg^{h^{-1}}, hk) = (f, h)(g, k)$ v grupi $G = K \text{ wr}_\Gamma H$. Sklepamo torej, da velja (ii) aksiom:

$$\Big((\delta, \gamma)^{(f,h)}\Big)^{(g,k)} = (\delta, \gamma)^{(f,h)(g,k)}.$$

Trditev 3.9. *Naj bosta K, H grupi in naj H deluje na neprazni množici Γ ter K na neprazni množici Δ. Če sta oba delovanja zvesta, potem venčni produkt $K \operatorname{wr}_\Gamma H$ deluje na $\Delta \times \Gamma$ zvesto.*

Dokaz. Naj bo $(\delta, \gamma) \in K \operatorname{wr}_\Gamma H$. Dokazati moramo, da še $(\delta, \gamma)^{(f,h)} = (\delta, \gamma)$ za vsak $(\delta, \gamma) \in \Delta \times \Gamma$, potem je $(f, h) = (e, 1_H)$.
Veljati mora, da $(\delta, \gamma)^{(f,h)} = (\delta^{f(\gamma)}, \gamma^h) = (\delta, \gamma)$. Sledi, da $\gamma^h = \gamma$ za vsak $\gamma \in \Gamma$. Ker H deluje zvesto na množici Γ, potem je $h = 1_H$. Veljati mora tudi, da $\delta^{f(\gamma)} = \delta$, za vsak $\delta \in \Delta$. Ker K deluje zvesto na Δ, je $f(\gamma) = 1_K$ za vsak $\gamma \in \Gamma$. Vemo, da edina funkcija, ki slika na takšen način, je $e \in \operatorname{Fun}(\Gamma, K)$. □

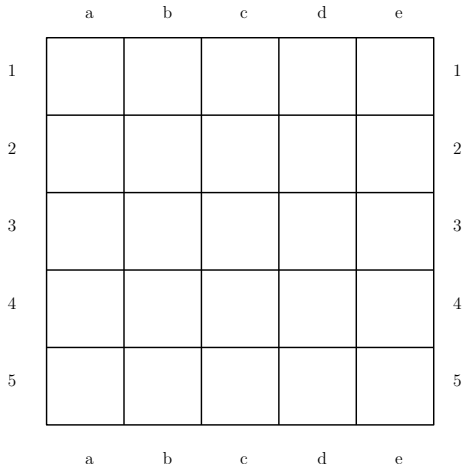
Opomba 3.10. Trditev 3.9 ima pomembno posledico. Namreč, če obstajata dve permutacijski grupi $K \leq \operatorname{Sym}(\Delta)$ in $H \leq \operatorname{Sym}(\Gamma)$, potem si lahko venčni produkt $K \operatorname{wr}_\Gamma H$ predstavljamo kot permutacijsko grupo množice $\Delta \times \Gamma$, ki deluje preko delovanja (3.2).

Primer 3.11 (Nadaljevanje Primera 3.8)**.** Naj bo $V = K \operatorname{wr}_\Gamma H$, kjer

$$K = \langle (12345) \rangle \text{ in } H = \langle (a\,b\,c\,d\,e) \rangle.$$

Naj K deluje na $\Delta = \{1, 2, 3, 4, 5\}$ in naj H deluje na $\Gamma = \{a, b, c, d, e\}$. V Primeru 3.8 smo že izračunali moč $|V| = 15625$.

Množico $\Delta \times \Gamma$ bomo predstavili s šahovnico velikosti 5×5 , glej sliko 3.1. Enotno polje, naprimer $(1, a)$ bomo zapisali na sledeči način: $1a$. Ker je K permutacijska grupa, si lahko zaradi Opombe 3.10 predstavljamo V kot permutacijsko grupo, ki permutira polja šahovnice.



Slika 3.1: Šahovnica 5×5.

