1 Teorem konačnim Abelovim grupama

Teorema 1. *(Theorem 2.10.2) Neka je G konačna Abelova grupa reda p^n, za neki prost broj p. Tada je $G = A \times Q$, pri čemu je A ciklička grupa generisana elementom a najvećeg reda u grupi G.*

Dokaz. Neka je $a \in G$ element najvećeg reda u grupi G i neka je A ciklička grupa generisana tim elementom.

Dokaz provodimo indukcijom u odnosu na n. Ako je $n = 1$, onda je grupa G ciklička grupa, pa je $G = A$. To znači da tvrdnja vrijedi, jer za Q možemo uzeti trivijalnu podgrupu.

Pretpostavimo da tvrdnja vrijedi za $m < n$. Dokažimo prvo da teorema vrijedi u slučaju da postoji element $b \in G$, takav da $b \notin A$ sa osobinom da je $b^p = e$. Neka je B podgrupa generisana elementom b. Tada je $A \cap B = \{e\}$, jer je B generisana svakim svojim nejediničnim elementom. Neka je $\overline{G} = G/B$. Kako je $B \neq \{e\}$, to u grupi $\overline{G}$ ima p^{n-1} elemenata. Prema indukcionoj pretpostavci teorema vrijedi za grupu $\overline{G}$. Postavlja se pitanje: Koliki je red elelementa $\overline{a} = aB$? Tvrdimo da vrijedi: $o(\overline{a}) = o(a)$. Vrijedi da je $o(a)$. Jasno je da vrijedi $o(\overline{a}) \leq o(a)$, jer a element maksimalnog reda. Prema tome $o(\overline{a})|o(a)$.

Sa druge strane je $(\overline{a})^{\overline{a}} = \overline{e}$, tako da je $a^{\overline{a}} \in B$. Prema tome $a^{\overline{a}} \in A \cap B = \{e\}$. Prema tome $o(a)|o(\overline{a})$, pa slijedi $o(a) = (\overline{a})$, jer je a element najvećeg reda. Dakle, $\overline{a}$ je element najvećeg reda u grupi $\overline{G}$, pa teorema vrijedi za ovu grupu, na osnovu indukcione pretpostavke. Prema tome, $\overline{G} = (\overline{a}) \times T$, za neku podgrupu T od $\overline{G}$.

Neka je Q podgrupa od G koja prema teoremi o korespondenciji odgovara grupi T. Jasno je $b \in Q$. Tvrdimo da je $G = A \times Q$. Neka je $g \in G$. Tada je $\overline{g} = \overline{a}^j \cdot \overline{x}, (x \in Q)$, iz čega slijedi $g \cdot a^{-j} \cdot x^{-1} = b^s$, za neki s, što znači da je $g = a^j \cdot x \cdot b^s \in A \cdot Q$. Dakle, $G = A \cdot Q$.

Dokažimo još da je $A \cap Q = \{0\}$. Neka je $a^i \in A \cap Q$. Tada je $\overline{a}^i \in T$, pa kako ja $(a) \cap T = (\overline{e})$, imamo $\overline{a} = \overline{e}$, a kako je $o(a) = o(\overline{a})$ slijedi da je $a^i = e$. Prema tome $A \cap Q = \{e\}$, čime je dokazano da je $G = A \times Q$.

Podsjećamo, ako je neko zaboravio, da smo teoremu dokazali pod uslovom da postoji $b \in G; b \notin A$ takav da je $b^p = e$. Pretpostavimo sada da takav element ne postoji. Dokažimo da je u tom slučaju $G = A$ ciklička grupa. Pretpostavimo da to nije tačno, te da je $G \neq A$. Neka je $x \in G$ i $x \notin A$ ima najmanji mogući red. Kako je očigledno $o(x^p) < o(x)$, zaključujemo da je $x^p \in A$. Prema tome, $x^p = a^i$ za neki i. Tvrdimo da $p|i$. Neka je $o(a) = p^s$. Vrijedi $x^{p^s} = e$, jer je a element maksimalnog reda. Vrijedi $e = x^{p^s} = (a^i)^{p^{s-1}}$ i kako je $o(a) = p^s$, yaključujemo da vrijedi $p|i$, tj. $x^p = a^i$, pri čemu $p|i$.

Neka je $y = a^{-\frac{i}{p}} \cdot x$. Tada je $y^p = a^{-i} x^p = e$. Međutim $y \notin A$ jer $x \notin A$. Ovo nas vraća na razmatranja sa početka.

Mada dokaz ove teoreme nije jednostavan, on nam omogućava da dokažemo jedan od najljepših rezultata u algebri, a to je potpuna karakterizacija konačnih Abelovih grupa.

Teorema 2 (Theorem 1.10.3)**.** *(Fundamentalna teorema o konačnim Abelovim grupama). Svaka končna Abelova grupa je (do izomorfizma) jednaka direktnom proizvodu* *cikličkih grupa.*

Dokaz. Neka je G konačna Abelova grupa i neka je p prosti faktor reda $|G|$ te grupe. Na osnovu leme 2.10.1 vrijedi $G = P \times T$, pri čemu je $|P| = p^n$, za neki n. Na osnovu teoreme teoreme 2.10.2 vrijedi $P = A_1 \times A_2 \times \cdots \times A_k$, pri čemu su $A_1, A_2, \ldots, A_k$ cikiličke podgrupe grupe P. Koristeći indukciju možemo pretpostavitida je i T direktni proizvod cikličkih grupa tj. da je $T = T_1 \times T_2 \times \cdots \times T_q$, Tako da na kraju dobijamo:

$$G = A_1 \times A_2 \times \cdots \times A_k \times T_1 \times T_2 \times \cdots \times T_q.$$

Na osnovu ove teoreme nije teško prebrojati koliko ima ukupno neizomorfnih Abelovih grupa datog reda. Ako je G Abelova grupa reda p^n, onda je $P = A_1 \times A_2 \times \cdots \times A_k$, gdje su $A_1, A_2, \ldots, A_k$ cikličke grupe reda $p^{n_1}, p^{n_2}, \ldots, p^{n_k}$, pri čemu je $n_1 \geq n_2 \geq \cdots \geq n_k$ i $n = n_1 + n_2 + \cdots + n_k$. Brojevi $n_1, n_2, \ldots, n_k$ se nazivaju invarijantama grupe P. Kao što vidimo te invarijante čine particiju broja n. Vrijedi i obrnuto, svaka particija od n određuje neko razlagnje grupe G na direktni proizvod cikličkih podgrupa. Prema tome, broj neizomorfnih Abelovih grupa reda p^n jednak je broju particija broja n.

Na primjer, broj 3 ima tri particije $3, 2+1, 1+1+1$, pa dakle imamo 3 neizomorfne Abelove grupe reda p^3. Takođe, imamo pet neizomorfnih Abelovih grupa reda P^4 itd.