Przygotowanie

21 września 2014

Wykłady:

1. Wstęp.
   Relacja równoważności, zbiory ilorazowe (zbiór klas reszt modulo n, liczby wymierne), odwzorowania, działania algebraiczne. Grupa reszt **Zn** modulo n.
2. Teoria grup.
   Podgrupy, warstwy, ich własności, twierdzenie Lagrange'a dla skończonych grup, podgrupy normalne, grupy ilorazowe, homomorfizmy i izomorfizmy grup, twierdzenie Cayleya, grupy cykliczne i ich podgrupy, izomorficzna klasyfikacja grup cyklicznych, grupy przekształceń, twierdzenia o izomorfizmach grup, produkty i sumy proste grup, działanie grupy na zbiorze, sprzężenie, centrum, centralizator, normalizator, twierdzenia Sylowa o grupach skończonych, grupy proste, grupy rozwiązalne, grupy nilpotentne, struktura skończenie generowanych grup abelowych.
3. Teoria pierścieni.
   Podpierścienie, ideały jednostronne i obustronne, podciała, charakterystyka. dzielniki zera, elementy odwracalne i elementy nilpotentne, pierścień reszt **Zn,** pierścień szeregów potęgowych, homomorfizmy i izomorfizmy pierścieni, pierścienie ilorazowe, związki z teorią liczb, twierdzenia o izomorfizmach pierścieni, ideały pierwsze i ideały maksymalne, ciało klas reszt **Zp,** ciała ułamków, chińskie twierdzenie o resztach.
4. Teoria podzielności w dziedzinach całkowitości.
   Relacje podzielności i stowarzyszenia, elementy rozkładalne i nierozkładalne, elementy pierwsze, NWD, NWW, pierścienie ideałów głównych, pierścienie euklidesowe, pierścienie faktorialne.
5. Teoria ciał.
   Rozszerzenie ciał, stopień rozszerzenia, element algebraiczny i jego wielomian minimalny, rozszerzenie ciał proste, rozszerzenie ciał skończone, element pierwotny, twierdzenie Kroneckera-Artina, ciało rozkładu wielomianu, ciała skończone, liczby algebraiczne i transcendentne, ciało liczb algebraicznych, domknięcia algebraiczne, ciała algebraicznie domknięte, zasadnicze twierdzenie algebry.

Twierdzenie Lagrange'a (teoria grup)

Twierdzenie Lagrange'a – twierdzenie teorii grup mówiące, że w grupie skończonej rząd dowolnej jej podgrupy jest dzielnikiem rzędu grupy.

Dokładniej, zachodzi równość

$$|G| = |G : H| \cdot |H|,$$

gdzie $|G : H|$ oznacza liczbę warstw grupy G względem jej podgrupy H, zaś $|G|, |H|$ odpowiednio rząd grupy i podgrupy.

Dowód [edytuj kod]

Niech G będzie grupą skończoną. Rozpatrzmy zbiór warstw lewostronnych $\{gH : g \in G\}$ grupy G względem podgrupy H. Zbiór ten stanowi rozbicie zbioru G na $n = |G : H|$ (z definicji indeksu podgrupy) równolicznych ze zbiorem H zbiorów: $g_1H, g_2H, \ldots, g_nH$.

Stąd

$$G = g_1H \cup g_2H \cup \ldots \cup g_nH,$$

ponieważ poszczególne warstwy są rozłączne, to

$$|G| = |g_1H| + |g_2H| + \ldots + |g_nH|,$$

a skoro zaś wszystkie warstwy są równoliczne z H, jest więc

$$|G| = |H| + |H| + \ldots + |H| = n|H|,$$

zatem

$$|G| = |G : H| \cdot |H|.$$

Podgrupę N grupy G nazywa się **podgrupą normalną**, jeśli wszystkie jej warstwy lewostronne równają się odpowiadającym im warstwom prawostronnym, tzn. gdy $gN = Ng$ dla wszystkich $g \in G$. Fakt ten oznacza się symbolem $N \trianglelefteq G$.