Naprimer, naj bo $(f,h) \in V$, kjer sta $f \in \mathrm{Fun}(\Gamma, K)$ in $h \in S_5$ dana:

$$\begin{aligned} f &: a \mapsto (12345),\ b \mapsto (12345)^{-1},\ c \mapsto id,\ d \mapsto id,\ e \mapsto id; \\ h &= (ab). \end{aligned}$$

Katera permutacija od V pripada torej elementom (f,h)? Da najdejmo to permutacijo, moramo uporabiti delovanje (3.2). Sledi, da za $i \in \{1,2,3,4,5\}$ velja

$$ia^{(f,h)} = i^{f(a)}\, a^h = (i+1)b, \text{ in } (i+1)b^{(f,h)} = ia.^{1}$$

Očitno je, da (f,h) ne premakne vsakega polja ix, kjer je $x \in \{c,d,e\}$; in tako sklepamo, da je naša permutacija sledeča:

$$(1a\ 2b)(2a\ 3b)(3a\ 4b)(4a\ 5b)(5a\ 1b).$$

V nadaljevanju bomo dobljeno permutacijo identificirali z elementom (f,h), in označili $(f,h) = (1a\ 2b)(2a\ 3b)(3a\ 4b)(4a\ 5b)(5a\ 1b)$.

Iz drugega dela Primera 3.8 hitro opazimo, da je grupa V generirana z naslednjimi permutacijami:

$$\begin{aligned} v_1 &= \prod_{i=1}^{5} (ia\ ib\ ic\ id\ ie), \\ v_2 &= (1e\ 2e\ 3e\ 4e\ 5e). \end{aligned}$$

$\Diamond$

[1] Opaziti moramo, da računamo vrednost $i+1$ po modulu 5.

Poglavje 4

p-Sylowke končnih simetričnih grup

Naj bo S_n oznaka za simetrično grupo množice $\{1, 2, ..., n\}$, t. j.

$$S_n = \mathrm{Sym}(\{1, 2, ..., n\}).$$

V tem poglavju se bomo osredotočili na glavni cilj zaključne naloge, in sicer konstrukcijo p-Sylowke simetrične grupe S_n, za vsako praštevilo $p \leq n$.

Spomniti se moramo, da je moč p-Sylowke enaka največji potenci števila p, ki deli $|S_n| = n!$ (glej Definicijo 1.15). To potenco bomo izračunali v naslednji lemi.

Lema 4.1. (glej [2, Exercise 2.6.8]) *Naj bo n pozitivno celo število in p praštevilo. Naj bo*

$$n = n_0 + n_1 p + \ldots + n_k p^k \quad \text{kjer } 0 \leq n_i < p \text{ za vsak } i.$$

Potem največja potenca števila p, ki deli $n!$, je $p^{\nu(n)}$, kjer

$$\nu(n) = \sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor = n_1 + n_2 \frac{(p^2 - 1)}{(p - 1)} + \ldots + n_k \frac{(p^k - 1)}{(p - 1)} < \frac{n}{p - 1}$$

Dokaz. Število $n!$ lahko zapišemo kot

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot p \cdot \ldots \cdot 2p \cdot \ldots \cdot 3p \cdot \ldots \cdot n$$

Opazimo, da je število vseh števil, ki so deljiva s p $\left\lfloor \frac{n}{p} \right\rfloor$, p^2 $\left\lfloor \frac{n}{p^2} \right\rfloor$, $\ldots$, p^k $\left\lfloor \frac{n}{p^k} \right\rfloor$. Če seštejemo vse vrednosti, dobimo največjo potenco p^k, ki deli $n!$. Torej

$$\nu(n) = \sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Opazimo naslednje:

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{n_0 + n_1 p + \ldots + n_k p^k}{p} \right\rfloor +$$

$$+ \left\lfloor \frac{n_0 + n_1 p + \ldots + n_k p^k}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{n_0 + n_1 p + \ldots + n_k p^k}{p^k} \right\rfloor =$$

$$= \frac{n_1 p + \ldots + n_k p^k}{p} + \frac{n_2 p^2 + n_3 p^3 + \ldots + n_k p^k}{p^2} + \ldots + \frac{n_k p^k}{p^k}$$

Ulomki $\frac{n_0}{p}, \frac{n_0 + n_1 p}{p^2}, \ldots, \frac{n_0 + n_1 p + \ldots + n_{k-1} p^{k-1}}{p^k}$ so strogo manjši od 1 in večji ali enaki 0, zato smo jih izpustili. Če zapišemo drugače:

$$\begin{aligned} \nu(n) = \sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor &= n_1 + n_2 p + \ldots + n_k p^{k-1} + n_2 + n_3 p + \ldots + n_k p^{k-2} + \\ &\quad + \ldots + n_k \\ &= n_1 + n_2(p+1) + \ldots + n_k(p^{k-1} + p^{k-2} + \ldots + 1) \\ &= n_1 + n_2 \frac{(p^2-1)}{(p-1)} + \ldots + n_k \frac{(p^k-1)}{(p-1)} \end{aligned}$$

