Notatki (definicje, fakty) z Algebry 2R

Wykład01.pdf

Niech $S \supset R$ to rozszerzenie pierścieni, $\bar{a} \subseteq S^n$. Wtedy mówimy, że

$$I(\bar{a}/R) = \{g \in R[\bar{X}] : g(\bar{a}) = 0\} \lhd R[\bar{X}]$$

to *ideał* $\bar{a}$ *nad* R. Jeśli $I(\bar{a}/R) = (f_1, \dots, f_m)$, to mówimy, że $\bar{a}$ jest *rozwiązaniem ogólnym* układu $f_1, \dots, f_m$.

Niech $K \subset L_1, K \subset L_2$ to rozszerzenia ciał. Mówimy, że L_1 i L_2 są *izomorficzne nad* K, gdy istnieje izomorfizm między nimi, który jest identycznością na K. Notacja: $L_1 \cong_K L_2$.

Załóżmy, że $K \subset L_1$ i $K \subset L_2$ to rozszerzenia ciał, $\bar{a}_1 \subseteq L_1$, $\bar{a}_2 \subseteq L_2$, $|\bar{a}_1| = |\bar{a}_2|$. Wówczas $I(\bar{a}_1/K) = I(\bar{a}_2/K)$ wtedy i tylko wtedy, gdy istnieje izomorfizm $f\colon K[\bar{a}_1] \to K[\bar{a}_2]$ przekształcający $\bar{a}_1$ na $\bar{a}_2$ i ustalający K.

Niech $I \lhd K[\bar{X}]$. Wtedy istnieje ciało $L \supset K$ oraz $\bar{a} = (a_1, \dots, a_n) \subset L$ takie, że $f(\bar{a}) = 0$ dla każdego $f \in I$.

Niech $f \in K[X]$ stopnia dodatniego. Wtedy istnieje rozszerzenie K, w którym f ma pierwiastek.

Załóżmy, że $f \in K[X]$ nierozkładalny oraz dla $i = 1, 2$ mamy $L_i = K(a_i)$ i $f(a_i) = 0$ (w L_i). Wtedy $L_1 \cong_K L_2$. Ogólniej: załóżmy, że $\varphi\colon K_1 \xrightarrow{\cong} K_2$, $f_i \in K_i[X]$, $\varphi(f_1) = f_2$ i f_i nierozkładalny nad K_i, $L_1 = K_1(a_1)$, $L_2 = K_2(a_2)$, gdzie a_i jest pierwiastkiem f_i. Wtedy istnieje $\varphi \subseteq \psi\colon L_1 \xrightarrow{\cong} L_2$ taki, że $\psi(a_1) = a_2$.

Mówimy, że ciało $L \supset K$ jest *ciałem rozkładu* wielomianu $f \in K[X]$ nad K, gdy f rozkłada się w $L[X]$ na czynniki liniowe i $L = K(a_1, \dots, a_n)$, gdzie a_i to wszystkie pierwiastki f w L.

Jeśli $f \in K[X]$ ma stopień dodatni, to istnieje jedyne co do izomorfizmu nad K ciało rozkładu f nad K.

Wykład02.pdf

Ciało L jest *algebraicznie domknięte*, gdy każdy $f \in L[X]$ stopnia > 0 ma pierwiastek w L.

Każde ciało jest algebraicznie domknięte w pewnym jego rozszerzeniu.

Każde ciało K zawiera się w pewnym ciele algebraicznie domkniętym.

Mówimy, że ciało jest *ciałem prostym*, gdy nie zawiera podciał właściwych.

Każde ciało zawiera jedyne podciało proste.

Z dokładnością do izomorfizmu, $\mathbb{Q}$ i $\mathbb{Z}_p$ (dla p pierwszych) to wszystkie ciała proste.

1. $a \in R$ jest *pierwiastkiem z* 1 (stopnia $n > 0$), gdy $a^n = 1$
2. $\mu_n(R) = \{a \in R : a^n = 1\} < R^*$
3. $\mu(R) = \{a \in R : \exists n > 0\ \ a^n = 1\} = \bigcup_{n>0} \mu_n(R) < R^*$
4. $a \in R$ jest *pierwiastkiem pierwotnym (primitive) stopnia n z jedynki*, gdy n jest najmniejsze takie, że $a^n = 1$.

Oznaczamy $W_n(X) = X^n - 1$. W ciele o charakterystyce 0 ten wielomian ma tylko pierwiastki jednokrotne. W ciele o charakterystyce p każdy pierwiastek tego wielomianu ma krotność p^l, gdzie p^l to najwyższa potęga p dzieląca n.

Załóżmy, że $G < \mu(K)$ to grupa skończona rzędu n. Wtedy $G = \mu_n(K)$, G jest cykliczna i $p \nmid n$ (gdy $\operatorname{char} K = p$).

Niech $a \in \mu_n(K)$. Wtedy Jeśli a jest pierwiastkiem pierwotnym stopnia n z 1, to a generuje $\mu_n(K)$.

Załóżmy, że K jest ciałem skończonym i $p = \operatorname{char} K$. Wtedy $|K| = p^n$ dla pewnego n. Dla każdego $n > 0$ istnieje dokładnie jedno (co do izomorfizmu) ciało mocy p^n.

