15 Izreki Sylowa

1. Če je $|G| = p^2$, kjer je p praštevilo, potem je G abelska.

Izrek (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 ($1 \le i \le k$) velja, da ima G najmanj edno podgrupo reda p^i.

2. Dokaži izrek zgoraj.

3. Če praštevilo p deli red končne grupe G, potem G vsebuje najmanj en element reda p.

Pripomba. Posledica tega primera je Cauchy-ev izrek za končne grupe.

Definicija (p-podgrupa, p-grupa)
Naj bo p praštevilo. Podgrupa H grupe G se imenuje p-podgrupa, če je red vsakega elementa iz H enak potenci števila p. Podobno, če je red vsakega elementa iz grupe G enak potenci števila p, potem se G imenuje p-grupa.

Izrek Končna grupa G je p-grupa če in samo če je $o(G)$ enak potenci števila p.

4. Dokaži izrek zgoraj.

5. Katera od naslednjih grup je p-grupa:
(i) grupa G reda 21?
(ii) grupa G reda 25?
(iii) grupa G reda 128?

Definicija (Sylowa p-podgrupa)
Naj bo G končna grupa in naj bo p praštevilo. Podgrupa grupe G reda p^k ($k \in \mathbb{N}$) se imenuje Sylowa p-podgrupa grupe G, če p^k deli $o(G)$ in p^{k+1} ne deli $o(G)$.

Pripomba. Po definiciji Sylowe p-podgrupe, so vse Sylove p-podgrupe končne grupe istega reda.

6. Če je P Sylowa p-podgrupa končne grupe G, potem je za vsak $x \in G$, $x^{-1}Px$ tudi Sylowa p-podgrupa grupe G.

Opomba. Če je P edina Sylowa p-podgrupa, potem je $x^{-1}Px = P\ \forall x \in G$. Naj bosta $g \in G$, $h \in P$. Potem $ghg^{-1} = (g^{-1})^{-1}hg^{-1} = x^{-1}hx \in x^{-1}Px$ (vzemo $x = g^{-1}$), $ghg^{-1} \in P\ \forall g \in G$, $h \in P$, P je edinka v grupi G.

7. Naj bo $o(G) = p^k q$ kje je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$ in naj bo P Sylowa p-podgrupa grupe G. Če je H p-podgrupa grupe G t.d. $P \subseteq H \subseteq G$, potem pokaži, da je $H = P$.

Opomba. Iz primera zgoraj opazimo, da p-podgrupa grupe G ne more strogo vsebovati Sylowe p-podgrupe grupe G.

Definicija (S konjugirana množici T, relacija konjigiranosti na množici)
Naj bo G grupa in naj bosta S, T neprazni podmnožici grupe G. Pravimo, da je množica S konjugirana množici T, če obstaja element $x \in G$ t. d.

$$S = x^{-1}Tx = \{x^{-1}tx : t \in T\}.$$

Če je S konjugiran množici T, pišemo $S \sim T$ in to relacijo '$\sim$' imenujemo relacijo konjigiranosti na množici vseh nepraznih podmnožic grupe G.

Izrek. Relacija konjugiranosti na množici vseh nepraznih podmnožic grupe G je ekvivalenčna relacija.

8. Dokaži izrek zgoraj.

Definicija (dvojni odsek)
Naj bo G grupa, x njen element in H ter K njeni podgrupi (ne nujno različni). Množici

$$HxK = \{hxk : h \in H,\, k \in K\}$$

rečemo dvojni odsek podgrup H in K v grupi G in označujemo s HxK.

Izrek. 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.

Izrek. Naj bosta H in K dve (ne nujno različni) podgrupi končne grupe G. Za $x \in G$

$$o(HxK) = \frac{o(H)\,o(K)}{o((x^{-1}Hx) \cap K)}.$$

Izrek. (Frobenius). Če sta H in K dve (ne nujno različni) podgrupi končne grupe G, potem

$$o(G) = \sum \frac{o(H)o(K)}{o((x^{-1}Hx) \cap K)},$$

kjer vsota (na desni strani) teče po elementih x, ki so predstavniki dvojnih odsekov HyK.

9. Dokaži izreke zgoraj.

Izrek (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.

10. Če je S Sylowa p-podgrupa končne grupe G, pokaži da je potem število Sylowih p-podgrup grupe G enako $\frac{o(G)}{o(N(S))}$.

Izrek (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 $o(G)$.

Definicija (enostavna grupa)
Grupa G je enostavna, če sta njeni edini edinki trivijalna grupa in grupa G.

11. Poišči mogoče število Sylowih 11-podgrup, Sylovih 7-podgrup in Sylowih 5-podgrup v grupi reda $5^2 \cdot 7 \cdot 11$.

12. (a.) Pokaži, da grupa reda 28 ni enostavna.
(b.) Pokaži, da grupa reda 40 ni enostavna.

13. Pokaži, da v grupi reda 20449 obstaja Sylowa 11-podgrupa, ter da grupa ni enostavna.

14. Pokaži, da grupa reda 56 ni enostavna.

15. Če ima grupa G reda 28 edinko reda 4, potem pokaži, da je grupa G abelska.

16. Pokaži, da ne obstaja enostavna grupa reda 48.

17. (a.) Do izomorfizma natančno določi vse grupe reda 99.
(b.) Do izomorfizma natančno določi vse grupe reda 66.

18. Pokaži, da je edina grupa reda 255 grupa $\mathbb{Z}_{255}$.