1 Grupa dihdralna

Niech będzie dane odwzorowanie α z $\mathbb{Z}_2$ w automorfizmy $\mathbb{Z}_n$ takie że $\alpha(0)$ to idetyczność zaś $\alpha(1)(m) = -m$.

Wtedy na produkcie $\mathbb{Z}_2 \times \mathbb{Z}_n$ działanie wprowadzamy wzorem

$$(z_1, m_1)(z_2, m_2) = (z_1 z_2, \alpha(z_2) m_1 m_2).$$

Otrzymaną w ten sposób grupę oznaczamy D_n i nazywamy grupą dihedralną (przy ogólnych grupach i ogólnym α wzór wyżej definiuje produkt półprosty).

Chcemy wyznaczyć reprezentacje nieprzywiedlne D_n na ciałem liczb zespolonych, tzn. moduły proste nad $\mathbb{C}[D_n]$. Zauważmy że D_n zawiera grupę $\mathbb{Z}_n$. Niech V będzie przestrzenią reprezentacji nieprzywiedlnej ρ grupy D_n. ρ możemy potraktować jako reprezentację $\mathbb{Z}_n$. Wtedy na mocy twierdzenia Maszkego V rozpadnie się na sumę prostą reprezentacji nieprzywiedlnych $\mathbb{Z}_n$:

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_l.$$

Jako że $\mathbb{Z}_n$ jest grupą abelową zaś $\mathbb{C}$ jest ciałem algebraicznie domkniętym to V_k są jednowymiarowe. Można przyjąć że dla $v \in V_1$ i $m \in \mathbb{Z}_n$ mamy wzór

$$\rho((0, m))v = \exp(\frac{2\pi i k m}{n})v$$

gdzie k jest parametrem reprezentacji. Oznaczmy przez s element $(1, 0) \in D_n$. Rozważmy teraz działanie $\mathbb{Z}_n$ na $\rho(s)V_1$. Mamy

$$\rho((0, m))\rho(s)v = \rho(s)\rho(s^{-1})\rho((0, m))\rho(s)v$$

$$= \rho(s)\rho(s^{-1}(0, m)s)v = \rho(s)\rho(-m)v$$

$$\rho(s)\exp(\frac{2\pi i k(-m)}{n})v = \exp(\frac{2\pi i(-k)m}{n})\rho(s)v.$$

Czyli $\rho(s)V_1$ jest przestrzenią reprezentacji $\mathbb{Z}_n$ z parametrem $-k$. Stosując podobne rozumowanie do reprezentacji na $\rho(s)V_1$ widać że $\rho(s)$ przeprowadzi ją na reprezentację z parameterem k. W więc

$$V = W_k \oplus W_{-k}$$

gdzie W_k jest sumą przestrzeni reprezentacji $\mathbb{Z}_n$ z parametrem k zaś W_{-k} jest sumą reprezentacji z parametrem $-k$. Mianowicie, $\rho(s)W_k \subset W_{-k}$, $\rho(s)W_{-k} \subset W_k$, zarówno W_k jak i W_{-k} są niezmniennicze na działanie $\mathbb{Z}_n$, więc suma $W_k \oplus W_{-k}$ jest niezmiennicza na działanie D_n. Jako że V jest nieprzywiedlna oznacza to równość $V = W_k \oplus W_{-k}$.

V możemy też potraktować jako przestrzeń reprezentacji $\mathbb{Z}_2$. Niech teraz v rozpina jednowymiarową podprzestrzeń niezmienniczą dla $\mathbb{Z}_2$. Piszemy $v = w_1 \oplus w_2$ gdzie $w_1 \in W_k$ zaś $w_2 \in W_{-k}$. Zakładając że $k \neq -k \mod n$ i $\rho(s)v = v$ mamy $w_2 = \rho(s)w_1$ i $w_1 = \rho(s)w_2$, a więc dwuwymiarowa podprzestrzeń rozpinana przez w_1 i w_2 jest niezmiennicza zarówno dla $\mathbb{Z}_2$ jak i dla $\mathbb{Z}_n$, a więc jest niezmiennicza dla D_n. Podobnie, jeśli $\rho(s)v = -v$, to $-w_2 = \rho(s)w_1$ i $-w_1 = \rho(s)w_2$ i również w tym przypadku podprzestrzeń rozpinana przez w_1 i w_2 jest niezmiennicza dla D_n. A więc reprezentacje nieprzywiedlne D_n są dwuwymiarowe, za wyjątkiem przypadku $k = -k \mod n$, gdy otrzymujemy reprezentacje jednowymiarowe. Ten przypadek zachochdzi gdy $k = 0$, lub n jest parzyste i $k = n/2$.