Wykład03.pdf

1. *a jest algebraiczny nad K*, gdy jest pierwiastkiem pewnego $f \in K[X] \setminus \{0\}$.
2. *a jest przestępny nad K*, gdy nie jest algebraiczny nad K.
3. Rozszerzenie $K \subset L$ jest *algebraiczne*, gdy każdy $l \in L$ jest algebraiczny nad K.
4. Rozszerzenie $K \subset L$ jest *przestępne*, gdy nie jest algebraiczne.
5. Liczba zespolona $z \in \mathbb{C}$ jest *algebraiczna / przestępna*, gdy jest algebraiczna / przestępna nad $\mathbb{Q}$.

a jest algebraiczny nad K wtedy i tylko wtedy, gdy $I(a/K) \neq \{0\}$.

Niech $K \subset L$ to rozszerzenie ciał. *Stopień rozszerzenia* $[L : K]$ to wymiar L jako przestrzeni liniowej nad K.

Załóżmy, że $a \in L \supset K$. Wtedy następujące warunki są równoważne:

1. a algebraiczny nad K
2. $K[a] = K(a)$
3. $[K(a) : K] < \infty$

Niech $K \subset L$ to rozszerzenie ciał, $a \in L$ jest algebraiczny nad K. Wtedy *wielomianem minimalnym a nad K* nazywamy moniczny wielomian generujący $I(a/K)$. Stopień tego wielomianu minimalnego nazywamy *stopniem a nad K*.

Wielomian minimalny f elementu a jest wielomianem unormowanym minimalnego stopnia takim, że $f(a) = 0$. $\deg f = [K(a) : K]$.

Niech $K \subset L \subset M$ to rozszerzenia ciał. Wtedy $[M : K] = [M : L][L : K]$.

$K_{alg}(L) = \{a \in L{:}a$ algebraiczny nad $K\}$ nazywamy *algebraicznym domknięciem ciała K w ciele L*. Jest ono podciałem L i nadciałem K. K jest algebraicznie domknięte w L, gdy $K_{alg}(L) = K$.

Algebraiczne domknięcie K w ciele algebraicznie domkniętym nazywamy *algebraicznym domknięciem*, które oznaczamy $\hat{K}$ lub K^{alg}.

Załóżmy, że $K \subset L \subset M$ to rozszerzenia ciał. Wtedy $K \subset M$ jest algebraiczne wtedy i tylko wtedy, gdy $K \subset L$ i $L \subset M$ są algebraiczne.

$K_{\mathrm{alg}}(L)$ jest algebraicznie domknięte w L.

Wykład04.pdf

Wielomiany cyklotomiczne

$$F_m(x) = \prod_{\substack{1 \leqslant k \leqslant m \\ \gcd(k,m)=1}} \left(x - e^{2\pi i \frac{k}{m}}\right)$$

$F_m(X)$ jest nierozkładalny w $\mathbb{Q}[X]$ (równoważnie w $\mathbb{Z}[X]$ z lematu Gaussa).

Załóżmy, że $\varepsilon \in \mathbb{C}$ jest pierwiastkiem pierwotnym z 1 stopnia m. Wtedy $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \varphi(m)$, bo F_m jest wielomianem minimalnym ε nad $\mathbb{Q}$.

(Lemat Liouville'a) Jeśli $a \in \mathbb{R}$ algebraiczna stopnia $N > 1$ nad $\mathbb{Q}$, to istnieje C taka, że dla każdego $p/q \in \mathbb{Q}$ mamy
$$\left|a - \frac{p}{q}\right| \geqslant \frac{C}{q^n}.$$

$L \supset K$ jest algebraicznym domknięciem ciała K, gdy L jest algebraicznie domknięte i rozszerzenie $L \subset L$ jest algebraiczne nad K. Oznaczamy $L = \hat{K} = K^{alg}$. $\hat{K}$ zawsze istnieje i jest jedyne co do izomorfizmu nad K.

Jeśli $f\colon K \xrightarrow{\cong} L$, to istnieje $f \subseteq \hat{f}\colon \hat{K} \xrightarrow{\cong} \hat{L}$.

Jeśli rozszerzenie $K \subset L$ jest algebraiczne, to istnieje zanurzenie L w $\hat{K}$ stałe na K.

Grupa Galois rozszerzenia $K \subset L$ to

$$G(L/K) = \{f \in \mathrm{Aut}(L) : f\,|_K = id_K\} < \mathrm{Aut}(L).$$

$G(\hat{K}/K)$ jest *absolutną grupą Galois ciała* K.

Jeśli $I(a/K) = I(b/K)$, to istnieje $f \in G(\hat{K}/K)$ taki, że $f(a) = b$.

Rozszerzenie algebraiczne ciał $K \subset L$ jest *normalne*, gdy każdy homomorfizm z L do $\hat{K}$, który jest identycznością na K, ma ten sam obraz.

Rozszerzenie algebraiczne $K \subset L$ jest normalne wtedy i tylko wtedy, gdy dla każdego $f \in G(\hat{K}/K)$ mamy $f[L] = L$.

Jeśli $K \subseteq L_1 \subseteq L$ i $K \subseteq L$ normalne, to $L_1 \subseteq L$ też.