Pokažimo še, da je

$$n_1 + n_2 \frac{(p^2-1)}{(p-1)} + \ldots + n_k \frac{(p^k-1)}{(p-1)} < \frac{n}{p-1}$$

Vemo, da je

$$\frac{n}{p} + \frac{n}{p^2} + \ldots + \frac{n}{p^k} + \ldots$$

neskončna geometrijska vrsta. Lahko zapišemo vsoto kot

$$\frac{n}{p} \frac{1}{\left(1 - \frac{1}{p}\right)} = \frac{n}{p-1}$$

□

Glavni cilj zaključne naloge bomo dosegli v treh korakih. Naprej bomo konstruirali p-Sylowko za grupo S_{p^2}, nato za S_{p^m}, in na koncu za grupo S_n.

4.1 p-Sylowke grupe S_{p^2}

Začnimo z eno enostavno nalogo.

Naloga 4.2. Poiščite dve permutaciji, ki generirata 5-Sylowko grupe S_{25}.

Rešitev. Moč 5-Sylowke grupe S_{25} je $5^6 = 15625$ (glej Lemo 4.1). Opazimo, da je permutacijska grupa V v Primeru 3.8 reda 25 in moči 5^6. Sledi, da je V 5-Sylowka simetrične grupe množice $\{1a, 1b, \ldots, 5e\}$. S pomočjo grupe V lahko hitro dobimo 5-Sylowko za grupo S_{25}.

Najprej identificiramo šahovnico z množico $\{1, 2, \ldots, 25\}$, kot je prikazano na sliki 4.1.

	a	b	c	d	e	
1	1	2	3	4	5	1
2	6	7	8	9	10	2
3	11	12	13	14	15	3
4	16	17	18	19	20	4
5	21	22	23	24	25	5
	a	b	c	d	e	

Slika 4.1: Šahovnica velikosti 5×5 z označenimi polji.

Očitno je, da bosta elementa v_1 in v_2 iz V (glej Primer 3.11) pripadala sledečima permutacijama:

$$\begin{aligned} \pi_1 &= (5\ 10\ 15\ 20\ 25), \\ \pi_2 &= (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)(11\ 12\ 13\ 14\ 15)(16\ 17\ 18\ 19\ 20)(21\ 22\ 23\ 24\ 25). \end{aligned}$$

Torej je permutacijska grupa P, ki je generirana s π_1 in π_2 izomorfna grupi V. Kot vemo, je $|P| = |V| = 5^6$. Sledi, da sta π_1 in π_2 generatorja 5-Sylowke grupe S_{25}.

□

Lahko posplošimo zgornjo rešitev za poljuben p^2 tako, da imamo dva generatorja p-Sylowke grupe S_{p^2}.

Trditev 4.3. *Naj bo p pravštevilo. p-Sylowka grupe S_{p^2} je generirana s permutacijima π_1 in π_2, kjer sta*

$$\begin{aligned} \pi_1 &= (\,p\ 2p\ 3p\ \ldots\ p^2\,), \\ \pi_2 &= (1\ 2\ \ldots\ p)(\,(p+1)\ (p+2)\ \ldots\ 2p\,)\cdots(\,((p-1)p+1)\ ((p-1)p+2)\ \ldots\ p^2\,). \end{aligned}$$

4.2 p-Sylowke grupe S_{p^m}

Za pozitivno celo število m in pravštevilo p definiramo permutacijo σ_{p^m} v S_{p^m} takole

$$\sigma_{p^m} = (1\,2\,\ldots\,p)(\,(p{+}1)\;(p{+}2)\;\ldots\;2p\,)\cdots(\,(p^m{-}p{+}1)\;(p^m{-}p{+}2)\;\ldots\;p^m\,).$$

