PIERŚCIENIE I CIAŁA
Wykład 9

Niech $F : A \to B$ będzie homomorfizmem pierścieni. Dla wielomianu

$$f = a_0 + a_1x + ... + a_nx^n \in A[x]$$

definiujemy

$$F(f) = F(a_0) + F(a_1)x + ... + F(a_n)x^n.$$

Otrzymujemy w ten sposób funkcję $F : A[x] \to B[x]$, która jest homomorfizmem, przy czym $\operatorname{st} F(f) \leqslant \operatorname{st} f$.

Twierdzenie 1 (**kryterium redukcyjne**). *Niech A będzie pierścieniem Gaussa, B będzie pierścieniem całkowitym, zaś $U(A)$, $U(B)$ będą odpowiednio ich ciałami ułamków. Załóżmy, że istnieje homomorfizm $F : A \to B$. Jeżeli $f \in A[x]$ jest taki, że $\operatorname{st} F(f) = \operatorname{st} f$ i wielomian $F(f)$ jest nierozkładalny w $U(B)[x]$, to f jest nierozkładalny w $U(A)[x]$.*

Przykład 1. Niech $f(x) = x^5+3x^2+1$. Ponieważ $\mathbb{Z}_2$ jest ciałem, więc możemy zastosować kryterium redukcyjne dla homomorfizmu $r_2 : \mathbb{Z} \to \mathbb{Z}_2$. Mamy

$$r_2(f)(x) = x^5 + x^2 + 1.$$

Zgodnie z kryterium redukcyjnym wystarczy wykazać, że wielomian $r_2(f)$ jest nierozkładalny w $\mathbb{Z}_2[x]$. Gdyby taki nie było, to mielibyśmy rozkład $r_2(f) = gh$ dla pewnych wielomianów $f, g \in \mathbb{Z}_2[x]$ stopnia mniejszego niż 5. Ponieważ $\operatorname{st} g + \operatorname{st} h = \operatorname{st} f = 5$, więc mamy dwa przypadki:

(1) Jeden z wielomianów g, h ma stopień 1. Ale wtedy wielomian ten ma postać $x - a$, gdzie $a \in \mathbb{Z}_2$, co oznacza, że $r_2(f)$ ma pierwiastek w $\mathbb{Z}_2$. Ale

$$r_2(f)(0) = 1, \quad r_2(f)(1) = 1 \oplus_2 1 \oplus_2 1 = 1,$$

czyli ten przypadek jest niemożliwy.

(2) Jeden z wielomianów g, h ma stopień 2. Z (1) wiemy, że wielomian ten nie może mieć pierwiastka w $\mathbb{Z}_2$. Jedynymi wielomianami stopnia 2 w $\mathbb{Z}_2[x]$ są:

$$x^2, \quad x^2 + 1, \quad x^2 + x, \quad x^2 + x + 1,$$

przy czym tylko ostatni z nich nie ma pierwiastka w $\mathbb{Z}_2$. Zatem wystarczy sprawdzić, że $r_2(f)$ nie dzieli sie przez $x^2 + x + 1$. Wykonując dzielenie z resztą otrzymujemy

$$r_2(f)(x) = x^5 + x^2 + 1 = (x^3 + x^2)(x^2 + x + 1) + 1,$$

więc $r_2(f)$ nie dzieli sie przez x^2+x+1. Także ten przypadek jest wiec niemożliwy.

Rozszerzenia ciał

Niech K będzie podciałem ciała E. Wtedy E nazywamy ***rozszerzeniem ciała*** K. Ponieważ elementy ciała E możemy dodawać i mnożyć przez elementy ciała K, więc rozszerzenie E ciała K można traktować jako przestrzeń liniową (wektorową) nad K. Wymiar tej przestrzeni nazywamy ***stopniem rozszerzenia*** i oznaczamy przez $(E : K)$. Możliwe są dwa przypadki:

I. Stopień $(E : K) = n$ jest liczbą skończoną. W tym przypadku mówimy, że E jest rozszerzeniem skończonym ciała K. Istnieje wtedy baza skończona $e_1, ..., e_n \in E$ przestrzeni wektorowej E nad ciałem K. Oznacza to, że

(1) wektory $e_1, ..., e_n$ są liniowo niezależne nad K, czyli jeżeli

$$\sum_{i=1}^{n} a_i e_i = 0,$$

gdzie $a_1, ..., a_n \in K$, to $a_1 = ... = a_n = 0$,

(2) każdy wektor $u \in E$ jest kombinacją liniową

$$u = \sum_{i=1}^{n} u_i e_i \tag{1}$$

dla pewnych $u_1, ..., u_n \in K$.

Rozkład (1) jest jednoznaczny i elementy $u_1, ..., u_n \in K$ nazywamy współrzędnymi wektora $u \in E$ w bazie $e_1, ..., e_n$.

II. Stopień $(E : K) = \infty$ jest nieskończony. W tym przypadku mówimy, że E jest rozszerzeniem nieskończonym ciała K. Wtedy również istnieje baza przestrzeni E, ale jest to zbiór nieskończony $\{e_t\}_{t\in T} \subset E$. Dowolny skończony układ wektorów $e_{t_1}, ..., e_{t_n}$ jest liniowo niezależny nad K i każdy wektor $u \in E$ ma rozwinięcie postaci

$$u = \sum_{i=1}^{n} u_i e_{t_i} \tag{2}$$

dla pewnych wektorów $e_{t_1}, ..., e_{t_n}$ i współczynników $u_1, ..., u_n \in K$ zwanych współrzędnymi wektora u. Jeśli $u \neq 0$, to rozkład taki jest jednoznaczny.

Przykład 2.
I. Przykładem rozszerzenia skończonego jest ciało liczb zespolonych $\mathbb{C}$ jako rozszerzenie ciała $\mathbb{R}$. Mamy $(\mathbb{C} : \mathbb{R}) = 2$ i bazą tego rozszerzenia są elementy 1, i. Rozwinięciem elementu $z \in \mathbb{C}$ w tej bazie jest zapis $z = a + bi$, gdzie $a, b \in \mathbb{R}$.
II. Przykładem rozszerzenia nieskończonego jest ciało liczb rzeczywistych $\mathbb{R}$ jako rozszerzenie ciała $\mathbb{Q}$.

Niech E będzie ciałem skończonym. Gdyby $\mathrm{char}(E) = 0$, to E miałoby podpierścień izometryczny z $\mathbb{Z}$, co jest niemożliwe. Zatem $\mathrm{char}(E) = p > 0$ jest liczbą pierwszą (patrz wykład 8).

Twierdzenie 2. *Jeżeli E jest ciałem skończonym, to liczba jego elementów jest postaci p^n, gdzie $p = \mathrm{char}(E)$ jest liczbą pierwszą i $n \in \mathbb{N}$.*

Dowód. Ponieważ $\mathrm{char}(E) = p$, więc E zawiera podciało K izomorficzne z $\mathbb{Z}_p$ (patrz wykład 8). Zatem E jest rozszerzeniem K i stopień tego rozszerzenia jest skończony, gdyż E nie może zawierać nieskończonej bazy. Niech $n = (E : K)$ i $e_1, e_2, ..., e_n$ będzie bazą rozszerzenia E ciała K. Wtedy każdy element $u \in E$ ma jednoznaczne przedstawienie

$$u = u_1 e_1 + u_2 e_2 + ... + u_n e_n,$$

gdzie $u_1, u_2, ..., u_n \in K$. Zatem liczba wszystkich elementów u ciała E jest równa liczbie wszystkich ciągów $(u_1, u_2, ..., u_n)$, których wyrazy należą do p-elementowego ciała K. Stąd E ma p^n elementów. □

Z twierdzenia 2 wynika np. że nie istnieje ciało o sześciu elementach, ale twierdzenie to nie rozstrzyga problemu istnienia ciał skończonych o p^n elementach. Dla dowolnej liczby pierwszej $p > 1$ istnieje ciało $\mathbb{Z}_p$ o p elementach. W dalszej części wykładów zobaczymy, że dla dowolnej liczby pierwszej $p > 1$ i dowolnej liczby naturalnej n istnieje ciało mające p^n elementów.