Rozszerzenie algebraiczne $K \subset L$ jest normalne wtedy i tylko wtedy, gdy wielomian minimalny każdego elementu L rozkłada się nad L na czynniki liniowe.

Wykład05.pdf

Rozszerzenie ciał $K \subseteq L$ jest *skończone*, gdy $[L : K] < \infty$.

Rozszerzenie skończone $L \supseteq K$ jest normalne $\iff$ L jest ciałem rozkładu pewnego wielomianu $W \in K[X]$ nad K.

Normalne domknięcie ciała L w $\hat{K}$ nad K to

$$L_1 = \text{ciało generowane przez } \bigcup\{f[L] : f \in G(\hat{K}/K)\}.$$

Rozszerzenie $K \subseteq L$ jest normalne.

Gdy wielomian minimalny $a \in \hat{K}$ nad K, $W_a(X) \in K[X]$, ma w $\hat{K}$ tylko pierwiastki jednokrotne, to mówimy, że element a jest *rozdzielczy* nad K.

Rozszerzenie algebraiczne $K \subset L$ jest *rozdzielcze*, gdy każdy element L jest rozdzielczy nad K.

Wielomian $W(X) \in K[X]$ jest *rozdzielczy*, gdy ma tylko pierwiastki jednokrotne w $\hat{K}$.

Wielomian W nierozkładalny jest nierozdzielczy wtedy i tylko wtedy, gdy W i W' są względnie pierwsze.

W ciele o charakterystyce 0 wszystkie wielomiany minimalne są rozdzielcze. W ciele K o charakterystyce p wielomiany nierozdzielcze należą do $K[X^p]$.

Jeśli $K \subseteq L$ jest rozdzielcze i $K \subseteq L_1 \subseteq L$, to $L_1 \subseteq L$ rozdzielcze.

Rozszerzenie $K \subseteq L$ ciał skończonych jest rozdzielcze.

Każde rozszerzenie algebraiczne ciała charakterystki 0 jest rozdzielcze.

Zachodzi $\{f(a) : f \in G(\hat{K}/K)\} \leqslant \deg(a/K)$, a jeśli a jest rozdzielczy nad K, to zachodzi równość.

Element $a \in L$ nazywamy *elementem pierwotnym rozszerzenia $K \subseteq L$*, gdy $L = K(a)$.

(Twierdzenia Abela o elemencie pierwotnym) Jeśli rozszerzenie $K \subset K(a_1, \ldots, a_n) = L$ jest skończone i a_i są rozdzielcze nad K, to istnieje $a^* \in L$ rozdzielczy nad K taki, że $L = K(a^*)$. Inaczej, rozszerzenie skończone rozdzielcze jest proste.

Element $a \in L$ nazywamy *czysto nierozdzielczym (radykalnym)* nad K, gdy $W_a(X) \in K[X]$ ma tylko jeden pierwiastek w $\hat{K}$.

Rozszerzenie $K \subseteq L$ nazywamy *radykalnym (czysto nierozdzielczym)*, gdy każdy $a \in L$ jest radykalny nad K.

Wykład06.pdf

Rozdzielcze domknięcie K w L to

$$\mathrm{sep}_L(K) = \{a \in L : a \text{ rozdzielczy nad } K\}.$$

Czysto nierozdzielcze (radykalne) domknięcie K w L to

$$\mathrm{rad}_L(K) = \{a \in L : a \text{ radykalny nad } K\}.$$

Jeśli $K \subseteq L$ algebraiczne, to

$$K \subseteq \mathrm{sep}_L(K), \mathrm{rad}_L(K) \subseteq L \subseteq \hat{K}, \;\; \mathrm{sep}_L(K) \cap \mathrm{rad}_L(K) = K.$$

Rozdzielcze domknięcie K to $\hat{K}^s = \mathrm{sep}_{\hat{K}}(K)$.

Radykalne domknięcie K to $\hat{K}^r = \mathrm{rad}_{\hat{K}}(K)$.

Gdy $K \subseteq L \subseteq \hat{K}$, to $\mathrm{sep}_L(K) = \hat{K}^s \cap L$, $\mathrm{rad}_L(K) = \hat{K}^r \cap L$.

Załóżmy, że $K \subseteq L \subseteq M \subseteq \hat{K}$. Wtedy

$$K \subseteq_{\mathrm{rad}} L \subseteq_{\mathrm{rad}} M \iff K \subseteq_{\mathrm{rad}} M.$$

Gdy $\mathrm{char}\, K = 0$, to $\mathrm{sep}_L(K) = K^{\mathrm{alg}}(L)$ i $\mathrm{rad}_L(K) = K$ oraz $\hat{K}^s = \hat{K}$ i $\hat{K}^r = K$.

Stopień rozdzielczy ciała L nad K to $[L : K]_s = [\mathrm{sep}_L(K) : K]$. *Stopień radykalny ciała L nad K* to $[L : K]_r = [L : \mathrm{sep}_L(K)]$.

Jeśli $\mathrm{char}\, K = p > 0$ i $[L : K]_r < \infty$, to $[L : K]_r$ jest potęgą p.