Naj bo k pozitivno celo število in naj bo $\pi \in S_n$, za katerega velja

$$\pi = (\,a_{11}\;\ldots\;a_{1l_1}\,)(\,a_{21}\;\ldots\;a_{2l_2}\,)\cdots(\,a_{c1}\;\ldots\;a_{cl_c}\,).$$

Definirajmo nato permutacijo $\pi^{[k]}$ iz S_{nk} na sledeči način:

$$\pi^{[k]} = (\,a_{11}k\;\ldots\;a_{1l_1}k\,)(\,a_{21}k\;\ldots\;a_{2l_2}k\,)\cdots(\,a_{c1}k\;\ldots\;a_{cl_c}k\,).$$

Definicija 4.4. Naj bo m pozitivno celo število in naj bo p praštevilo. Definirajmo torej permutacijsko grupo $P_{p^m} \leq S_{p^m}$ kot $P_{p^m} = \langle \pi : \pi \in M_{p^m} \rangle$, generatorsko množico M_{p^m} pa definirajmo rekurzivno:

- $M_p = \{\sigma_p\}$;
- če je $m > 1$, je $M_{p^m} = \{\pi^{[p]} : \pi \in M_{p^{m-1}}\} \cup \{\sigma_{p^m}\}$.

Primer 4.5. Ogledajmo si množice M_i, $i = 2, 4, 8, 16$, in pripadajoče grupe P_i. Elemente v M_i dobimo po zgornji definiciji, in sicer so dani v Tabeli 4.1.

i	elementi v M_i
2	(1 2)
4	(2 4), (1 2)(3 4)
8	(4 8), (2 4)(6 8), (1 2)(3 4)(5 6)(7 8)
16	(8 16), (4 8)(12 16), (2 4)(6 8)(10 12)(14 16) (1 2)(3 4)(5 6)(7 8)(9 10)(11 12)(13 14)(15 16)

Tabela 4.1: Generatorske množice M_i, $i = 2, 4, 8, 16$.

Prvi dve grupi, P_2 in P_4 je lahko opisati:

$$P_2 = \langle (12) \rangle = C_2 \quad \text{in} \quad P_4 = \langle (24), (12)(34) \rangle = D_8,$$

kjer je D_8 diederska grupa reda 4. Nato se hitro prepričamo, da je P_2 2-Sylowka grupe S_2 in da je P_4 2-Sylowka grupe S_4.

Lepo bi bilo, da bi P_8 in P_{16} bile 2-Sylowki grupe S_8 oziroma S_{16}. Izjava je namreč pravilna, vendar jo moramo dokazati v splošnem.

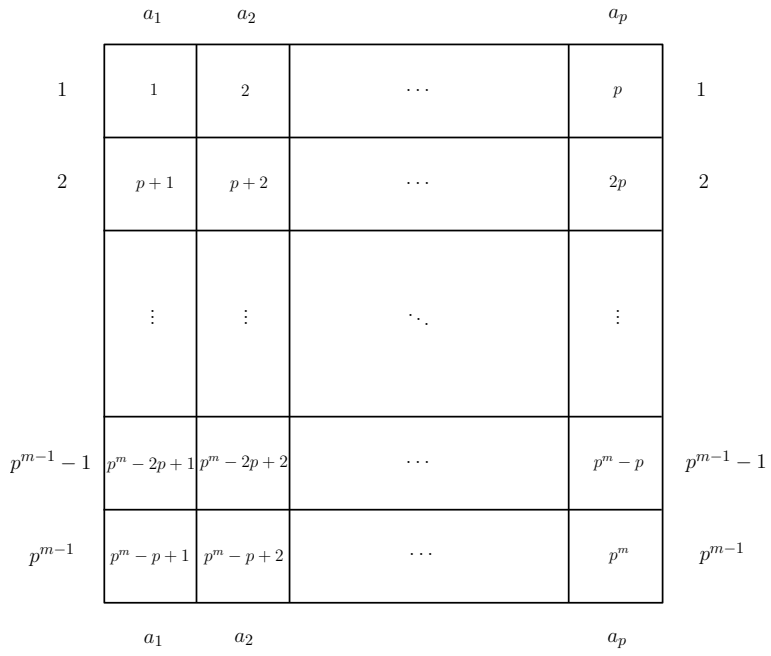
$\Diamond$

Trditev 4.6. *Grupa P_{p^m} je moči $p^{\mu(m)}$, kjer $\mu(m) = \dfrac{(p^m - 1)}{(p - 1)}$, torej je P_{p^m} p-Sylowka grupe S_{p^m}.*