Warunki równoważne [edytuj kod]

Niech N będzie podgrupą grupy G. Wówczas następujące warunki są równoważne:

(i) N jest podgrupą normalną,
(ii) zbiory warstw lewo- i prawostronnych N w G są równe, czyli $G/H = G\backslash H$,
(iii) relacja równoważności $\sim$ na zbiorze G określona wzorem

$$a \sim b \overset{\text{def}}{\iff} ab^{-1} \in N$$

jest zgodna z działaniem w grupie G, czyli dla wszystkich $a, b, c, d \in G$

$$(a \sim b) \wedge (c \sim d) \Rightarrow (ac) \sim (bd),$$

(iii') relacja równoważności $\backsim$ na zbiorze G określona wzorem

$$a \backsim b \overset{\text{def}}{\iff} a^{-1}b \in N$$

jest zgodna z działaniem w grupie G, czyli dla wszystkich $a, b, c, d \in G$

$$(a \backsim b) \wedge (c \backsim d) \Rightarrow (ac) \backsim (bd),$$

(iv) dla każdego $g \in G$ zachodzi $gNg^{-1} \subseteq N$,
(iv') dla każdego $g \in G$ zachodzi $g^{-1}Ng \subseteq N$,
(v) dla każdego $g \in G$ zachodzi $gNg^{-1} = N$,
(v') dla każdego $g \in G$ zachodzi $g^{-1}Ng = N$,
(vi-vi') grupa N jest niezmiennicza ze względu na sprzężenia, czyli

$$\varphi(N) = N \text{ dla } \varphi(n) = gng^{-1} \text{ dla dowolnego } g \in G$$

lub

$$\psi(N) = N \text{ dla } \psi(n) = g^{-1}ng \text{ dla dowolnego } g \in G,$$

(vii) N jest sumą klas sprzężoności G,
(viii) istnieje pewien homomorfizm określony na G, którego jądrem jest N.

Każdy z powyższych warunków może być przyjęty za definicję normalności podgrupy.

Niektórzy autorzy używają oznaczenia $\mathrm{NSub}\ G$ dla rodziny wszystkich podgrup normalnych grupy G (od ang. ***N**ormal **Sub**group*).

Twierdzenie Cayleya

Każda grupa G jest izomorficzna z pewną podgrupą grupy permutacji $\mathrm{Sym}(G)$ zbioru G. W szczególności, każda grupa G rzędu n jest izomorficzna z pewną podgrupą grupy S_n.

Dowód [edytuj kod]

Dla dowolnej grupy $(G, \cdot)$ i dowolnego elementu $g \in G$, niech odwzorowanie $\psi_g \colon G \to G$ będzie zadane wzorem $\psi_g(x) = gx$. Funkcja ψ_g jest bijekcją zbioru elementów. Należy udowodnić, że przekształcenie $\psi \colon G \to \mathrm{Sym}(G),\ \psi(g) = \psi_g$ jest zanurzeniem (monomorfizmem):

$$\begin{aligned}\psi(g_1g_2)(x) &= \psi_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = \psi_{g_1}(\psi_{g_2}(x)) \\ &= (\psi_{g_1} \circ \psi_{g_2})(x) = (\psi(g_1) \circ \psi(g_2))(x)\end{aligned},$$

zatem $\psi(g_1g_2) = \psi(g_1) \circ \psi(g_2)$.

Homomorfizm ψ nazywa się niekiedy *reprezentacją regularną* G. Powyższe rozumowanie jest dowodem na to, iż działanie ψ grupy G na sobie przez mnożenie z lewej strony jest wierne.

Działanie grupy – w algebrze i geometrii sposób opisania symetrii obiektów za pomocą pojęcia grupy. Istotne elementy obiektu opisane są za pomocą zbioru, a jego symetrie za pomocą jego grupy symetrii, która składa się z wzajemnie jednoznacznych przekształceń geometrycznych wspomnianego zbioru. Wówczas grupę tę nazywa się także **grupą permutacji** (szczególnie, jeśli zbiór jest skończony lub nie jest przestrzenią liniową) lub **grupą przekształceń** (szczególnie, gdy zbiór jest przestrzenią liniową, a grupa działa jak przekształcenia liniowe zbioru).

Grupa permutacji

Grupa permutacji – grupa wszystkich bijekcji pewnego zbioru w siebie (czyli permutacji) z działaniem składania pełniącego rolę działania grupowego i identycznością jako elementem neutralnym. Elementem odwrotnym do danego jest funkcja (permutacja) odwrotna do danej, która zawsze istnieje z definicji bijekcji.

Niekiedy nazywana jest ona także **grupą symetryczną**, zaś przez niektórych autorów[1] nazwa **grupy permutacji** stosowana jest na określenie jej (właściwej) podgrupy.

Oznaczenia

W literaturze matematycznej istnieje szereg różnych systemów oznaczeń używanych w kontekscie grup permutacji.

Gleichgewicht[2] wprowadza symbol $S(X)$ na oznaczenie grupy wszystkich permutacji zbioru *X*. Gdy $X = \{1, 2, \ldots, n\}$, to zamiast $S(X)$ pisze on S_n. Ten ostatni symbol jest także używany przez Langa[3] oraz Browkina [4] Natomiast Komorowski[5] używa oznaczeń $\mathrm{Bij}(X, X)$, $\Pi(n)$ na $S(X)$, S_n odpowiednio.

