PIERŚCIENIE I CIAŁA
Wykład 10

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 $f(a) = 0$. Przypomnijmy, 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 1. *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.*

Przypomnijmy, że elementy pierścienia są ze sobą stowarzyszone, jeśli jeden różni się od drugiego czynnikiem odwracalnym. W pierścieniu wielomianów $K[x]$ elementami odwracalnymi są wszystkie niezerowe elementy ciała K. Zatem wielomiany $f, g \in K[x]$ są stowarzyszone, gdy $f = ag$ dla pewnego niezerowego $a \in K$.

Wniosek 1. *$f \in K[x]$ będzie wielomianem minimalnym elementu algebraicznego $a \in E$. Jeżeli $g \in K[x]$ jest wielomianem nierozkładalnym takim, że $g(a) = 0$, to g jest stowarzyszony z f w $K[x]$ i w konsekwencji* $\operatorname{st} g = \operatorname{st} f$.

Dowód. Z twierdzenia 1 (2) wiemy, że f dzieli g, a ponieważ g jest nierozkładalny, to g jest stowarzyszony z f, a więc $\operatorname{st} g = \operatorname{st} f$. □

Widzimy więc, że $f \in K[x]$ jest wielomianem minimalnym elementu algebraicznego $a \in E$ wtedy i tylko wtedy, gdy
1) $f(a) = 0$,
2) f jest nierozkładalny,
3) współczynnik przy najwyższej potędze x w f jest równy 1.

Przykład 1. Niech $f(x) = x^n - 2 \in \mathbb{Q}[x]$. Z kryterium Eisensteina zastosowanego dla $p = 2$ wynika, że f jest wielomianem nierozkładalnym w $\mathbb{Q}[x]$. Zatem f jest wielomianem minimalnym liczby algebraicznej $a = \sqrt[n]{2}$.

Niech E będzie rozszerzeniem ciała K i $M \subset E$. Przez $K(M)$ oznaczmy iloczyn mnogościowy wszystkich rozszerzeń ciała K zawartych w E i zawierających zbiór M. Ciało $K(M)$ jest najmniejszym podciałem ciała E będącym rozszerzeniem K i zawierającym zbiór M. W przypadku, gdy $M = \{a_1, ..., a_m\}$ jest zbiorem skończonym, zamiast $K(M)$ piszemy $K(a_1, ..., a_m)$. Jeśli $M = \{a\}$ jest zbiorem jednopunktowym, to

$$K(a) = \left\{ \frac{f(a)}{g(a)} : f, g \in K[x],\ g(a) \neq 0 \right\}. \tag{1}$$

Rozszerzenie $K(a)$ jest więc ciałem, którego elementami są wartości w punkcie a funkcji wymiernych $\frac{f(x)}{g(x)}$, gdzie $f, g \in K[x]$.

Uwaga 1. Jeżeli M, N są podzbiorami ciała E, to $K(M \cup N) = K(M)(N)$. W szczególności jeśli $a, b \in E$, to $K(a, b) = K(a)(b)$.

Następne twierdzenie pokazuje, że jeżeli $a \in E$ jest elementem algebraicznym nad K, to we wzorze (1) zamiast funkcji wymiernych wystarczy brać wielomiany.

Twierdzenie 2. *Jeżeli $a \in E$ jest elementem algebraicznym nad K, to*

$$K(a) = \{f(a) : f \in K[x]\}.$$

Dowód. Oznaczmy $K[a] = \{f(a) : f \in K[x]\}$. Oczywiście $K[a] \subset K(a)$. Ponadto wielomiany stałe należą do $K[a]$, czyli $K \subset K[a]$, zaś biorąc $f(x) = x$ widzimy, że $a \in K[a]$. Zatem wystarczy wykazać, że $K[a]$ jest ciałem. W tym celu należy wykazać, że jeśli $f \in K[x]$ jest taki, że $f(a) \neq 0$, to $f(a)^{-1} = h(a)$ dla pewnego wielomianu $h \in K[x]$.