Jeśli $K \subseteq L$ to rozszerzenie skończone $a \in L$, to $f_a \colon L \to L$, $f_a(x) = a \cdot x$ jest przekształceniem K-liniowym. *Normą* nazywamy $\mathrm{N}_{L/K}(a) = \det f_a$, a *śladem* $\mathrm{Tr}_{L/K}(a) = \mathrm{tr}\, f_a$.

Niech $K \subseteq L$ to rozszerzenie skończone, $\{f_1, \ldots, f_k\} = \{f \in \mathrm{Hom}(L, \hat{K}) : f|_K = id\}$, $k = [L : K]_s$, $a \in L$. Wtedy

$$\mathrm{N}_{L/K}(a) = \left(\prod_{i=1}^{k} f_i(a)\right)^{[L:K]_r}, \;\; \mathrm{Tr}_{L/K}(a) = [L : K]_r \sum_{i=1}^{k} f_i(a).$$

Wykład07.pdf

Rozszerzenie algebraiczne ciał $K \subset L$ jest *rozszerzeniem Galois*, gdy $\forall a \in L \setminus K \, \exists f \in G(L/K)$, $f(a) \neq a$.

Niech $G < \mathrm{Aut}(L)$. Wtedy *ciałem punktów stałych grupy G* nazywamy

$$L^G = \{a \in L : \forall f \in G f(a) = a\} = \bigcup_{f \in G} Fix(f).$$

Roszerzenie algebraiczne $K \subset L$ jest Galois wtedy i tylko wtedy, gdy $K = L^{G(L/K)}$.

Niech $K \subset L$ to rozszerzenie algebraiczne. Jest ono Galois wtedy i tylko wtedy, gdy jest rozdzielcze i normalne.

Niech $K \subset L \subset M \subset \hat{K}$. Jeśli $K \subset M$ Galois, to $L \subset M$ Galois.

Jeśli $G < \mathrm{Aut}(L)$ skończona, to $L^G \subset L$ Galois i $[L : L^G] = |G|$.

Jeśli $K \subset L$ to skończone rozszerzenie Galois, to $[L : K] = |G(L/K)|$.

Niech $K \subset L$ to rozszerzenie algebraiczne,

$$\begin{aligned} \mathcal{L} &= \{L' : K \subseteq L' \subseteq L\}, & \mathcal{G} &= \{H : H < G(L/K)\}, \\ \Gamma \colon \mathcal{L} &\to \mathcal{G}, & \Lambda \colon \mathcal{G} &\to \mathcal{L}, \\ L' &\overset{\Gamma}{\mapsto} G(L/L') < G(L/K), & G &\overset{\Lambda}{\mapsto} L^G \subseteq L. \end{aligned}$$

Jeśli $K \subset L$ jest rozszerzeniem skończonym, to Γ i Λ są wzajemnie odwrotne.

Jeśli $K \subset L$ jest skończonym rozszerzeniem Galois, to dla $H < G(L/K)$

$$H \lhd G(L/K) \iff K \subset L^H \text{ normalne Galois.}$$

Wykład08.pdf

Załóżmy, że rozszerzenie $K \subset L$ jest skończone Galois. Mówimy, że jest ono *abelowe / cykliczne*, gdy $G(L/K)$ jest *abelowa / cykliczna*.

Załóżmy, że $K \subset L_1 \subset L$ to rozszerzenia ciał. Jeśli $K \subset L$ abelowe/cykliczne, to $K \subset L_1$ i $L_1 \subset L$ też.

Załóżmy, że rozszerzenie $K \subset L$ cykliczne, $[L : K] = n$, $\zeta \in K$ to pierwiastek pierwotny z 1 stopnia n. Wtedy $\exists a \in K \;\; L = K(\sqrt[n]{a})$.

(Tw. Dedekinda o liniowej niezależności charakterów) Załóżmy, że $\alpha_1, \ldots, \alpha_n \in \mathrm{Aut}(L)$ i $(a_1, \ldots, a_n)$ to niezerowa krotka w L^n. Wtedy $\exists c \in L \;\; (\sum_{i=1}^n a_i \alpha_i)(c) \neq 0$, tzn. α_i są liniowo niezależne w przestrzeni L^L nad L.

Załóżmy, że $K \subset L$ to skończone rozszerzenie ciał. Mówimy, że jest ono *rozwiązalne*, gdy jest Galois i grupa $G(L/K)$ jest rozwiązalna. Mówimy, że jest ono *przez pierwiastniki*, jeśli istnieje ciąg zstępujący

$$L = L_0 \supset L_1 \supset \ldots \supset L_k = K$$

taki, że L_i jest ciałem rozkładu nad L_{i+1} wielomianu

$$\begin{aligned} X^{n_i} - b_i &\quad (\text{gdy } \operatorname{char} K = p \nmid n_i) \\ \text{lub } X^p - X - b_i &\quad (\text{gdy } \operatorname{char} K = p), \end{aligned}$$

gdzie $b_i \in L_{i+1}$.

Załóżmy, że $K \subset L$ to rozszerzenie skończone ciał. Wtedy $K \subset L$ jest roszerzeniem przez pierwiastniki wtedy i tylko wtedy, gdy istnieje L' takie, że $K \subset L'$ rozwiązalne.

Wykład09.pdf

Rozszerzenie $K \subset L$ nazywamy *przestępnym*, gdy istnieje $a \in L$ przestępny nad K (tzn. $I(a/K) = \{0\}$).