Dokaz. Porazdelimo števila $1, 2, \ldots, p^m$ v tabeli velikosti $p^{m-1} \times p$ kot prikazano na sliki 4.2. Da se hitro dokazati, da je grupa P_{p^m} izomorfna venčnemu produktu:

$$P_{p^m} \cong P_{p^{m-1}} \operatorname{wr}_\Gamma C_p, \tag{4.1}$$

kjer je C_p generirana s permutacijo $(a_1\ a_2\ \ldots\ a_p)$, ki deluje na $\Gamma = \{a_1, \ldots, a_p\}$.



Slika 4.2: Tabela velikosti $p^{m-1} \times p$.

Trditev dokažemo z indukcijo. Najprej preverimo za $m = 1$. Dobimo naslednje: $|P_p| = p$, in torej je $\mu(1) = 1$.

Predpostavimo, da velja $\mu(m-1) = \dfrac{(p^{m-1}-1)}{(p-1)}$ za nek $m \geq 2$. Dokažimo, da trditev velja tudi za m. Iz (4.1) sledi, da je

$$p^{\mu(m)} = |P_{p^m}| = |P_{p^{m-1}}|^p \cdot p = p^{p\mu(m-1)+1}.$$

Torej je

$$\mu(m) = p\mu(m-1) + 1$$
$$\mu(m) = p\frac{(p^{m-1}-1)}{(p-1)} + 1$$
$$\mu(m) = \frac{(p^m-1)}{(p-1)}.$$

□

Opomba 4.7. Iz definicije generatorske množice M_{p^m} sledi neposredno, da je $|M_{p^m}| = m$. Torej je p-Sylowka P_{p^m} generirana z m permutacijami. Dobili smo tako rešitev naloge [2, Exercise 2.6.10].

4.3 p-Sylowke grupe S_n

p-Sylowko končnih simetričnih grup S_n lahko konstruiramo na sledeči način. Naj bo p praštevilo in n pozitivno celo število, za katerega velja $p \leq n$. Zapišimo n kot

$$n = n_0 + n_1 p + \ldots + n_k p^k \quad \text{kjer } 0 \leq n_i < p \text{ za vsak } i.$$

Potem iz Leme 4.1 sledi, da je p-Sylowka grupe S_n moči $p^{\nu(n)}$, kjer

$$\nu(n) = n_1 + n_2 \frac{(p^2-1)}{(p-1)} + \ldots + n_k \frac{(p^k-1)}{(p-1)}.$$

Sedaj iz množice $\{1, 2, \ldots, n\}$ ustvarimo particijo z n_0 razredov moči 1, n_1 razredov moči p, ... in n_k razredov moči p^k. Na vsak ustvarjen razred moči p^m, kjer $1 \leq m \leq k$, apliciramo konstrukcijo Definicije 4.4, da ustvarimo podgrupo moči $p^{\mu(m)}$ v S_n. Naj bo P direktni produkt vseh podgrup pridobljenih na takšen način. Podgrupa P je moči p^h, kjer

$$h = \sum n_m \mu(m) = \sum n_m \frac{(p^m-1)}{(p-1)} = \nu(n).$$

P je p-Sylowka grupe S_n.

Primer 4.8. (glej [2, Exercise 2.6.9]) Konstrukcija 2-Sylowke grupe S_{14}.

S pomočjo Leme 4.1 dobimo, da je moč 2-Sylowke simetrične grupe S_{14} enaka $2^{11} = 2048$.

Število 14 lahko zapišemo kot $14 = 2^3 + 2^2 + 2^1$. Opazimo torej, da lahko sestavimo particijo, ki bo vsebovala en razred moči 8, en razdred moči 4 in en rezred moči 2.