Niech $g \in K[x]$ będzie wielomian minimalnym elementu a. Ponieważ $f(a) \neq 0$, więc g nie dzieli f. Ponadto g jest nierozkładalny, więc g, f są względnie pierwsze. Stosując algorytm Euklidesa można zatem znaleźć wielomiany $h, k \in K[x]$ takie, że

$$hf + kg = 1.$$

Zatem

$$1 = h(a)f(a) + k(a)g(a) = h(a)f(a),$$

a więc $f(a)^{-1} = h(a) \in K[a]$. Stąd $K[a]$ jest ciałem, a więc $K[a] = K(a)$. □

Uwaga 2. Element $a \in E$ jest algebraiczny nad K wtedy i tylko wtedy, gdy istnieje n takie, że elementy $1, a, ..., a^n$ są liniowo zależne nad K. Rzeczywiście, fakt, że $1, a, ..., a^n$ są liniowo zależne nad K oznacza, że istnieją $a_0, a_1, ..., a_n \in K$, nie wszystkie równe 0 takie, że $a_0 + a_1 a + ... + a_n a^n = 0$, czyli a jest pierwiastkiem niezerowego wielomianu $f(x) = a_0 + a_1 x + ... + a_n x^n \in K[x]$.

Jeśli więc $a \in E$ jest elementem przestępnym nad K, to dla każdego n elementy $1, a, ..., a^n$ są liniowo niezależne. Wynika stąd, że $(K(a) : K) = \infty$. W szczególności biorąc dowolną liczbę przestępną $a \in \mathbb{R}$ widzimy, że $\mathbb{Q}(a) \subset \mathbb{R}$, więc

$$(\mathbb{R} : \mathbb{Q}) = (\mathbb{Q}(a) : \mathbb{Q}) = \infty.$$

Twierdzenie 3. *Niech $a \in E$ będzie elementem algebraicznym nad K i $h \in K[x]$ będzie wielomianem minimalnym dla a. Jeżeli $n = \operatorname{st} h$, to $(K(a) : K) = n$ i elementy $1, a, ..., a^{n-1}$ tworzą bazę rozszerzenia $K(a)$.*

Dowód. Wykażemy najpierw, że elementy $1, a, ..., a^{n-1}$ są liniowo niezależne nad K. Załóżmy w tym celu, że

$$a_0 + a_1 a + ... + a_{n-1} a^{n-1} = 0,$$

gdzie $a_0, a_1, ..., a_{n-1} \in K$. Oznacza to, że a jest pierwiastkiem wielomianu $g = a_0 + a_1 x + ... + a_{n-1} x^{n-1} \in K[x]$ stopnia mniejszego od $n = \operatorname{st} h$. Ponieważ h jest wielomianem minimalnym dla a, więc $g = 0$, czyli $a_0 = a_1 = ... = a_{n-1} = 0$. Zatem elementy $1, a, ..., a^{n-1}$ są liniowo niezależne nad K.

Z twierdzenia 2 wiemy, że $K(a) = \{f(a) : f \in K[x]\}$. Niech $b \in K(a)$. Wtedy $b = f(a)$ dla pewnego wielomianu $f \in K[x]$. Dzielimy f przez h z resztą i otrzymujemy $f = qh + r$, gdzie $q, r \in K[x]$ i $\operatorname{st} r < \operatorname{st} h = n$. Zatem $r = b_0 + b_1 x + ... + b_{n-1} x^{n-1}$ i

$$b = f(a) = q(a)h(a) + r(a) = r(a) = b_0 + b_1 a + ... + b_{n-1} a^{n-1}.$$

Pokazuje to, że $1, a, ..., a^{n-1}$ tworzą bazę rozszerzenia $K(a)$. □

Przykład 2.
1. Liczba i jest elementem algebraicznym nad $\mathbb{R}$ stopnia 2. Jej wielomianem minimalnym jest $f(x) = x^2 + 1$. Zatem $1, i$ jest bazą rozszerzenia $\mathbb{R}(i)$. Elementy tego rozszerzenia mają postać $a + bi$, gdzie $a, b \in \mathbb{R}$. Zatem $\mathbb{R}(i) = \mathbb{C}$.
2. Z przykładu 1 wiemy, że $a = \sqrt[n]{2}$ jest liczbą algebraiczną i jej wielomian minimalny ma stopień n. Stąd $(\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}) = n$ i bazą rozszerzenia $\mathbb{Q}(\sqrt[n]{2})$ jest ciąg