Rozszerzenie $K \subset L$ nazywamy *czysto przestępnym*, gdy każdy $a \in L \setminus K$ przestępny.

Element a jest przestępny nad K wtedy i tylko wtedy, gdy $K(a) \cong K(X)$.

Niech $U = \hat{U}$ to ciało oraz $K \subset U$ to jego podciało, a $F \subset K$ to podciało proste. *Operatorem domknięcia algebraicznego nad K* nazywamy $\operatorname{acl}_K \colon \mathcal{P}(U) \to \mathcal{P}(U), \operatorname{acl}_K(A) = K(A)^{\mathrm{alg}}$.

Zbiór $A \subseteq U$ jest *algebraicznie domknięty nad K*, gdy $A = \operatorname{acl}_K(A)$.

1. $\operatorname{acl}_K(\emptyset) = \hat{K}$
2. $\operatorname{acl}_K(\operatorname{acl}_K(A)) = \operatorname{acl}_K(A)$
3. $\operatorname{acl}_K(A) = \bigcup_{A_0 \subset_{\mathrm{fin}} A} \operatorname{acl}_K(A_0)$ (skończony charakter)
4. $a \in \operatorname{acl}_K(A \cup \{b\}) \setminus \operatorname{acl}_K(A) \implies b \in \operatorname{acl}_K(A \cup \{a\})$ (własność wymiany)

Zbiór $A \subset U$ jest *algebraicznie niezależny nad K*, gdy $\forall a \in A \ a \notin \operatorname{acl}_K(A \setminus \{a\})$. Równoważnie, dla dowolnych różnych $a_1, \ldots, a_n \in A$ i niezerowego $W(X_1, \ldots, X_n) \in K[\bar{X}]$ mamy $W(\bar{a}) \neq 0$.

Zbiór A jest *bazą przestępną zbioru $B \subset U$ nad K*, gdy A jest algebraicznie niezależny nad K i $A \subseteq B \subseteq \operatorname{acl}_K(A)$.

Moc (jakiejkolwiek) bazy przestępnej zbioru B nad K nazywamy wymiarem przestępnym B nad K i oznaczamy $\operatorname{tr\,deg}_K(B)$.

Jeśli $A \subseteq B \subseteq U$ i A jest algebraicznie niezależny nad K, to istnieje A' taki, że $A \subseteq A' \subseteq B$ i A' jest bazą przestępną B nad K.

Każde dwie bazy przestępne zbioru B nad K są równoliczne.

Zbiór $\{X_i : i \in I\} \subseteq K(\bar{X}) = U$ jest niezależny nad K i $\operatorname{tr\,deg}_K(U) = |I|$.

Jeśli $K \subset L \subset U$ oraz $\{a_i : i \in I\}$ to baza przestępna L/K, to

$$K(a_i : i \in I) \cong K(X_i : i \in I),$$

$$K \overset{\text{czysto przestępne}}{\subseteq} K(a_i : i \in I) \overset{\text{algebraiczne}}{\subseteq} L.$$

Wykład10.pdf

$(M, +, r)_{r \in R}$ to *moduł* (domyślnie lewostronny) nad R, jeśli

1. dla każdego r mamy operację mnożenia elementu modułu przez skalar r z lewej;
2. $(M, +)$ to grupa abelowa, jej zero 0 nazywamy zerem modułu M;
3. $r(m_1 + m_2) = rm_1 + rm_2$;

4. $(r_1 + r_2)m = r_1m + r_2m$;
5. $r_1(r_2m) = (r_1r_2)m$ (zgodność);
6. $1m = m$

Analogicznie możemy zdefiniować moduł prawostronny, z odpowiednio zmienionym aksjomatem zgodności. Jeśli R przemienny, to te pojęcia są równoważne.

Przestrzeń liniowa nad K to K-moduł.

Grupy abelowe to dokładnie $\mathbb{Z}$-moduły.

Grupa abelowa G jest $\mathrm{End}(G)$-modułem, gdzie $\mathrm{End}(G)$ to jej pierścień endomorfizmów.

Załóżmy, że $j\colon R \to \mathrm{End}(G)$ to homomorfizm pierścieni z jednością. Wtedy j wyznacza w G strukturę R-modułu, gdzie $r \cdot g = j(r)(g)$. Na odwrót, gdy $(G, +, r)$ to R-moduł, to możemy wziąć za j mnożenie skalarne.

Jeśli $R_1 \subset R$, to R jest modułem nad R_1.

Niech $j\colon R_1 \to R$ to homomorfizm pierścieni z jednością. Wtedy R-moduł jest R_1-modułem z operacją mnożenia przez wartość j.

Jeśli $I \subseteq R$ to ideał lewostronny, to I jest R-modułem.

Załóżmy, że M to R-moduł. Mówimy, że $N \subseteq M$ jest R-podmodułem M, gdy jest podgrupą abelową z dodawaniem (więc N jest niepusty) i zamknięty na mnożenie przez skalary.

Załóżmy, że M to R-moduł. Wtedy

1. $0 \cdot m = 0$;
2. $r \cdot 0 = 0$;
3. $(-1) \cdot m = -m$.

Niech M to R-moduł. Przekrój dowolnej niepustej rodziny podmodułów M jest podmodułem M.