Particijo ustvarimo na sledeči način:

$$1\,2 \mid 3\,4\,5\,6 \mid 7\,8\,9\,10\,11\,12\,13\,14.$$

Na dobljene razrede apliciramo konstrukcijo Definicije 4.4.

$$P_2 = \langle (1\,2) \rangle,$$

$$P_4 = \langle (4\,6), (3\,4)(5\,6) \rangle \text{ in}$$

$$P_8 = \big\langle (10\,14), (8\,10)(12\,14), (7\,8)(9\,10)(11\,12)(13\,14) \big\rangle.$$

Direktni produkt od P_2, P_4 in P_8, t. j.

$$\big\langle (1\,2), (4\,6), (3\,4)(5\,6), (10\,14), (8\,10)(12\,14), (7\,8)(9\,10)(11\,12)(13\,14) \big\rangle$$

nam porodi 2-Sylowko grupe S_{14}.

$\Diamond$

Poglavje 5

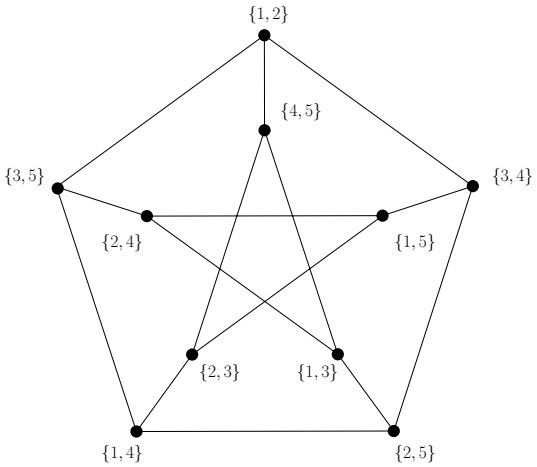
Venčni produkt v teoriji grafov

V tem poglavju bomo na kratko predstavili aplikacijo venčnega produkta v teoriji grafov. Večina vsebine tega poglavja je prevzeta iz članka [9].

Definicija 5.1. Graf X je par $(V(X), E(X))$, kjer je $V(X)$ množica vozlišč grafa X in $E(X)$ seznam povezav grafa X. Veljati mora še, da $V(X) \neq \emptyset$ in da so elementi seznama $E(X)$ oblike $\{u, v\}$, kjer sta u in $v \in V(X)$.

V nadaljevanju se bomo osredotočili samo na *končne* in *enostavne* grafe, oziroma grafe, ki imajo končno število vozlišč ter nimajo zank in niti vzporednih povezav.

Primer 5.2. Petersenov graf X je definiran takole $V(X) = \{$dvoelementne podmnožice množice $\{1, 2, 3, 4, 5\}\}$ in $E(X) = \{\{a, b\} : a, b \in V(X),\ a \cap b = \emptyset\}$, glej sliko 5.1.



Slika 5.1: Petersenov graf.

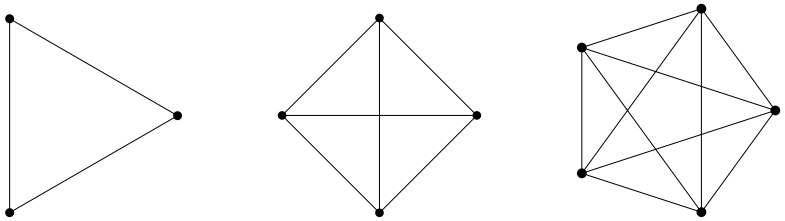
Definicija 5.3. Naj bo $X = (V(X), E(X))$ graf. *Sprehod* grafa X je zaporedje vozlišč $v_0, v_1, \ldots, v_k$ z lastnostjo, da sta vozlišči v_i in v_{i+1} povezani za vsak $i = 0, 1, \ldots, k-1$. Tak sprehod je dolžine k.

Sprehod je *enostaven*, če so vse njegove povezave različne.

Definicija 5.4. Graf X je *povezan*, če za poljubni dve vozlišči u, v grafa X obstaja sprehod grafa X, ki se začne v vozlišču u, konča pa v vozlišču v.

Definicija 5.5. Naj bo n poljubno naravno število. Graf $K_n = (V(X), E(X))$ je *poln reda* n, natanko takrat ko $|V(K_n)| = n$ in $E(K_n) = \{\{u, v\} : \ u, v \in V(X), u \neq v\}$.