$$1, \sqrt[n]{2}, (\sqrt[n]{2})^2, ..., (\sqrt[n]{2})^{n-1}.$$

Mówimy, że rozszerzenie E ciała K jest ***algebraiczne***, jeżeli każdy element $a \in E$ jest algebraiczny nad K, czyli jest pierwiastkiem niezerowego wielomianu o współczynnikach z K.

Twierdzenie 4. *Jeżeli rozszerzenie E ciała K ma wymiar skończony, to E jest algebraiczne.*

Dowód. Niech $(E : K) = n$. W n wymiarowej przestrzeni liniowej dowolny układ złożony z więcej niż n wektorów jest liniowo zależny, więc jeżeli $a \in E$, to układ $1, a, a^2, ..., a^n$ jest liniowo zależny, czyli

$$a_0 + a_1 a + a_2 a^2 + ... + a_n a^n = 0,$$

gdzie $a_0, a_1, ..., a_n \in K$ nie są wszystkie równe 0. Zatem a jest pierwiastkiem wielomianu $f(x) = a_0 + a_1 x + ... + a_n x^n \in K[x]$, czyli a jest elementem algebraicznym. □

Kwaterniony tworzą pierścień $\mathbb{H}$ zawierający ciało liczb zespolonych $\mathbb{C}$ jako podpierścień. Ale $\mathbb{H}$ nie jest pierścieniem przemiennym, więc nie jest ciałem. Zatem nie jest to rozszerzenie ciała $\mathbb{C}$.

Okazuje się, że nie istnieje skończone (czyli skończonego wymiaru) rozszerzenie ciała $\mathbb{C}$. Rzeczywiście, gdyby E było takim rozszerzeniem, to zgodnie z twierdzeniem 4 dowolny element $a \in E$ byłby algebraiczny nad $\mathbb{C}$. Oznacza to, że a byłby pierwiastkiem pewnego wielomianu $f \in \mathbb{C}[x]$. Ale wszystkie pierwiastki wielomianu o współczynnikach zespolonych są liczbami zespolonymi, więc $a \in \mathbb{C}$. Stąd $E = \mathbb{C}$.

Istnieją jednak nieskończenie wymiarowe rozszerzenia ciała $\mathbb{C}$. Takim rozszerzeniem jest ciało $\mathbb{C}(x)$ wszystkich funkcji wymiernych, czyli funkcji postaci $\frac{f(x)}{g(x)}$, gdzie $f, g \in \mathbb{C}[x]$, $g \neq 0$.

Zauważmy, że jeśli F jest ciałem pośrednim między K i E oraz $a \in E$ jest elementem algebraicznym nad K, to $f(a) = 0$, gdzie $f \in K[x]$ jest wielomianem minimalnym dla a. Oczywiście $f \in F[x]$, a więc

$$(F(a) : F) \leqslant \operatorname{st} f = (K(a) : K). \tag{2}$$

Nierówności ta może być ostra. Np. jeśli $F = E$, to $(F(a) : F) = (E : E) = 1$, zaś $K(a)$ może być różne od K.

Uwaga 3. Jeśli $c \in E$ jest elementem algebraicznym nad K, to

$$(K(c) : K) < \infty,$$

więc z twierdzenia 4 wynika, że $K(c)$ jest algebraicznym rozszerzeniem K.

Bardziej ogólnie, jeżeli $a_1, ..., a_n \in E$ są algebraiczne nad K, to

$$K(a_1, ..., a_n) = ((K(a_1))(a_2)...)(a_n)$$

i korzystając z nierówności (2) otrzymujemy

$$(K(a_1, ..., a_n) : K) = (K(a_1) : K)(K(a_1, a_2) : K(a_1))...(K(a_1, ..., a_n) : K(a_1, ..., a_{n-1})) \leqslant$$
$$\leqslant (K(a_1) : K)(K(a_2) : K)...(K(a_n) : K) < \infty.$$

Rozszerzenie $K(a_1, ..., a_n)$ jest więc skończone i z twierdzenia 4 wynika, że jest ono algebraiczne.