Mówimy, że $\{0\} \subseteq M$ to podmoduł zerowy.

Jeśli $A \subseteq M$, to istnieje najmniejszy podmoduł $N \subseteq M$ zawierający A. Nazywamy go podmodułem generowanym przez A.

Jeśli N_1, N_2 to podmoduły M, to $N_1 + N_2$ też.

Produkt prosty R-modułów definiujemy podobnie jak dla przestrzeni liniowych i oznaczamy $M \times N$.

(Suma prosta wewnętrzna) Mówimy, że $M = N_1 \oplus \ldots \oplus N_k$, gdy N_i są podmodułami M i każdy element M się jednoznacznie zapisuje jako suma elementów N_1 (po jednym z każdego).

Niech $h\colon M \to N$ to homomorfizm R-modułów. Jeśli $N' \subset N$ jest podmodułem, to $h^{-1}[N'] \subset M$ też. Jeśli $M' \subset M$ jest podmodułem, to $h[M'] \subset N$ też.

Niech $M' \subset M$ to podmoduł. Wtedy $M/M' = \{x + M' : x \in M\}$ nazywamy modułem ilorazowym (ze standardowymi operacjami).

(zasadnicze tw. o homomorfizmie R-modułów)

(tw. o faktoryzacji)

Definiujemy $\mathrm{Hom}_R(M, N) = \{h\colon M \to N : h \text{ to homomorfizm}\}$.

M jest R-modułem prostym, gdy $M \neq \{0\}$ i każdy jego podmoduł jest zerowy lub całym M.

Pierścień endomorfizmów R-modułu M zapisujemy $\mathrm{End}_R(M)$.

(Lemat Schura) Jeśli M to R-moduł prosty, to $\mathrm{End}_R(M)$ to pierścień z dzieleniem.

Załóżmy, że M to R-moduł oraz $K = \mathrm{End}_R(M)$ to pierścień z dzieleniem (ciało nieprzemienne). Wtedy M jest też K-modułem.

Wykład11.pdf

Niech M to R-moduł. Układ $(m_i : i \in I) \subseteq M$ jest liniowo niezależny, gdy jego (skończona) kombinacja liniowa (ze współczynnikami z R) się zeruje dokładnie kiedy wszystkie współczynniki są zerami.

Zbiór $S \subseteq M$ jest liniowo niezależny, gdy układ z niego utworzony (bez powtórzeń) jest liniowo niezależny.

Zbiór $\mathcal{B} \subseteq M$ jest bazą R-modułu M, gdy $\mathcal{B}$ jest liniowo niezależny (nad R) i generuje M jako R-moduł.

Zbiory $\{0\}, \{m_0, m_0\}$ są liniowo zależne.

Rozpatrzmy $\mathbb{Q}$ jako $\mathbb{Z}$-moduł. Wtedy dowolna para jego elementów jest liniowo zależna.

Moduł $\mathbb{Q}$ nie ma bazy jako $\mathbb{Z}$-moduł!

(Abstrakcyjna) suma prosta (koprodukt) rodziny modułów $\{M_i : i \in I\}$ to

$$\coprod_{i\in I} M_i \cong \left\{ f \in \prod_{i\in I} M_i : f(i) = 0 \text{ dla prawie wszystkich } i \in I \right\}.$$

M jest wolnym R-modułem, gdy M ma bazę.

M jest wolnym R-modułem, z bazą $\{1\}$.

Jeśli M_i to wolne R-moduły, to $\coprod_{i\in I} M_i$ jest wolnym R-modułem.

Niech $A = \{a_i : i \in I\} \subseteq M$. Następujące warunki są równoważne:

1. A to baza M;
2. każdy element M się jednoznacznie przedstawia jako kombinacja R-liniowa A;
3. Każda funkcja z A w R-moduł się rozszerza do homomorfizmu z M.

Jeśli $A = \{a_i : i \in I\}$ to baza M, to Ra_i jest podmodułem M i $M = \bigoplus_{i \in I} Ra_i$.

Jeśli A to zbiór, to istnieje R-moduł o bazie A (koprodukt izomorficznych kopii R dla każdego elementu A).

Jeśli R jest pierścieniem przemiennym, to każde dwie bazy R-modułu wolnego M są równoliczne.

Każdy R-moduł jest homomorficznym obrazem R-modułu wolnego.

Załóżmy, że M, N to R-moduły, N jest wolny i $f \colon M \to N$ to epimorfizm. Wtedy $M \cong \ker f \oplus N$. Więcej: istnieje podmoduł $N' \subseteq M$ izomorficzny z N i $M = \ker f \oplus N'$.

Mówimy, że R-moduł N jest *projektywny*, gdy Dla każdego epimorfizmu $f \colon M \to N$ mamy $M = \ker f \oplus M'$ dla pewnego podmodułu $M' \subset M$. Mówimy, że f rozszczepia się (*splits*).

Dualnie, mówimy, że R-moduł M jest *iniektywny*, gdy dla każdego monomorfizmu $g \colon M \to N$ mamy $N = \operatorname{Im} g \oplus N'$ dla pewnego podmodułu $N' \subset N$.

Jeśli R to ciało, to każdy R-moduł jest iniektywny i projektywny.