Rozszerzenia ciał możemy otrzymać przy użyciu pierścieni ilorazowych pierścienia wielomianów. Konstrukcja ta jest analogiczna do konstrukcji pierścieni $\mathbb{Z}_n$ jako pierścieni ilorazowych $\mathbb{Z}/(n)$. Dla danego ciała K i wielomianu $w \in K[x]$ otrzymujemy ideał $I = (w)$ pierścienia wielomianów $K[x]$. Elementami pierścienia ilorazowego $E = K[x]/I$ są klasy abstrakcji względem relacji

$$f \sim g \;\Leftrightarrow\; w \text{ dzieli } f - g,$$

gdzie $f, g \in K[x]$.

Załóżmy, że w ma stopień n. Dla dowolnego $f \in K[x]$ stosując wzór na dzielenie z resztą dostajemy

$$f = qw + r_w(f),$$

gdzie $r_w(f) \in K[x]$ jest resztą z dzielenia f przez w, a więc $\operatorname{st} r_w(f) < n$. Otrzymujemy w ten sposób funkcję r_w określoną na pierścieniu $K[x]$ o wartościach w zbiorze $K[x]_n$ wszystkich wielomianów z $K[x]$ stopnia mniejszego niż n. Zbiór $K[x]_n$ ze zwykłym dodawaniem wielomianów i mnożeniem określonym wzorem

$$f \odot g = r_w(fg)$$

jest pierścieniem.

Funkcja r_w jest homomorfizmem, gdyż jeśli $f = pw + r_w(f)$, $g = qw + r_w(g)$ są wzorami na dzielenie z resztą f i g, to

$$f + g = (p + q)w + r_w(f) + r_w(g) \tag{3}$$

i $\operatorname{st}(r_w(f) + r_w(g)) \leqslant \max\{\operatorname{st} r_w(f), \operatorname{st} r_w(g)\} < n$, więc (3) jest wzorem na dzielenie z resztą $f + g$ przez w. Stąd

$$r_w(f + g) = r_w(f) + r_w(g).$$

Ponadto

$$fg = (pqw + qr_w(f) + pr_w(g))w + r_w(f)r_w(g), \tag{4}$$

skąd wynika, że

$$r_w(fg) = r_w(r_w(f)r_w(g)) = r_w(f) \odot r_w(g).$$

Zatem r_w jest homomorfizmem i w konsekwencji obraz $r_w(K[x]) = K[x]_n$ jest izomorficzny z pierścieniem $K[x]/(w)$.

Jeżeli w jest wielomianem nierozkładalnym, to ideał (w) jest ideałem maksymalnym, a więc $K[x]/(w)$ jest ciałem (patrz wykład 6). Zatem również $K[x]_n$ jest ciałem i jest to rozszerzenie ciała K. Elementami ciała $K[x]_n$ są wielomiany postaci

$$f = a_0 + a_1x + ... + a_{n-1}x^{n-1},$$

gdzie $a_0, a_1, ..., a_{n-1} \in K$, przy czym jeśli $f = 0$, to $a_0 = a_1 = ... = a_{n-1} = 0$. Zatem ciąg $1, x, ..., x^{n-1}$ jest bazą rozszerzenia $K[x]_n$, czyli $(K[x]_n : K) = n$.

Przykład 3. Niech $K = \mathbb{R}$ i $w(x) = x^2 + 1$. Wielomian w jest nierozkładalny w $\mathbb{R}[x]$, gdyż nie ma pierwiastków rzeczywistych. Stąd $E = \mathbb{R}[x]_2$ jest rozszerzeniem ciała $\mathbb{R}$. Jego elementy mają postać $a + bx$, gdzie $a, b \in \mathbb{R}$, przy czym $x^2 = w(x) - 1$, więc

$$x \odot x = r_w(x^2) = -1.$$

Ciało E jest więc izomorficzne z ciałem liczb zespolonych $\mathbb{C}$.