Wniosek 2. *Niech E będzie rozszerzeniem ciała K. Jeżeli $a, b \in E$ są algebraiczne nad K, to również elementy $a + b$, $-a$, ab i a^{-1} (jeśli $a \neq 0$) są algebraiczne nad K. W konsekwencji zbiór wszystkich elementów ciała E algebraicznych nad K jest ciałem.*

Dowód. Jeżeli $a, b \in E$ są elementami algebraicznymi nad K, to $K(a, b)$ jest rozszerzeniem algebraicznym ciała K. Zatem każdy element ciała $K(a, b)$ jest algebraiczny nad K. W szczególności $a + b$, $-a$, ab i a^{-1} (jeśli $a \neq 0$) są algebraiczne nad K. □

Z wniosku 2 wiemy, że jeżeli $a, b \in E$ są algebraiczne nad K, to $a + b$ jest elementem algebraicznym nad K. Powstaje pytanie, jak znaleźć wielomian o współczynnikach z K, którego $a + b$ jest pierwiastkiem. Wiemy, że $f(a) = 0$ i $g(b) = 0$ dla pewnych niezerowych wielomianów $f, g \in K[x]$. Załóżmy, że $a_0 = a, a_1, a_2, ..., a_n$ są wszystkimi pierwiastkami f, zaś $b_0 = b, b_1, b_2, ..., b_m$ są wszystkimi pierwiastkami g w pewnym rozszerzeniu ciała K. Wtedy $a + b$ jest pierwiastkiem wielomianu

$$h(x) = \prod_{i,j}(x - a_i - b_j) \tag{3}$$

i wielomian ten ma współczynniki z ciała K. Podobnie wielomian

$$k(x) = \prod_{i,j}(x - a_i b_j),$$

którego jednym z pierwiastków jest iloczyn ab ma współczynniki z ciała K.

Wielomiany otrzymane w ten sposób nie muszą być wielomianami minimalnymi dla $a + b$ i ab.

Przykład 3. Niech $K = \mathbb{Q}$, $a = \sqrt{2}$, $b = \sqrt{3}$. Wtedy $ab = \sqrt{6}$ ma wielomian minimalny $h(x) = x^2 - 6$. Wielomianem minimalnym dla a jest $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$, zaś wielomianem minimalnym dla b jest $g(x) = x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$, więc powyższa konstrukcja daje nam wielomian

$$k(x) = (x - \sqrt{2}\sqrt{3})(x - (-\sqrt{2})\sqrt{3})(x - \sqrt{2}(-\sqrt{3}))(x - (-\sqrt{2})(-\sqrt{3})) =$$
$$= (x - \sqrt{2}\sqrt{3})^2(x + \sqrt{2}\sqrt{3})^2 = (x - \sqrt{6})^2(x + \sqrt{6})^2 = (x^2 - 6)^2.$$

Korzystając z wniosku 2 możemy także stwierdzić, że pewne liczby są przestępne. Jak wiemy π jest liczbą przestępną i dla dowolnej liczby wymiernej q liczba $\pi + q$ jest przestępna. Fakt ten można wzmocnić: dla dowolnej liczby algebraicznej a suma $b = a + \pi$ jest liczbą przestępną. Rzeczywiście, gdyby b było liczbą algebraiczną, to $\pi = b - a$ byłoby liczbą algebraiczną, a tak nie jest. Podobnie dla dowolnej liczby algebraicznej $a \neq 0$ iloczyn $b = a\pi$ jest liczbą przestępną. Prawdziwy jest jednak znacznie mocniejszy wynik.