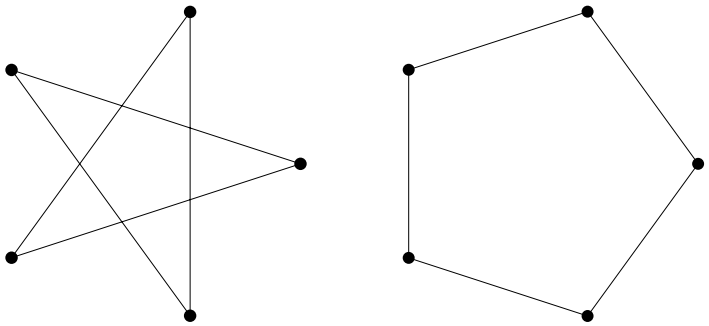
Primer 5.6. Oglejmo si grafe K_3, K_4 in K_5 na sliki 5.2.



Slika 5.2: Grafi K_3, K_4 in K_5.

Definicija 5.7. Naj bo $X = (V(X), E(X))$ graf. *Komplement* grafa X je graf X' pri katerem je $V(X') = V(X)$, $E(X') = \{\{u, v\} : \ u, v \in V(X'), u \neq v, \{u, v\} \notin E(X)\}$.

Primer 5.8. Oglejmo si graf X in njegov komplement na sliki 5.3.



Slika 5.3: Graf X in njegov komplement.

Definicija 5.9. *Avtomorfizem* grafa X je bijekcija ϕ iz $V(X)$ v $V(X)$ tako da $\{\phi u, \phi v\} \in E(X)$ natanko takrat, ko $\{u, v\} \in E(X)$.

Grupo vseh avtomorfizmov grafa X bomo označili z $\mathrm{Aut}(X)$. Opaziti moramo, da je $\mathrm{Aut}(X)$ permutacijska grupa, ki deluje na množici vozlišč $V(X)$. Očitno je, da $\mathrm{Aut}(X) = \mathrm{Aut}(X')$.

Definicija 5.10. Grafa $X = (V(X), E(X))$ in $Y = (V(Y), E(Y))$ sta *izomorfna*, če obstaja bijekcija $f : V(X) \to V(Y)$ z naslednjo lastnostjo: za poljuben par vozlišč $v, u \in V(X)$ velja, da je število povezav, ki povezujejo u in v enako številu povezav, ki povezujejo $f(u)$ in $f(v)$. V tem primeru preslikavi f pravimo *izomorfizem* grafov X in Y.

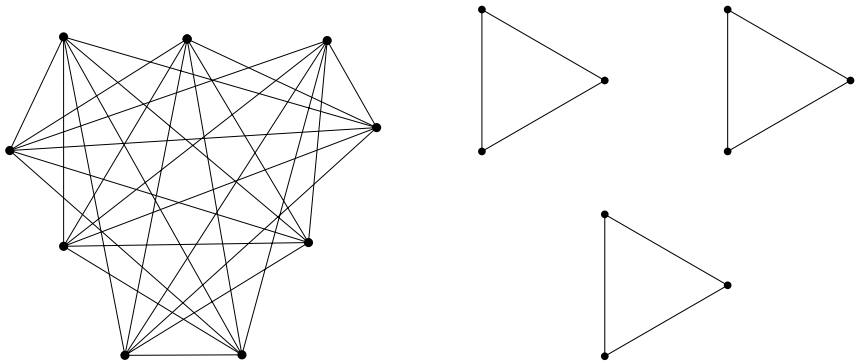
Definicija 5.11. Naj bosta X in Y grafa. Leksikografski produkt (ali *kompozitum*) grafa $X \circ Y$ je graf

$$V(X \circ Y) = V(X) \times V(Y),$$

$$E(X \circ Y) = \{\{(x, y), (x', y')\} \ : \ \{y, y'\} \in E(Y),$$
$$\text{ali} \quad y = y' \text{ in } \{x, x'\} \in E(X)\}.$$

Opomba 5.12. Navedli bomo, da je naša definicija za leksikografski produkt ekvivalentna definiciji Sabidussija [9, Definition 2] (glej tudi [1]).

Primer 5.13. Oglejmo si grafa $K_3' \circ K_3$ ter $K_3 \circ K_3'$ na sliki 5.4.



Slika 5.4: Grafa $K_3' \circ K_3$ in $K_3 \circ K_3'$.