Niech R to pierścień przemienny z jednością. Mówimy, że R-moduł jest *cykliczny*, gdy jest generowany przez jeden element a (równy Ra).

R-moduł jest cykliczny, jeśli jest izomorficzny z pewnym ilorazem R.

Niech M to R-moduł. Wtedy

1. dla $a \in M$ mówimy, że $I_a = \{r \in R : ra = 0\} \lhd R$ jest *torsją elementu* a;
2. mówimy, że $a \in M$ jest *torsyjny*, gdy $I_a \neq \{0\}$ (w przeciwnym razie *beztorsyjny*);
3. mówimy, że M jest *torsyjny*, gdy każdy jego element jest torsyjny (*beztorsyjny*, gdy każdy niezerowy beztorsyjny);
4. zbiór $M_t = \{a \in M : a \text{ torsyjny}\}$ nazywamy *częścią torsyjną modułu* M.

Załóżmy, że R jest dziedziną. Wtedy M_t jest podmodułem M i M/M_t jest beztorsyjny.

Grupy abelowe torsyjne / beztorsyjne to dokładnie $\mathbb{Z}$-moduły torsyjne / beztorsyjne.

Załóżmy, że R jest przemienny, M, N to R-moduły, $f \colon M \to N$ to epimorfizm, $M' = \ker f$, $N \cong M/M'$. Wtedy jeśli N, M' skończenie generowane, to M skończnie generowany i jeśli M skończenie generowany, to N skończenie generowany.

Załóżmy, że R to pierścień przemienny. Wtedy noetherowskość R jest równoważna temu, że podmoduły skończenie generowanego R-modułu są skończenie generowane.

Niech X to R-moduł wolny o bazie $M_1 \times M_2$ (jako zbiór). Niech $L \subseteq X$ to podmoduł generowany przez elementy „dające dwuliniowość”. Wtedy $f \colon M_1 \times M_2 \to X/L$ jest R-2-linowe. Moduł X/L nazywamy *produktem tensorowym* M_1 i M_2 oraz oznaczamy $M_1 \otimes M_2$.

Wykład12.pdf

Niech $f\colon M_1 \times M_2 \to M_1 \otimes M_2$ i $f(m_1, m_2) = m_1 \otimes m_2$. Wtedy f jest dwuliniowe (często oznaczane przez $\otimes$) oraz dla każdego dwuliniowego homomorfizmu $g\colon M_1 \times M_2 \to N$ istnieje jedyny homomorfizm R-liniowy $h\colon M_1 \otimes M_2 \to N$ taki, że $g = h \circ f$ (warunek uniwersalności). Intuicyjnie, $f = \otimes$ to najogólniejsze odwzorowanie 2-liniowe z $M_1 \times M_2$ w jakikolwiek R-moduł.

Powyższy warunek wyznacza iloczyn tensorowy z dokładnością do izomorfizmu.

Wykład13.pdf

Mamy $R[X] \otimes R[Y] \cong R[X, Y]$ w tym sensie, że $W(X) \otimes W(Y) = W(X)W(Y)$.

Jeśli M_n to wolny R-moduł wymiaru n o bazie $\{b_1, \ldots, b_n\}$ i analogicznie M_n wymiaru m o bazie $\{c_1, \ldots, c_m\}$, to $M_n \otimes M_M$ jest wolnym R-modułem o bazie $\{b_i \otimes c_j : 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$.

Iloczyn tensorowy jest co do izomorfizmu przemienny, łączny i ma element neutralny R (jako R-moduł).

Jeśli A generuje M i B generuje M, to $A \otimes B = \{a \otimes b : a \in A, b \in B\}$ generuje $M \otimes N$.

Załóżmy, że $f\colon M \to M'$, $g\colon N \to N'$ są R-liniowe. Wtedy istnieje jedyne $h\colon M \otimes N \to M' \otimes N'$ takie, że $h(m \otimes n) = f(m) \otimes g(n)$. Funkcję h nazywamy iloczynem tensorowym f i g.

$$M \otimes (\bigoplus_{i \in I} N_i) \cong \bigoplus_{i \in I} (M \otimes N_i)$$

Niech V to przestrzeń liniowa nad K. Oznaczmy $V^{\otimes n} = V \otimes \ldots \otimes V$. $\sigma \in S_n$ działa nad $V^{\otimes n}$ (permutuje współrzędne w tensorach prostych).

Niech $x \in V^{\otimes n}$. Mówimy, że x jest *symetryczny*, gdy dla każdego $\sigma \in S_n$ mamy $\sigma(x) = x$. Mówimy, że x jest *antysymetryczny*, gdy dla każdego $\sigma \in S_n$ mamy $\sigma(x) = \operatorname{sgn}(\sigma)x$.

Niech $\Lambda^n V$ to zbiór elementów antysymetrycznych a $S^n V$ to zbiór elementów symetrycznych $V^{\otimes n}$. Jeśli charakterystyka ciała to zero, to są to podprzestrzenie.

Mamy $V \otimes V = \Lambda^2 V \oplus S^2 V$, bo $x = \frac{1}{2}(x + \sigma(x)) + \frac{1}{2}(x - \sigma(x))$.

Wykład14.pdf

Podmoduł modułu wolnego nad PID jest wolny niewiększego wymiaru.