Twierdzenie 5. *Niech E będzie rozszerzeniem ciała K i $a \in E$ będzie elementem przestępnym nad K. Wtedy każdy element $b \in K(a) \setminus K$ jest przestępny.*

Dowód. Jeśli $b \in K(a) \setminus K$, to b ma postać $b = \frac{f(a)}{g(a)}$, gdzie $f, g \in K[x]$ są względnie pierwsze i $\operatorname{st} f > 0$. Gdyby b nie był przestępny, to istniałby wielomian

$$h(x) = a_0 + a_1 x + ... + a_n x^n \in K[x],$$

taki, że $n \geqslant 1$, $a_n \neq 0$ i $h(b) = 0$. Podstawiając $b = \frac{f(a)}{g(a)}$ otrzymujemy

$$a_0 + a_1 \frac{f(a)}{g(a)} + a_2 \frac{f(a)^2}{g(a)^2} + ... + a_n \frac{f(a)^n}{g(a)^n} = 0.$$

Mnożąc obie strony przez $g(a)^n$ dostajemy

$$a_0 g(a)^n + a_1 f(a) g(a)^{n-1} + a_2 f(a)^2 g(a)^{n-2} + ... + a_n f(a)^n = 0.$$

Oznacza to, że a jest pierwiastkiem pewnego wielomianu o współczynnikach z K. Ale a jest elementem przestępnym, więc jedynym takim wielomianem jest wielomian zerowy. Zatem

$$a_0 g^n + a_1 f g^{n-1} + a_2 f^2 g^{n-2} + ... + a_n f^n = 0.$$

Stąd f dzieli g^n i g dzieli f^n. Ponieważ f, g są względnie pierwsze, więc f dzieli g i g dzieli f. Oznacza to, że wielomiany f, g są stowarzyszone, co jest sprzeczne z założeniem, że są one względnie pierwsze. □

Twierdzenie 6. *Jeżeli E jest rozszerzeniem ciała K i $a \in E$ jest elementem przestępnym nad K, to rozszerzenie $K(a)$ jest izomorficzne z ciałem funkcji wymiernych $K(x)$.*

Dowód. Dla $\frac{f}{g} \in K(x)$ przyjmujemy

$$\Phi\left(\frac{f}{g}\right) = \frac{f(a)}{g(a)}.$$

Wzór ten definiuje homomorfizm $\Phi : K(x) \to K(a)$. Mamy $\Phi(K(x)) = K(a)$ i aby wykazać, że Φ jest izomorfizmem wystarczy sprawdzić, że funkcja Φ jest różnowartościowa. W tym celu wystarczy wykazać, że $\operatorname{Ker} \Phi = \{0\}$.

Załóżmy, że $\frac{f}{g} \in \operatorname{Ker} \Phi$. Wtedy $\frac{f(a)}{g(a)} = 0$, więc $f(a) = 0$. Ponieważ a jest elementem przestępnym, więc $f = 0$, czyli $\frac{f}{g} = 0$. Zatem $\operatorname{Ker} \Phi = \{0\}$, co dowodzi, że Φ jest izomorfizmem. □

Wniosek 3. *Jeżeli $a, b \in E$ są elementami przestępnymi nad K, to rozszerzenia $K(a)$, $K(b)$ są izomorficzne.*

W szczególności rozszerzenia $\mathbb{C}(\pi)$ i $\mathbb{C}(e)$ są izomorficzne ze sobą i izomorficzne z ciałem funkcji wymiernych $\mathbb{C}(x)$.

Z wykładu 9 wiemy, że rozszerzenia ciała K można konstruować jako pierścienie ilorazowe postaci $K[x]/(f)$, gdzie $f \in K[x]$ jest wielomianem nierozkładalnym. Następne twierdzenie podaje inny model takiego pierścienia ilorazowego.

Twierdzenie 7. *Niech $a \in E$ jest elementem algebraicznym nad K. Wtedy rozszerzenie $K(a)$ jest izomorficzne z $K[x]/(f)$, gdzie $f \in K[x]$ jest wielomianem minimalnym elementu a.*

Dowód. Z twierdzenia 2 wiemy, że $K(a) = \{g(a) : g \in K[x]\}$. Dla $g \in K[x]$ oznaczamy $\Phi(g) = g(a)$. Funkcja $\Phi : K[x] \to E$ jest homomorfizmem pierścienia $K[x]$ na ciało $K(a)$. Zatem $K(a)$ jest izomorficzne z pierścieniem ilorazowym $K[x]/\operatorname{Ker}\Phi$.

