1 Twierdzenie Maschkego

Lemat 1.1 *Niech G będzie grupą skończoną mocy n, V przestrzenią wektorową nad ciałem K charakterystyki nie dzielącej n zaś ρ reprezentacją G na V. Jeśli W jest podprzestrzenią niezmienniczą dla ρ to istnieje podprzestrzeń U niezmienniczą dla ρ taka że $U + W = V$, $U \cap W = \{0\}$.*

Uwaga: Oznacza to że ρ jest równoważne sumie prostej reprezentacji działających na U i W.

Dowód: Zauważmy najpierw że istnieje operator liniowy P z V w W spełniający $P(x) = x$ dla $x \in W$. Mianowicie, możemy wybrać bazę B przestrzeni V w ten sposób że napierw wybieramy bazę A przestrzeni W a następnie uzupełniamy ją do bazy V. Czyli $A \subset B$. Dowolny element $v \in V$ można zapisać w postaci

$$v = \sum_{b \in B} c_b b.$$

Operator P defininujemy wzorem

$$P(v) = \sum_{b \in A} c_b b.$$

Oczywiście dla $v \in W$ mamy $P(v) = v$, bo $c_b = 0$ dla $b \notin A$. Z definicji P jest operatorem liniowym. Teraz definiujemy operator Q wzorem

$$Q = \frac{1}{n} \sum_{g \in G} \rho(g) P \rho(g^{-1}).$$

Mamy

$$\begin{aligned} \rho(h)Q = \frac{1}{n} \sum_{g \in G} \rho(h)\rho(g) P \rho(g^{-1}) &= \frac{1}{n} \sum_{g \in G} \rho(hg) P \rho((hg)^{-1}) \rho(h) \\ &= \frac{1}{n} \sum_{g \in G} \rho(g) P \rho(g^{-1}) \rho(h) = Q\rho(h). \end{aligned}$$

gdzie przedostatnia równość zachodzi bo hg przebiega przez wszystkie elementy G. Teraz niech U będzie jądrem Q, tzn. $U = \{v \in V : Q(v) = 0\}$. Jeśli $v \in U$ to

$$Q\rho(g)v = \rho(g)Qv = 0,$$

czyli $\rho(g)v \in U$. A więc U jest niezmiennicze na działanie v. Jako że $Q(v) = v$ dla $v \in W$ to $U \cap V = \{0\}$. Jako że $Qv \in W$ to $QQv = Qv$, czyli

$$Q(v - Qv) = Qv - QQv = Qv - Qv = 0$$

czyli $v - Qv \in U$. A więc biorąc $w = Qv \in W$ i $u = v - w \in U$ mamy $v = u + w$ co pokazuje że $V = U + W$. □

2 Lemat Schura, wersja algebraiczna

Lemat 2.1 *Jeśli M i N są modułami, zaś ϕ jest niezerowym homomorfizmem z M w N to*

- *jeśli M jest prosty to ϕ jest różnowartościowy*
- *jeśli N jest prosty to ϕ jest na*
- *jeśli M i N są proste to ϕ jest izomorfizmem*

Dowód: Jądro $\ker(\phi)$ jest podmodułem M, jeśli M jest prosty to $\ker(\phi) = \{0\}$ lub $\ker(\phi) = M$. W drugim przypadku ϕ byłby zerowy, co jest wykluczone z założenia. A więc gdy M jest prosty to $\ker(\phi) = \{0\}$ czyli ϕ jest różnowartościowy. Podobnie, obraz $\phi(M)$ jest podmodułem N i jeśli N jest prosty to musimy mieć $\phi(M) = N$. □

Lemat 2.2 *Algebra endomorfizmów R-modułu prostego jest algebrą z dzieleniem. Jeśli R jest skończenie wymiarową algebrą nad ciałem algebraicznie domkniętym K to każdy endomorfizm modułu prostego jest operatorem mnożenia przez element K.*

Dowód: Na mocy poprzedniego lematu niezerowe endomorfzmy są odwracalne, co daje pierwszą część. Dla dowodu drugiej części zauważmy że wtedy moduł prosty M jest skończenie wymiarową przestrzenią wektorową nad ciałem K. Endomorfizm ϕ możemy przedstawić przy pomocy macierzy. Wiadomo że nad ciałem algebraicznie domkniętym macierz ma wartość własną λ i odpowiający jej wektor własny v, tzn.

$$\phi v = \lambda v$$

czyli

$$(\phi - \lambda)v = 0$$

Jako że M jest modułem prostym oznacza to że $(\phi - \lambda)w = 0$ dla dowolnego $w \in M$. □

Lemat 2.3 *Jeśli R jest skończenie wymiarową algebrą przemienną nad ciałem algebraicznie domkniętym K to każdy R-moduł M prosty jest przestrzenią jednowymiarową nad K zaś R działa na M za pomocą mnożenia przez element K.*

Dowód: Jako że R jest przemienny, to elementy R działają za pomocą mnożenia przez element K. A więc podprzestrzenie jednowymiarowe są niezmiennicze na działanie R, czyli M jest jednowymiarowy. □

Uwaga. Jeśli G jest skończoną grupą abelową to na mocy lematu (gdy są spełnione założenia) moduły proste nad $K[G]$ (czyli reprezentacje nieprzywiedlne G) są jednowymiarow. Elementy G działają za pomocą mnożenia przez element K. A więc jeśli ρ jest reprezentacją nieprzywiedlną, to dla $g \in G$ istnieje a_g takie że $\rho(g)v = a_g v$. W grupie skończonej istnieje k_g takie że $g^{k_g} = e$ gdzie e jest jedynką w G. Wtedy mamy

$$v = \rho(e)v = \rho(g^{k_g})v = \rho(g)^{k_g}v = a_g^{k_g}v$$

czyli $a_g^{k_g} = 1$, czyli wartości a_g są pierwiastkami z 1. W szczególności, jeśli G jest skończoną grupą cykliczną to G jest izomorfizne z liczbami całkowitymi modulo k dla pewneho k. Reprezentacja grupy cyklicznej jest jednoznacznie wyznaczona przez wartość na generatorze, (tzn. 1). Poprzednie rozumowanie pokazuje że dla reprezentacji nad liczbami zespolonymi mamy

$$\rho(l)v = \exp(2\pi i l m/k)v$$

gdzie $m = 0, 1, \ldots k - 1$ jest parametrem opisującym reprezentację, zaś i jest jednostką urojoną.