Jeśli wielomian w nie jest nierozkładalny, to $K[x]_n$ nie jest ciałem.

Przykład 4. Niech $K = \mathbb{Z}_2$ i $w(x) = x^2 + 1$. W ciele $\mathbb{Z}_2$ mamy $w(x) = (x + 1)^2$, więc w nie jest nierozkładalny. Elementami pierścienia $\mathbb{Z}_2[x]_2$ są: 0, 1, x, $1 + x$, przy czym

$$(1 + x) \odot (1 + x) = r_w((x + 1)^2) = r_w(w) = 0,$$

zatem $1 + x$ jest dzielnikiem zera.

Przykład 5. Aby otrzymać ciało, które jest rozszerzeniem ciała $K = \mathbb{Z}_2$ bierzemy wielomian $w(x) = x^2 + x + 1$. Jest to wielomian nierozkładalny, gdyż nie ma w $\mathbb{Z}_2$ pierwiastka. Zatem w tym przypadku $\mathbb{Z}_2[x]_2 = \{0, 1, x, 1 + x\}$ jest ciałem. W odróżnieniu od poprzedniego przykładu mamy

$$(1 + x) \odot (1 + x) = r_w((x + 1)^2) = r_w(x^2 + 1) = x.$$

Otrzymaliśmy w ten sposób ciało czteroelementowe.

Stosując tę konstrukcję do ciała $K = \mathbb{Z}_p$, gdzie p jest liczbą pierwszą i wielomianu nierozkładalnego $w \in \mathbb{Z}_p[x]$ stopnia n otrzymujemy ciało skończone o p^n elementach.

Ciągi rozszerzeń

Będziemy rozważać rozszerzenia „piętrowe". Przykładem są ciała $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, z których każde następna jest rozszerzeniem poprzedniego.

Twierdzenie 3. *Jeżeli E jest rozszerzeniem skończonym ciała K i F jest rozszerzeniem skończonym ciała E, to F jest rozszerzeniem skończonym ciała K oraz*

$$(F : K) = (F : E)(E : K). \tag{5}$$

Dowód. Niech $u_1, ..., u_n \in E$ będzie bazą rozszerzenia E ciała K, zaś $v_1, ..., v_m$ będzie bazą rozszerzenia F ciała E. Wystarczy wykazać, że iloczyny $u_i v_j$ tworzą bazę F nad K.

Sprawdzamy najpierw liniową niezależność tych wektorów. W tym celu załóżmy, że

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} u_i v_j = 0,$$

gdzie $a_{ij} \in K$. Mamy

$$0 = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} u_i \right) v_j = \sum_{j=1}^{m} b_j v_j,$$

przy czym $b_j = \sum_{i=1}^{n} a_{ij} u_i \in E$, gdyż $a_{ij} \in K \subset E$ oraz $u_i \in E$. Ale wektory $v_1, ..., v_m$ są liniowo niezależne nad ciałem E, więc $b_1 = ... = b_m = 0$. Zatem

$$\sum_{i=1}^{n} a_{ij} u_i = 0$$

dla $j = 1, ..., m$ i z liniowej niezależności wektorów $u_1, ..., u_n$ nad ciałem K wynika, że $a_{ij} = 0$ dla wszystkich i, j.

Niech teraz $a \in F$. Istnieją $b_1, ..., b_m \in E$ takie, że

$$a = \sum_{j=1}^{m} b_j v_j.$$

Następnie każde b_j można zapisać jako

$$b_j = \sum_{i=1}^{n} c_{ij} u_i,$$

gdzie $c_{ij} \in K$. Zatem

$$a = \sum_{j=1}^{m} \sum_{i=1}^{n} c_{ij} u_i v_j. \qquad \square$$

Korzystając kilkakrotnie z tego twierdzenia widzimy, że jeśli $K_1 \subset K_2 \subset ... \subset K_n$ jest ciągiem rozszerzeń skończonych, to K_n jest rozszerzeniem skończonym ciała K_1 oraz