Warunek $g \in \operatorname{Ker}\Phi$ oznacza, że $g(a) = 0$. Z twierdzenia 1 wiemy, że g dzieli się przez wielomian minimalny f, czyli $g \in (f)$. Stąd $\operatorname{Ker}\Phi = (f)$. □

Wniosek 4. *Jeżeli elementy algebraiczne $a, b \in E$ mają ten sam wielomian minimalny, to rozszerzenia $K(a)$, $K(b)$ są izomorficzne.*

Przykład 4.
1. Ciało liczb zespolonych $\mathbb{C}$ jest rozszerzeniem ciała $\mathbb{R}$ o jednostkę urojoną i, która jest elementem algebraicznym nad $\mathbb{R}$, przy czym jej wielomian minimalny to $f(x) = x^2 + 1$. Twierdzenie 7 pokazuje, że ciało $\mathbb{C}$ jest izomorficzne z pierścieniem ilorazowym $\mathbb{R}[x]/(f)$.
2. Może się zdarzyć, że dwa elementy algebraiczne mają różne wielomiany minimalne, ale rozszerzenia o te elementy sa identyczne. Np. $h(x) = x^2 - 2x + 2$ jest wielomianem minimalnym liczby $1 + i$. Zatem liczby i oraz $1 + i$ mają różne wielomiany minimalne, ale $\mathbb{R}(i) = \mathbb{R}(1 + i) = \mathbb{C}$. Rzeczywiście, $1 + i \in \mathbb{C}$, więc $\mathbb{R}(1 + i) \subset \mathbb{C} = \mathbb{R}(i)$, a ponadto $i = (1 + i) - 1 \in \mathbb{R}(1 + i)$, więc $\mathbb{R}(i) \subset \mathbb{R}(1 + i)$.

Ciało rozkładu wielomianu

Konstrukcja pierścienia $K[x]/(f)$ prowadzi też do następującego twierdzenia.

Twierdzenie 8. *Niech K będzie ciałem i $f \in K[x]$, $\operatorname{st} f > 0$. Istnieje rozszerzenie E ciała K, w którym wielomian f ma pierwiastek.*

Dowód. Zastępując ewentualnie f jednym z jego czynników w rozkładzie na czynniki nierozkładalne, możemy założyć, że f jest nierozkładalny. Wtedy ideał (f) generowany przez ten wielomian jest maksymalny, a więc pierścień ilorazowy $E = K[x]/(f)$ jest ciałem. Dla wielomianu $g \in K[x]$ przez $[g]$ oznaczamy jego klasę abstrakcji względem relacji odpowiadającej ideałowi (f).

Dla $a \in K$ klasa abstrakcji wielomianu stałego $[a]$ nie zawiera innego elementu ciała K. Jeśli bowiem $b \in K$ i $b \in [a]$, to $b - a$ dzieli się przez wielomian f. Ale $\operatorname{st} f \geqslant 1$, wiec $b - a = 0$, czyli $b = a$. Zatem funkcja $\phi : K \to K[x]/(f)$ określona wzorem $\phi(a) = [a]$ jest różnowartościowa i jest to homomorfizm. Ciało E zawiera więc podciało $\phi(K)$ izomorficzne z K i utożsamiając $a \in K$ z $\phi(a) = [a]$ możemy uważać E za rozszerzenie ciała K.

Niech $f(x) = a_0 + a_1x + ... + a_nx^n$. Mamy

$$0 = [f] = [a_0] + [a_1][x] + ... + [a_n][x]^n = a_0 + a_1[x] + ... + a_n[x]^n,$$

zatem $[x] \in E$ jest pierwiastkiem wielomianu f. □

Jeśli wielomian f ma pierwiastek a, to $f(x) = (x - a)g$ i pozostałe pierwiastki f są pierwiastkami wielomianu g. Ta uwaga w połączeniu z twierdzeniem 8 pozwala otrzymać następujący wynik.