2 Suma prosta

Na nieskończonym iloczynie kartezjańskim modułów mamy naturalną strukturę modułu, mianowicie operacje wykonujemy po składowych. Sumą prostą potencjalnie nieskończonej rodziny modułów M_α, $\alpha \in I$ jest podzbiór produktu kartezjańskiego M_α, $\alpha \in I$ składający się z tych elementów które mają tylko skończenie wiele składowych różnych od zera. Oznaczenie:

$$M = \bigoplus_{\alpha \in I} M_\alpha$$

Każdy z modułów M_α jest naturalnie izomorficzny z podmodułem M, dlatego zwykle możemy zakładać że $M_\alpha \subset M$. Przy takim założeniu dla $\alpha \neq \beta$ mamy $M_\alpha \cap M_\beta = \emptyset$.

Jeśli M jest modułem a M_α, $\alpha \in I$ są podmodułami M to sumą M_α nazywamy najmniejszy podmoduł $N \subset M$ taki że dla każdego $\alpha \in I$ mamy $M_\alpha \subset N$.

Jeśli M jest sumą M_α, $\alpha \in I$ oraz dla $\alpha \neq \beta$ mamy $M_\alpha \cap M_\beta = \emptyset$, to wtedy M jest izomorficzny z sumą prostą M_α, $\alpha \in I$. W tej sytuacji dalej będziemy mówić że M jest sumą prostą.

Jeśli M jest sumą prostą $M_1 \oplus M_2$ swoich podmodułów M_1 i M_2 to mówimy że M_2 jest modułem dopełniczym do M_1.

3 Moduły półproste

Najpierw potrzebujemy lemat opisujący moduły proste

Lemat 3.1 *Moduł M jest prosty wtedy i tylko wtedy gdy M jest izomorficzy z modułem postaci R/I gdzie I jest lewostronnym ideałem maksymalnym w R.*

Dowód. Niech I będzie lewostronnym ideałem maksymalnym w R i N będzie podmodułem w R/I. Wtedy $J = \{r \in R : r + I \subset N\}$ jest ideałem lewostronnym zawierającym I. Jako że I jest ideałem maksymalnym oznacza to że $J = R$ lub $J = I$. W pierwszym przypadky mamy $N = R/I$, w drugim $N = \{0\}$, a więc R/I jest modułem prostym. Jeśli M jest modułem prostym i $x \in M$, $x \neq 0$ to przyjmujemy $I = \{r : rx = 0\}$. Wtedy I jest ideałem lewostronnym w R. Zauważmy że Rx jest niezerowym podmodułem w M, czyli $Rx = M$. Innymi słowy M jest izomorficzne z R/I. Jeśli J jest ideałem lewostronnym i $I \subset J$ to Jx jest podmodułem w M, czyli $Jx = M$ lub $Jx = \{0\}$. Jeśli $Jx = M$ to dla dowolnego $r \in R$ istnieje $s \in J$ takie że $rx = sx$, czyli $(r - s)x = 0$, czyli

$r - s \in I$. Jako że $I \subset J$ i $s \in J$ oznacza to że $r \in J$, czyli $J = R$. Jeśli $Jx = \{0\}$ to mamy $J = I$. Razem oznacza to że I jest ideałem maksymalnym. $\square$

Lemat 3.2 *Następujące warunki są równoważne*

- *moduł M jest sumą prostą modułów prostych*
- *moduł M jest sumą algebraiczną modułów prostych*
- *każdy podmoduł $V \subset M$ ma podmoduł dopełniczy będący sumą prostą modułów prostych*
- *każdy podmoduł $V \subset M$ ma podmoduł dopełniczy*

Moduł spełniający jeden (a więc i wszystkie) warunki wyżej nazywamy modułem półprostym.

Dowód: Warunek pierwszy jest oczywiście silniejszy niż drugi. Warunek trzeci jest oczywiście silniejszy niż czwarty. Dla $V = \{0\}$ warunek trzeci implikuje warunek pierwszy. Pozostaje pokazać że warunek drugi implikuje trzeci i że warunek czwarty implikuje drugi.

Aby otrzymać warunek trzeci z drugiego rozważmy rodzinę S składającą się z takich modułów N że N jest sumą prostą modułów prostych i $V \cap N = \emptyset$. Zauważymy że suma V i N jest sumą prostą, tzn $V + N = V \oplus N$.