Podmoduł PID-modułu skończenie generowanego jest skończenie generowany.

Załóżmy, że M jest PID-modułem skończenie generowanym. Jeśli jest on beztorsyjny, to jest wolny. Więcej, rozkłada się on na sumę prostą części torsyjnej i jego pewnego podmodułu wolnego.

Niech R to PID, $p \in R$ jest nierozkładalny (a więc pierwszy), M to R-moduł. Mówimy, że

1. $m \in M$ jest *p-torsyjny*, gdy torsja $I_m = \{r \in R : rm = 0\} = (p^k)$ dla pewnego $k > 0$;
2. zbiór elementów zerowych lub p-torsyjnych M to *p-prymarna składowa M*;
3. M jest *p-prymarny*, gdy $M = M_p$.

Niech R to PID i M to R-moduł. Wtedy M_p jest podmodułem M_t. Więcej, $M_t = \oplus_{i \in I} M_{p_i}$, gdzie p_i to wszystkie elementy pierwsze R z dokładnością do stowarzyszenia.

Jeśli R-moduł jest cykliczny p-prymarny, to jest izomorficzny z ilorazem $R/(p^k)$ dla pewnego k.

Skończenie generowany moduł p-prymarny jest sumą prostą modułów cyklicznych.

Załóżmy, że M to skończenie generowany R-moduł p-prymarny. Wtedy

$$M \cong R/(p^{k_1}) \oplus \ldots \oplus R/(p^{k_l})$$

dla pewnych $1 \leqslant k_1 \leqslant \ldots \leqslant k_l$. Ponadto ciąg (k_i) jest wyznaczony jednoznacznie.

Niech R to PID i M to R-moduł skończenie generowany. Wtedy M się rozkłada na sumę prostą podmodułów nierozkładalnych cyklicznych, wyznaczoną jednoznacznie.

Wykład15.pdf

Załóżmy, że V to przestrzeń liniowa nad K skończonego wymiaru. Wtedy jest to skończenie generowany i torsyjny $K[X]$-moduł. Ponadto, $K[X]$ to PID, więc $V = \oplus_{p_i} V_{p_i}$ dla pewnych $p_i \in K[X]$ i

$$V_{p_i} \cong K[X]/(f_i^{k_1}) \oplus \ldots \oplus K[X]/(f_i^{k_l}) \quad (1 \leqslant k_1 \leqslant \ldots \leqslant k_l).$$

(Tw. Jordana) Załóżmy, że V to przestrzeń liniowa skończonego wymiaru nad ciałem algebraicznie domkniętym K i ψ to endomorfizm liniowy V. Wtedy istnieje baza Jordana $B \subseteq V$ taka, że $m_B(\psi)$ ma postać Jordana. Rozmiary klatek macierzy są wyznaczone jednoznacznie.

Załóżmy, że R to pierścien przemienny z $1 \neq 0$. R-algebra (przemienna) to R-moduł S z dodatkowym mnożeniem $\cdot \colon S \times S \to S$ takim, że S tworzy z nim i dodawaniem modułowym pierścień (przemienny). Ponadto musi zachodzić zgodność

$$r(ss') = (rs)s' = s(rs').$$

Załóżmy, że R to pierścien przemienny z $1 \neq 0$. R jest $\mathbb{Z}$-algebrą. $R[X], R[X,Y]$ to R-algebry. Jeśli $R \subset S$ to podpierścień z jedynką, to S jest R-algebrą.

Jeśli S jest R-algebrą z jednością 1, to $\eta \colon R \to S$ dana przez $\eta(r) = r \cdot 1$ jest homomorfizmem R-algebr.

Gdy R jest ciałem, to η jest monomorfizmem i R jest podciałem pierścienia S.

Gdy S to pierścień z jedynką i $R \subseteq S$ to podciało, to S jest R-algebrą.

Załóżmy, że S to R-algebra z jedynką i M to R-moduł. Wtedy $S \otimes_R M$ to R-moduł, lecz także S-moduł. Istnieje jedyna operacja mnożenia (na pierwszym argumencie tensora bazowego).

Jeśli G to $\mathbb{Z}$-moduł, to $\mathbb{Q} \otimes_Z G$ to $\mathbb{Q}$-moduł.

Jeśli V to przestrzeń liniowa nad $\mathbb{R}$, to $\mathbb{C} \otimes_{\mathbb{R}} V$ to przestrzeń liniowa nad $\mathbb{C}$ (kompleksyfikacja V).

Jeśli S_1, S_2 to R-algebry z jedynką, to ich iloczyn tensorowy nad R też.

(Nullstellensatz Hilberta) Niech $I \lhd K[\bar{X}]$ i $f \in K[\bar{X}]$ takie, że $Z_{\hat{K}}(I) \subseteq Z_{\hat{K}}(f)$, gdzie $\mathbb{Z}_L(I)$ to zbiór wspólnych pierwiastków I.

Załóżmy, że K to ciało algebraicznie domknięte takie, że układ równań wielomianowych $f_1(\bar{x}) = \ldots = f_k(\bar{x}) = 0$, gdzie $f_i \in K[\bar{X}]$, nie ma rozwiązań w K. Wtedy $1 \in (f_1, \ldots, f_k)$. $f_i \in K[\bar{X}]$.