Twierdzenie 9. *Niech K będzie ciałem i $f \in K[x]$, $\operatorname{st} f > 0$. Istnieje rozszerzenie E ciała K zawierające wszystkie pierwiastki wielomianu f, czyli takie, że*

$$f(x) = a(x - a_1)(x - a_2)...(x - a_n),$$

gdzie $a \in K$, $a_1, a_2, ..., a_n \in E$.

Ciało $K(a_1, a_2, ..., a_n)$ nazywamy ***ciałem rozkładu wielomianu*** f. Jest to więc najmniejsze podciało ciała E zawierające K i wszystkie pierwiastki wielomianu f. Jeśli f jest wielomianem stałym, to uznajemy K za ciało jego rozkładu.

Ciało rozkładu wielomianu zależy od rozszerzenia E ciała K, ale jest w pewnym sensie wyznaczone w sposób jednoznaczny. Jeżeli F i F_1 są ciałami rozkładu wielomianu $f \in K[x]$, to istnieje izomorfizm $\Phi : F \to F_1$ taki, że $\Phi(a) = a$ dla $a \in K$. Taki izomorfizm nazywamy K***-izomorfizmem***.

Ogólna konstrukcja ciał skończonych

Z wykładu 9 wiemy, że jeśli K jest ciałem skończonym, to liczba jego elementów ma postać p^n, gdzie $p > 1$ jest liczbą pierwszą i $n \in \mathbb{N}$. Poznaliśmy także pewną szczególną metodę konstrukcji takich ciał. Dowód następnego twierdzenia opisuje ogólną konstrukcję.

Twierdzenie 10. *Dla dowolnej liczby pierwszej $p > 1$ i $n \in \mathbb{N}$ istnieje ciało K o p^n elementach.*

Dowód. Rozważmy wielomian

$$f(x) = x^{p^n} - x \in \mathbb{Z}_p[x].$$

Zauważmy, że $f'(x) = p^n x^{p^n-1} - 1$, czyli $f'(x) = -1$ w $\mathbb{Z}_p[x]$. Stąd f nie ma pierwiastków wielokrotnych. Niech K będzie ciałem rozkładu f. Zatem $K = \mathbb{Z}_p(a_1, ..., a_{p^n})$, gdzie $a_1, ..., a_{p^n}$ są pierwiastkami f i jak wiemy $a_i \neq a_j$ dla $i \neq j$.

Mamy $f(0) = f(1) = 0$, więc 0 i 1 są pierwiastkami f. Ponadto

$$(a_i + a_j)^p = \sum_{k=0}^{p} \binom{p}{k} a_i^k a_j^{p-k}.$$

Ale $\binom{p}{k}$ dzieli się przez p dla $0 < k < p$, zatem

$$(a_i + a_j)^p = a_i^p + a_j^p$$

w ciele K. Następnie

$$\begin{aligned}(a_i + a_j)^{p^n} &= ((a_i + a_j)^p)^{p^{n-1}} = (a_i^p + a_j^p)^{p^{n-1}} = ((a_i^p + a_j^p)^p)^{p^{n-2}} = \\ &= ... = a_i^{p^n} + a_j^{p^n} = a_i + a_j,\end{aligned}$$

a więc $f(a_i + a_j) = 0$. Ponieważ 1 jest pierwiastkiem f, więc wynika stąd w szczególności, że dowolne $k \in \mathbb{Z}_p$ jest pierwiastkiem f. Dalej

$$(a_i a_j)^{p^n} = a_i^{p^n} a_j^{p^n} = a_i a_j,$$

a więc $f(a_i a_j) = 0$. Ponadto jeśli $a_i \neq 0$, to $f\left(a_i^{-1}\right) = 0$. Zatem $\{a_1, ..., a_{p^n}\}$ jest podciałem ciała K i zawiera $\mathbb{Z}_p$. Ponieważ K jest najmniejszym ciałem zawierającym $\mathbb{Z}_p$ i wszystkie pierwiastki $a_1, ..., a_{p^n}$, więc $K = \{a_1, ..., a_{p^n}\}$. Widzimy więc, że ciało K ma p^n elementów. □

Uwaga 4. Dwa ciała skończone mające taką samą liczbę elementów są izomorficzne.