Na mocy lematu o maksymalnym łańcuchu w rodzinie S istnieje element maksymalny, tzn. taki moduł N że dla każdego modułu prostego $P \subset M$ mamy $P \cap (V \oplus N) \neq \{0\}$ (w przeciwnym razie możnaby dołączyć P jako kolejny składnik N przecząc maksymalności). A więc dla dowolnego modułu prostego $P \subset M$ mamy $P \subset V \oplus N$, czyli jako że M jest sumą modułów prostych to $M = V \oplus N$. Ponadto N jest sumą prostą modułów prostych co daje warunek trzeci.

Aby zakończyć dowód lematu musimy pokazać że warunek czwarty implikuje drugi.

Zauważmy najpierw że jeśli warunek czwarty jest spełniony dla M i U jest podmodułem M to warunek czwarty zachodzi dla M zastąpionego przez U. Mianowicie, jeśli V jest podmodułem U to jest też podmodułem M. Używając warunek dla M dostajemy moduł N dopełniczy do V w M. Lecz wtedy $N \cap U$ jest modułem dopełniczym do V w U. Pokażemy teraz że dowolny moduł M spełniający warunek czwarty zawiera podmoduł prosty. Mianowicie, bez utraty ogólności można przyjąć że $M = Rx$ dla pewnego $x \in M$. Niech $J = \{r \in R : rx = 0\}$. J jest ideałem lewostronnym w R. Na mocy pewnika wyboru (lematu o maksymalnym łańcuchu) istnieje ideał maksymalny I zawierający J. Wtedy $N = Ix$ jest podmodułem w $M = Rx$ takim że M/N jest izomorficzne z R/I, czyli iloraz jest modułem prostym. Na mocy warunku czwartego istnieje podmoduł P dopełniczy do M, czyli $Rx = P \oplus N$ czyli P jest izomorficzne z Rx/N czyli P jest modułem prostym. Rozważmy teraz sumę S wszystich modułów prostych zawartych w M. Gdyby S było podmodułem właściwym to S miałby niezerowy moduł dopełniczy, a więc dopełnienie S zawierałoby moduł prosty. Lecz to jest niemożliwe z definicji S czyli M jest sumą modułów prostych czyli zachodzi warunek drugi. $\square$

4 Lemat o gęstości

Jeśli M jest modułem to endomorfizmy M tworzą pierścień który oznaczymy przez E. M możemy potraktować jako moduł nad E. Dla zaznaczenia że pierścieniem jest E będziemy pisać M_E. Istotny dla nas jest opis endomorfizmów M_E.

Lemat 4.1 *Jeśli M jest modułem półprostym, ϕ jest endomorfizmem M_E zaś $x \in M$ to istnieje $\alpha \in R$ takie że $\phi(x) = \alpha x$.*

Dowód: $N = Rx$ jest podmodułem M, a więc na mocy półprostoty jest składnikiem prostym M. A więc rzut π_N z M na N należy do E. Wtedy

$$\pi_N(\phi(x)) = \phi(\pi_N(x)) = \phi(x)$$

czyli $\phi(x) \in N$, co daje wynik. $\square$

Lemat 4.2 *(Jacobsona o gęstości) Jeśli M jest modułem półprostym, ϕ jest endomorfizmem M_E zaś S jest skończonym podzbiorem M. Wtedy istnieje $\alpha \in R$ takie że dla dowolnego $x \in S$ mamy $\phi(x) = \alpha x$.*

Dowód: Niech $n = |S|$ czyli $S = \{x_1, \ldots, x_n\}$. Rozważmy n-krotną sumę prostą M^n. Na M^n rozpatrujemy odwzorowanie $\phi^{(n)}$ zadane wzorem

$$(y_1, \ldots, y_n) \mapsto (\phi(y_1), \ldots, \phi(y_n)).$$

Niech $E^{(n)}$ będzie pierścieniem endomorfizmów M^n. Zauważmy że elementy $E^{(n)}$ to macierze n na n o współczynnikach będących endomorfizmami M. Ze wzoru na $\phi^{(n)}$ wynika więc że $\phi^{(n)}$ jest homomorfizmem M^n jako modułu nad $E^{(n)}$. Moduł M^n jest oczywiście półprosty. Z poprzedniego lematu istnieje element $\alpha \in R$ taki że $\phi^{(n)}(x_1, \ldots, x_n) = \alpha(x_1, \ldots, x_n)$. Lecz to oznacza że $\phi(x_i) = \alpha x_i$. $\square$