

Rozkład permutacji na cykle.

Permutację nazywamy *cyklem*, jeśli jest postaci $(i \mapsto j \mapsto k \mapsto \dots \mapsto z \mapsto i)$ dla pewnych parami różnych $i, j, k, \dots, z$ (o których to mówimy, że tworzą *nośnik* cyklu). Cykl zapisujemy tak: $(i j k \dots z)$. Np. (ij) to transpozycja i i j . Każda permutacja jest iloczynem cykli o rozłącznych nośnikach; taki iloczyn jest przemienny i – z dokładnością do kolejności – jednoznaczny. Nośnikami czynników permutacji $\sigma \in S_n$ są po prostu orbity $\langle \sigma \rangle$ na $\{1, 2, \dots, n\}$.

Sprzężenie cyklu $(i j k \dots z)$ przez σ to cykl $(\sigma(i) \sigma(j) \sigma(k) \dots \sigma(z))$.

Stąd wynika, że dwie permutacje są sprzężone w $S_n \iff$ ich rozkłady na rozłączne cykle składają się z cykli tej samej długości.

Prostota A_n

Lemat 1. Grupa A_n jest generowana przez

- cykle długości 3: $A_n = \langle \{(ijk)\} \rangle$;
- iloczyn par rozłącznych transpozycji: $A_n = \langle \{(ij)(kl)\} \rangle$ (dla $n \geq 5$).

Permutacje parzyste są iloczynami parzystości wielu transpozycji, które można połączyć w pary. Elementy pary mogą być rozłączne lub nie, ale jeśli nie są, można je sztucznie rozdzielić wstawiając między nie rozłączną z nimi transpozycję: $(ij)(jk) = ((ij)(ab))((ab)(jk))$. Aby pokazać a) obserwujemy, że:

$$(ij)(jk) = (ijk); \quad (ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl).$$

Lemat 2. ($n \geq 5$) A_n jest jedynym dzielnikiem normalnym S_n .

Niech σ będzie nietrywialnym elementem $N \triangleleft S_n$; niech $\sigma(i) \neq i$, i niech $j \neq i, \sigma(i)$. Weźmy $\tau = (ij)$. Wtedy

$$N \ni \sigma(\tau\sigma^{-1}\tau^{-1}) = (\sigma\tau\sigma^{-1})\tau^{-1} = (\sigma(i)\sigma(j))(ij).$$

Ten ostatni iloczyn jest postaci $(ab)(cd)$ lub postaci (abc) ; w obu przypadkach Lemat 1 daje $N = A_n$.

Tw. ($n \geq 5$) A_n jest prosta.

Jeśli nie, to weźmy minimalny jej dzielnik normalny N . Grupa $N' = (12)N(12)$:

- jest różna od N (inaczej $N \triangleleft S_n$, wbrew Lematowi 2);
- jest dzielnikiem normalnym A_n ;
- kroi się trywialnie z N (z minimalności N);
- generuje wraz z N podgrupę $NN' \simeq N \times N'$.

Ta podgrupa NN' jest normalna w S_n : A_n normalizuje każdy czynnik, zaś permutacje nieparzyste transponują czynniki. Stąd $A_n = NN' \simeq N \times N'$. To oczywiście bzdura.

(Nieoczywisty prosty dowód można zrobić tak. $2||N|$, więc w N jest element rzędu 2 – iloczyn rozłącznych transpozycji; jego sprzężenie przez jedną z tych transpozycji jest nim samym, a leży w N' . Sprzeczność z $N \cap N' = \{e\}$.)

Skończona grupa abelowa jest produktem grup cyklicznych

Indukcja względem liczby elementów. Niech x będzie elementem maksymalnego rzędu w skończonej abelowej grupie G , $N = \langle x \rangle$. Znajdziemy w G podgrupę H “dopełniczą” do N , tj. taką, że $G = NH \simeq N \times H$.

Weźmy monomorfizm φ grupy N w grupę $\mathbf{T}$ liczb zespolonych o module 1, i wyindukujemy z niego reprezentację G . To znaczy, rozważmy przestrzeń funkcji $f: G \rightarrow \mathbf{C}$ spełniających $f(gx) = \varphi(x^{-1})f(g)$. Ta przestrzeń ma naturalny iloczyn skalarny – ograniczenie standardowego iloczynu skalarnego na przestrzeni wszystkich funkcji na G (dla którego delty Diraca są bazą ortonormalną). Ma też rodzinę komutujących (dzięki przemienności grupy) unitarnych automorfizmów $(\rho(g))_{g \in G}$: $\rho(g)$ przesuwają funkcję po grupie elementem g , $(\rho(g)f)(g') = f(g^{-1}g')$. Ta rodzina diagonalizuje się we wspólnej bazie, a wartość własna któregośkolwiek z wektorów własnych zadaje homomorfizm $\Phi: G \rightarrow \mathbf{T}$ rozszerzający φ .

Obraz Φ jest skończoną podgrupą $\mathbf{T}$, jest więc cykliczny. Nie ma on więcej niż $|N|$ elementów (inaczej dowolny przeciwobraz generatora $\text{Im}(\Phi)$ byłby elementem G rzędu większego niż rząd x), więc ma dokładnie $|N|$ elementów ($\varphi = \Phi|_N$ jest 1-1). Niech $H = \ker(\Phi)$. Wtedy $|H| = |G/N|$, $H \cap N = \{e\}$ – czyli $G = NH \simeq N \times H$. Z założenia indukcyjnego H jest produktem grup cyklicznych.

Niech n, k będą względnie pierwsze. Homomorfizm $\mathbf{Z} \ni x \mapsto (x \bmod n, x \bmod k) \in \mathbf{Z}/n \times \mathbf{Z}/k$ ma jądro $nk\mathbf{Z}$; zatem $\mathbf{Z}/nk \simeq \mathbf{Z}/n \times \mathbf{Z}/k$.

Tw. *Skończona grupa abelowa jest produktem grup postaci $\mathbf{Z}/p^k$, gdzie p są liczbami pierwszymi.*

Rozkład, o którym mowa w twierdzeniu, jest jednoznaczny (zad.).

Wniosek. *Skończona podgrupa grupy mnożymy ciała jest cykliczna.*

Gdyby tak nie było, miałyby ona podgrupę postaci $\mathbf{Z}/p^k \times \mathbf{Z}/p^n$. W czynnikach tej podgrupy widać $2p - 1$ pierwiastków wielomianu $X^p - 1$ – więcej niż jego stopień.

Wniosek: grupa mnożymy reszt modulo p jest cykliczna; inaczej mówiąc, istnieje pierwiastek pierwotny modulo p – liczba, której potęgi dają wszystkie niezerowe reszty modulo p .