Algebra ISIM 2. Wykład 14: Moduły.

Moduł nad pierścieniem R to grupa abelowa wyposażona w mnożenie $R \times M \to M$. Mnożenie ma spełniać: $1 \cdot m = m$; $(r+s)m = rm + sm$; $r(m+n) = rm + rn$; $(rs)m = r(sm)$.

Przykłady:

- Przestrzeń liniowa nad ciałem.
- R^n – moduł wolny nad pierścieniem R.
- Ideał $I \lhd R$ i moduł ilorazowy R/I.
- Grupa abelowa to $\mathbf{Z}$-moduł ($n \cdot g = g + g + \ldots + g$, n razy).
- Przestrzeń liniowa nad K z endomorfizmem F jako $K[X]$-moduł: $P(X) \cdot v = P(F)(v)$.
- Cięcia wiązek. Np. cięcia wstęgi Möbiusa tworzą moduł $M \simeq \{f \in C[0,1] \mid f(0) = -f(1)\}$ nad pierścieniem funkcji ciągłych na okręgu $R \simeq \{f \in C[0,1] \mid f(0) = f(1)\}$ spełniający $M \oplus M \simeq R \oplus R$, mimo że $M \not\simeq R$.

Układ $(m_1, \ldots, m_n)$ elementów M nazywamy *zbiorem generatorów* modułu M, jeśli każdy $m \in M$ da się przedstawić w postaci $r_1 m_1 + \ldots + r_n m_n$ dla pewnych $r_i \in R$. Jeśli takie przedstawienie jest dla każdego m jednoznaczne, to moduł nazywamy *wolnym,* a układ (m_i) nazywany jego *bazą.* Odwzorowanie $R^n \ni (r_i) \mapsto \sum_i r_i m_i \in M$ jest wówczas izomorfizmem. Dla zbioru generatorów takie odwzorowanie jest epimorfizmem; dzięki niemu można przedstawić skończenie generowany moduł jako iloraz R^n/N (gdzie N to jądro). Dla modułu M *cyklicznego* (generowanego przez jeden element) dostajemy $M \simeq R/I$ (gdzie I jest ideałem).

Podmoduł to niepusty podzbiór modułu zamknięty na dodawanie i mnożenie. Moduł jest *noetherowski,* jeśli każdy jego podmoduł jest skończenie generowany (jak dla pierścieni, jest to równoważne warunkowi stabilizacji wstępujących ciągów podmodułów).

Fakt. *Skończenie generowany moduł nad pierścieniem noetherowskim jest modułem noetherowskim.*

Dowód. Niech M będzie skończenie generownym modułem, zaś N jego podmodułem. Ze skończonym zbiorem generatorów modułu M związany jest epimorfizm $\phi\colon R^n \to M$. Wystarczy sprawdzić, że $S = \phi^{-1}N$ jest skończenie generowanym podmodułem R^n. Pokazujemy to przez indukcję względem n.

$$0 \to S \cap R^{n-1} \to S \to S/(S \cap R^{n-1}) \to 0$$

Lewy wyraz jest skończenie generowany z założenia indukcyjnego, a prawy – bo wkłada się w noetherowski $R \simeq R^n/R^{n-1}$.

Tw. *Skończenie generowany moduł nad PID jest sumą prostą skończenie wielu modułów cyklicznych.*

Dowód. (Dla R euklidesowych.) Zapisujemy M jako R^n/N. Układ generatorów N rozpisany w bazie R^n daje macierz A o wyrazach z R. Operacje elementarne na tej macierzy odpowiadają zmianom bazy R^n (wierszowe) lub układu generatorów N (kolumnowe). Okazuje się, że takimi operacjami można sprowadzić A do postaci diagonalnej (co daje tezę). Najpierw wybieramy lewy górny róg i inne miejsce w pierwszym wierszu (lub kolumnie), i na elementach tam stojących wykonujemy algorytm Euklidesa – tak, by największy wspólny dzielnik znalazł się na końcu w lewym górnym rogu. Powtarzamy to z różnymi wyborami 'innego miejsca', aż wszystkie wyrazy pierwszego wiersza i kolumny – za wyjątkiem lewego górnego rogu – wyzerują się. Procedura kończy się, gdyż ideał generowany przez element z lewego górnego rogu rośnie, a pierścień jest noetherowski. Następnie zapominamy o pierwszym wierszu i kolumnie i powtarzamy procedurę w pozostałej części macierzy.

Lemat. *Jeśli R jest PID, zaś $p, q \in R$ są względnie pierwsze, to $R/(pq) \simeq R/(p) \oplus R/(q)$.*

Dowód. (dla R euklidesowych) Rozważamy homomorfizm $R \ni r \mapsto (r + (p), r + (q)) \in R/(p) \oplus R/(q)$. Jego jądro to $(p) \cap (q) = (pq)$. By pokazać surjektywność dobierzmy $a, b \in R$ tak, by $ap + bq = 1$. Wtedy dla dowolnych $x, y \in R$ mamy $(y-x)ap + x = y + (x-y)bq \mapsto (x + (p), y + (q))$.

Wnioski.

- Skończenie generowany moduł nad PID jest skończoną sumą prostą składników postaci R lub $R/(p^k)$, gdzie $p \in R$ są nierozkładalne, $k \in \mathbf{Z}$.
- Każda skończenie generowana grupa abelowa jest postaci $\mathbf{Z}^n \oplus \bigoplus_{p,k} \mathbf{Z}/p^k$, gdzie p są liczbami pierwszymi (składniki mogą się powtarzać).

- Niech V będzie skończenie wymiarową przestrzenią liniową nad algebraicznie domkniętym ciałem K (np. $K = \mathbf{C}$), i niech F będzie endomorfizmem V. Traktując V jako $K[X]$-moduł dostajemy:

$$V \simeq \bigoplus_{\lambda,k} K[X]/((X-\lambda)^k).$$

Jeśli zbudować bazę V biorąc w każdym składniku bazę $(1, X-\lambda, \ldots, (X-\lambda)^{k-1})$, to w takiej bazie macierz F ma postać blokową, a blokami są klatki Jordana:

$$\begin{pmatrix} \lambda & 0 & 0 & \ldots & 0 & 0 \\ 1 & \lambda & 0 & \ldots & 0 & 0 \\ 0 & 1 & \lambda & \ldots & 0 & 0 \\ & \vdots & & & \vdots & \\ 0 & 0 & 0 & \ldots & \lambda & 0 \\ 0 & 0 & 0 & \ldots & 1 & \lambda \end{pmatrix}$$