V prejšnjem primeru lahko opazimo, da operacija kompozituma grafov ni komutativna. Velja pa asociativnost in sledeča enakost: $(X \circ Y)' = X' \circ Y,'$ kot je omenjeno v [9] brez dokaza. Sedaj bomo dokazali drugo lastnost.

Trditev 5.14. *Naj bosta X, Y grafa. Potem $(X \circ Y)' = X' \circ Y'$.*

Dokaz. Vemo, da je

$$V(X \circ Y) = V(X) \times V(Y),$$

$$E(X \circ Y) = \{\{(x,y),(x',y')\} \ : \ \{y,y'\} \in E(Y) \\ \text{ali} \quad y = y' \text{ in } \{x,x'\} \in E(X)\}.$$

$(X \circ Y)'$ pa je

$$V(X \circ Y)' = V(X) \times V(Y),$$
$$E(X \circ Y)' = \{\{(x,y),(x',y')\} \ : \ y \neq y', \{y,y'\} \notin E(Y) \\ \text{ali} \quad y = y' \text{ in } \{x,x'\} \notin E(X)\}.$$

Hitro opazimo, da je $X' \circ Y'$ sestavljen iz

$$V(X' \circ Y') = V(X) \times V(Y),$$

$$\begin{aligned} E(X \circ Y) &= \{\{(x,y),(x',y')\} \ : \ \{y,y'\} \in E(Y') \\ &\quad \text{ali} \quad y = y' \text{ in } \{x,x'\} \in E(X')\} \\ &= \{\{(x,y),(x',y')\} \ : \ y \neq y', \{y,y'\} \notin E(Y) \\ &\quad \text{ali} \quad y = y' \text{ in } \{x,x'\} \notin E(X)\} = E(X \circ Y)'. \end{aligned}$$

□

Zaključili bomo poglavje z naslednjim izrekom brez dokaza. Ta predstavlja glavno aplikacijo venčnega produkta na grafih. Več informacij o tem lahko dobimo v [1, 9].

Izrek 5.15. *Naj bosta X in Y grafa. Potem je*

$$\mathrm{Aut}(X) \ \mathrm{wr}_{V(Y)} \ \mathrm{Aut}(Y) \leq \mathrm{Aut}(X \circ Y).$$

Poglavje 6

Zaključek

Opazili smo, da so venčni produkti, kot poseben primer semidirektnega produkta, ključnega pomena pri konstrukciji p-Sylowk končne simetrične grupe. Seveda obstaja veliko zanimivih aplikacij omenjenega produkta. Najdemo jih lahko v knjigi [2, J. D. Dixon, B. Mortimer]. Da bi poglobili naše znanje glede leksikografskega produkta grafov, pa priporočam [9, G. Sabidussi].

Literatura

[1] L. Babai, Automorphism groups, isomorphism, reconsruction, in: R. L. Graham et al. (ed.), *Handbook of combinatorics, Volume 2*, Elsevier Science B.V., Amsterdam-New York, 1995, 1447–1540.

[2] J. D. Dixon, B. Mortimer, *Permutation Groups,* Springer-Verlag, New York 1996.

[3] J. B. Fraleigh, *A First Course in Abstract Algebra,* Addison-Wesley, 7th edition, 2002.

[4] B. Frelih, I. Kovács, *Permutacijske grupe,* gradivo (`http://e.famnit.upr.si`).

[5] L. Kaloujnine, La structure des p-groupes de Sylow de groupes symetriques finis, *Ann. sci. École Normale Supérieure, Sér. 3* **65** (1948), 239–276.

[6] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen, *Acta Math.* **68** (1937), 145–254

[7] Á Seress, *Permutation group algorithms,* Cambridge Tracts in Math. **152**, Cambridge University Press, Cambridge 2003.

[8] T. W. Judson, Abstract algebra - theory and applications, `http://abstract.ups.edu/download/aata-original.pdf`, (15.9.2012).

[9] G. Sabidussi, The composition of graphs, *Duke Math. J.* **26**, Number 4 (1959), 693–696.

[10] A. J. Weir, The Sylow subgroups of the symmetric groups, *Proc. American Math. Soc.* **6**, Number 4 (1955), 534–541.