$$(K_n : K_1) = (K_n : K_{n-1})(K_{n-1} : K_{n-2})...(K_2 : K_1). \tag{6}$$

Elementy algebraiczne i elementy przestępne

Niech E będzie rozszerzeniem ciała K. Element $a \in E$ jest ***algebraiczny*** nad ciałem K, jeśli istnieje wielomian $f \in K[x]$ taki, że $\operatorname{st} f \geqslant 1$ i $f(a) = 0$. Elementy ciała E, które nie są algebraiczne nazywamy elementami ***przestępnymi*** nad K. ***Liczbami algebraicznymi*** (lub ***przestępnymi***) nazywamy elementy ciała liczb zespolonych $\mathbb{C}$, które są algebraiczne (lub przestępne) nad ciałem $\mathbb{Q}$.

Przykłady

1. Liczby wymierne są liczbami algebraicznymi. Liczba $a \in \mathbb{Q}$ jest pierwiastkiem wielomianu $x - a \in \mathbb{Q}[x]$.

2. Pierwiastki z liczb wymiernych są liczbami algebraicznymi. Liczba $\sqrt[n]{a}$, gdzie $a \in \mathbb{Q}$ jest pierwiastkiem wielomianu $x^n - a \in \mathbb{Q}[x]$.

3. Wartości funkcji cos i sin dla kątów postaci $\alpha = \frac{n\pi}{m}$, gdzie $n, m \in \mathbb{Z}$, $m \neq 0$ są liczbami algebraicznymi. Dla przykładu pokażemy, że $\cos \frac{2\pi}{5}$ jest liczbą algebraiczną. Aby to wykazać korzystamy ze wzoru De Moivre'a:

$$\left(\cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}\right)^5 = \cos 2\pi + i \sin 2\pi = 1.$$

Ale

$$\begin{aligned}\left(\cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}\right)^5 = {} & \cos^5 \frac{2\pi}{5} - 10 \cos^3 \frac{2\pi}{5} \sin^2 \frac{2\pi}{5} + 5 \cos \frac{2\pi}{5} \sin^4 \frac{2\pi}{5} \\ & + i \left(5 \cos^4 \frac{2\pi}{5} \sin \frac{2\pi}{5} - 10 \cos^2 \frac{2\pi}{5} \sin^3 \frac{2\pi}{5} + \sin^5 \frac{2\pi}{5}\right),\end{aligned}$$

a więc

$$\begin{aligned}1 &= \cos^5\frac{2\pi}{5} - 10\cos^3\frac{2\pi}{5}\sin^2\frac{2\pi}{5} + 5\cos\frac{2\pi}{5}\sin^4\frac{2\pi}{5}\\ &= \cos^5\frac{2\pi}{5} - 10\cos^3\frac{2\pi}{5}\left(1-\cos^2\frac{2\pi}{5}\right) + 5\cos\frac{2\pi}{5}\left(1-\cos^2\frac{2\pi}{5}\right)^2\\ &= 16\cos^5\frac{2\pi}{5} - 20\cos^3\frac{2\pi}{5} + 5\cos\frac{2\pi}{5}.\end{aligned}$$

Zatem $\cos\frac{2\pi}{5}$ jest pierwiastkiem wielomianu $16x^5 - 20x^3 + 5x - 1 \in \mathbb{Q}[x]$.

