

Charakterystyka.

Niech K będzie ciałem. Homomorfizm pierścieni $\mathbf{Z} \ni n \mapsto n \cdot 1 \in K$ ma jądro, które jest ideałem $\mathbf{Z}$, więc jest postaci (p) dla pewnego $p \in \mathbf{Z}$ zwanego *charakterystyką* ciała K . Obraz tego homomorfizmu – izomorficzny z $\mathbf{Z}/(p)$ – jest dziedziną, więc p jest liczbą pierwszą lub zerem.

Rozszerzenie pojedyncze.

Niech E/K będzie rozszerzeniem ciał (znaczy to, że K jest podciałem E). Dla $e \in E$ oznaczamy przez $K(e)$ najmniejsze podciało ciała E zawierające $K \cup \{e\}$. Aby zrozumieć strukturę tego ciała posłużymy się homomorfizmem ewaluacji: $\eta: K[X] \rightarrow E$, $\eta(P(X)) = P(e)$. Jak poprzednio: obraz η jest dziedziną, więc $\ker \eta$ jest albo ideałem pierwszym maksymalnym, generowanym przez pewien wielomian nierozkładalny $Q(X)$, albo też ideałem zerowym. W pierwszym przypadku mówimy, że e jest *algebraiczny* nad K ; mamy wówczas $K(e) \simeq K[X]/(Q(X))$ i $Q(e) = 0$. W drugim przypadku η rozszerza się na ciało ułamków pierścienia $K[X]$ dając izomorfizm ciał $K(X) \simeq K(e)$; mówimy, że e jest *przestępny* nad K .

Rozszerzenia algebraiczne.

Rozszerzenie E/K nazywamy algebraicznym, jeśli każdy element E jest algebraiczny nad K . Rozszerzenie jest *skończone*, jeśli jego *stopień* $\dim_K E$ jest skończony. Rozszerzenie skończone jest algebraiczne: potęgi dowolnego elementu są liniowo zależne nad K . W szczególności rozszerzenie pojedyncze o element algebraiczny jest algebraiczne.

Lemat. Niech E/F i F/K będą rozszerzeniami. Jeśli oba te rozszerzenia są algebraiczne, to i E/K jest algebraiczne; jeśli oba są skończone, to i E/K jest skończone.

Dowód. Skończoność: jeśli (e_i) jest bazą E nad F , zaś (f_j) bazą F nad K , to $(e_i f_j)$ jest bazą E nad K .

Algebraiczność. Jeśli $e \in E$, to e jest pierwiastkiem wielomianu o współczynnikach z F . Rozszerzamy K o kolejne współczynniki, a na końcu o e . Każdy etap jest rozszerzeniem pojedynczym o element algebraiczny, więc jest rozszerzeniem skończonym. A zatem ciało uzyskane na końcu jest skończonym rozszerzeniem K , skąd wynika algebraiczność e nad K .

Algebraiczne domknięcie.

Rozszerzenie E/K jest algebraicznym domknięciem, jeśli jest algebraiczne i jeśli ciało E nie ma nietrywialnych algebraicznych rozszerzeń. (Ten drugi warunek można też wyrazić tak: nie ma w $E[X]$ nierozkładalnych wielomianów stopnia > 1 .)

Twierdzenie. Każde ciało ma algebraiczne domknięcie, jedyne z dokładnością do izomorfizmu.

Dowód.

Istnienie. Moc algebraicznego rozszerzenia K nie przekracza mocy $K \times \mathbf{Z}$; weźmy zbiór X o mocy jeszcze większej, zawierający K . Wśród rozszerzeń algebraicznych ciała K zawartych w X wybierzmy maksymalne E (LKZ). Gdyby E miało nietrywialne rozszerzenie algebraiczne, to miałoby też rozszerzenie postaci $E[X]/(Q(X))$, a to dałoby się izomorficznie włożyć w X – sprzeczność z maksymalnością E . Jest więc E domknięciem algebraicznym K .

Jedyność. Niech E, E' będą domknięciami algebraicznymi K . Wybieramy (LKZ) maksymalną parę (F, f) , gdzie ciało F spełnia $K \subseteq F \subseteq E$, a $f: F \rightarrow E'$ jest włożeniem ciał identycznościowym na K .

Pokażemy, że $F = E$. Gdyby nie, to niech $e \in E \setminus F$. Wtedy $F(e) \simeq F[X]/(Q(X))$. Wielomian $Q(X)$, po przekształceniu współczynników przez f , ma pierwiastek e' w E' . Dostajemy $(f(F))(e') \simeq F[X]/(Q(X)) \simeq F(e)$, co przeczy maksymalności pary (F, f) .

Ciało E' jest algebraicznym rozszerzeniem K , więc i algebraicznym rozszerzeniem $f(E)$; ale $f(E) \simeq E$ nie ma nietrywialnych rozszerzeń algebraicznych. Stąd $f(E) = E'$.

Ciała skończone.

Na algebraicznym domknięciu E ciała $\mathbf{F}_p$ działa automorfizm Frobeniusa: $F(x) = x^p$. Zbiór punktów stałych n -tej potęgi F jest podciałem $\mathbf{F}_{p^n}$ ciała E . Elementy $\mathbf{F}_{p^n}$ to pierwiastki wielomianu $X^{p^n} - X$, których jest dokładnie p^n gdyż wielomian ów nie ma pierwiastków wielokrotnych z uwagi na niezerowość swej pochodnej.

Dalej, każde podciało E mające p^n elementów jest równe $\mathbf{F}_{p^n}$. Istotnie, grupa mnożenia tego podciała ma rząd $p^n - 1$, więc ka/dy jej element spełnia równanie $X^{p^n-1} = 1$, zatem należy do $\mathbf{F}_{p^n}$.

Jeśli L jest innym ciałem o p^n elementach, to $\mathbf{F}_p \subseteq L \subseteq E'$, gdzie E' jest algebraicznym domknięciem L (więc i $\mathbf{F}_p$). Niech $\phi: E' \rightarrow E$ będzie izomorfizmem. Wtedy $\phi(L)$ jest podciałem E o p^n elementach, więc $\phi(L) = \mathbf{F}_{p^n}$. Pokazaliśmy:

Twierdzenie. *Dla każdej liczby pierwszej p i każdej liczby całkowitej dodatniej n istnieje ciało o p^n elementach, jedyne z dokładnością do izomorfizmu.*