Twierdzenie 4. *Zbiór liczb algebraicznych jest przeliczalny.*

Dowód. Zbiór $\mathbb{Q}_n[x]$ wszystkich wielomianów o współczynnikach wymiernych stopnia co najwyżej n jest zbiorem ciągów postaci $(a_0, a_1, ..., a_n, 0, 0, ...)$, gdzie $a_0, a_1, ..., a_n \in \mathbb{Q}$, a więc jest równoliczny z $\mathbb{Q}^{n+1}$. Zatem $\mathbb{Q}_n[x]$ jest zbiorem przeliczalnym. Stąd zbiór wszystkich wielomianów

$$\mathbb{Q}[x] = \bigcup_{n=0}^{\infty} \mathbb{Q}_n[x]$$

jest również zbiorem przeliczalnym. Każdy wielomian $f \in \mathbb{Q}$ stopnia $n \geqslant 1$ ma skończony zbiór pierwiastków zespolonych Z_f. Zatem zbiór wszystkich liczb algebraicznych

$$A = \bigcup_{f \in \mathbb{Q}[x]\setminus\{0\}} Z_f$$

jest przeliczalny. □

Wniosek 1. *Zbiór wszystkich rzeczywistych (a więc tym bardziej zespolonych) liczb przestępnych jest nieprzeliczalny.*

Wiadomo, że liczby π oraz e są przestępne. Stąd również dowolne potęgi tych liczb o wykładniku naturalnym są liczbami przestępnymi. Ponadto liczby $\pi + q$ i $e + q$ oraz $q\pi$ i qe, gdzie $q \in \mathbb{Q}$ są przestępne. Nie wiadomo, czy liczby $\pi + e$ i $\pi \cdot e$ są niewymierne, a więc tym bardziej nie wiadomo, czy są one przestępne.

Załóżmy, że ciało E jest rozszerzeniem ciała K i $a \in E$ jest elementem algebraicznym nad K. Istnieje niezerowy wielomian $f \in K[x]$ najmniejszego stopnia, dla którego $f(a) = 0$. Mówimy, że $f \in K[x]$ jest ***wielomianem minimalnym*** elementu a, jeśli $f \in K[x]$ jest niezerowym wielomianem najmniejszego stopnia takim, że $f(a) = 0$ i f jest ***unormowany***, czyli współczynnik przy najwyższej potędze x w f jest równy 1. Stopień takiego wielomianu f nazywamy ***stopniem elementu*** a.

Twierdzenie 5. *Niech $a \in E$ i $f \in K[x]$ będzie niezerowym wielomianem najmniejszego stopnia, dla którego $f(a) = 0$. Wtedy*

(1) *wielomian f jest nierozkładalny w $K[x]$,*
(2) *jeśli $g(a) = 0$ dla pewnego $g \in K[x]$, to f dzieli g,*
(3) *jeśli wielomian f jest unormowany, to f jest wyznaczony w sposób jednoznaczny.*

Dowód. (1) Aby wykazać, że f jest nierozkładalny, załóżmy, że tak nie jest, czyli $f = gh$, gdzie $g, h \in K[x]$, $\operatorname{st} g < \operatorname{st} f$ i $\operatorname{st} h < \operatorname{st} f$. Wtedy $0 = f(a) = g(a)h(a)$, zatem $g(a) = 0$ lub

$h(a) = 0$. Jest to sprzeczne z założeniem, że f jest niezerowym wielomianem najmniejszego stopnia, dla którego $f(a) = 0$. Zatem f jest wielomianem nierozkładalnym w $K[x]$.

(2) Załóżmy, że $g(a) = 0$ dla pewnego wielomianu $g \in K[x]$. Dzieląc g przez f z resztą otrzymujemy $g = qf + r$ gdzie $q, r \in K[x]$, $\operatorname{st} r < \operatorname{st} f$. Zatem

$$0 = g(a) = q(a)f(a) + r(a) = r(a).$$

Ponieważ f jest niezerowym wielomianem najmniejszego stopnia, dla którego $f(a) = 0$ i $\operatorname{st} r < \operatorname{st} f$, więc $r = 0$, czyli f dzieli g.

(3) Załóżmy, że $f_1 \in K[x]$ jest również wielomianem minimalnym elementu a. Wtedy przyjmując $h = f - f_1$ otrzymujemy wielomian $h \in K[x]$ taki, że $h(a) = f(a) - f_1(a) = 0$ i $\operatorname{st} h < \operatorname{st} f$. Z założenia, że f jest wielomianem minimalnym dla a wynika, że $h = 0$, czyli $f_1 = f$. □