Wśród innych oznaczeń spotyka się również $\mathfrak{S}(X)$, Σ_n oraz $\mathrm{Sym}(X)$. Ostatni rodzaj oznaczeń jest używany szczególnie w odniesieniu do zbiorów nieskończonych (i wtedy zwykle używa się nazwy *grupa symetryczna'*).

Przykłady

Gdy $X = \{0, 1\}$, mamy tylko dwie permutacje zbioru X: $0 \mapsto 0, 1 \mapsto 1$ (identycznościowa) oraz $0 \mapsto 1, 1 \mapsto 0$ (transpozycja). Jeśli $X = \{0, 1, 2\}$, to mamy już 6 permutacji.

Zastosowania

- Grupy permutacji okazały się szczególnie pomocne przy badaniu rozwiązywalności równań algebraicznych.
- Dla każdej liczby naturalnej *n*, rząd (liczba elementów) grupy S_n jest równy *n*!.
- Dla $n > 2$ grupa S_n nie jest przemienna, a dla $n > 4$ nie jest rozwiązalna.
- Zachodzi tzw. twierdzenie Cayleya: każdą grupę można utożsamiać z pewną podgrupą permutacji zbioru składającego się z elementów tej grupy.

Twierdzenia o izomorfizmie zostaną najpierw wyrażone dla grup, gdzie przyjmują prostszą postać i wyrażają ważne własności grup ilorazowych. Wszystkie trzy dotyczą „dzielenia" przez podgrupę normalną.

Pierwsze twierdzenie [edytuj kod]

Jeżeli G, H są grupami, a

$$f: G \to H$$

jest homomorfizmem to

- jądro K homomorfizmu f jest podgrupą normalną G,
- obraz f jest podgrupą H, a
- grupa ilorazowa G/K, nazywana czasem **koobrazem**, jest izomorficzna z obrazem f.

Jeżeli ciąg rozszczepia się, to G jest w rzeczywistości iloczynem półprostym. W kategorii abelowej lemat o rozszczepianiu uściśla ten fakt do rozkładu G na sumę prostą.

Drugie twierdzenie (znane też jako trzecie) [edytuj kod]

Niech

H, K będą podgrupami G i
H będzie podgrupą normalną G.

Wówczas

Iloczyn HK grup H oraz K jest podgrupą w G,
$H \cap K$ jest podgrupą normalną w K, a
HK/H jest izomorficzna z $K/(H \cap K)$.

Trzecie twierdzenie (znane też jako drugie) [edytuj kod]

Jeżeli

M, N są podgrupami normalnymi w G,
takimi, że M zawiera się w N,

to

M jest podgrupą normalną w N,
N/M jest podgrupą normalną w G/M, a
$(G/M)/(N/M)$ jest izomorficzna z G/N.

Wynik ten uogólnia się przez lemat dziewiątkowy na kategorie abelowe i bardziej ogólne odwzorowania między obiektami.

Iloczyn kartezjański [edytuj kod]

Osobny artykuł: iloczyn kartezjański.

Niech $\{G_i : i \in I\}$ będzie rodziną grup, gdzie I jest co najwyżej przeliczalnym zbiorem indeksów. Rozważmy zbiór

$$\prod_{i\in I} G_i = G_1 \times G_2 \times \ldots \times G_n \times \ldots = \{(g_1, g_2, \ldots, g_n, \ldots) : g_i \in G_i, i \in I\}$$

z działaniem

$$(g_1, g_2, \ldots, g_n, \ldots)(h_1, h_2, \ldots, h_n, \ldots) \stackrel{\text{def}}{=} (g_1h_1, g_2h_2, \ldots, g_nh_n, \ldots).$$

Powyższe działanie wprowadza w tym zbiorze strukturę grupy, gdyż

- elementem neutralnym jest $e = (e_1, e_2, \ldots, e_n, \ldots)$, gdzie e_i jest elementem neutralnym grupy G_i dla każdego $i \in I$,
- elementem odwrotnym do elementu $g = (g_1, g_2, \ldots, g_n, \ldots)$ jest $g^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}, \ldots)$.

Powyższą konstrukcję nazywa się **iloczynem kartezjańskim** grup i oznacza symbolem $\prod_{i\in I} G_i$.

W definicji zastosowano dla każdej grupy zapis multyplikatywny.

Iloczyn prosty [edytuj kod]

Iloczynem (produktem) prostym (zewnętrznym) grup G_i określonych wyżej nazywa się podgrupę iloczynu kartezjańskiego grup $\prod_{i\in I} G_i$ określonego równością

$$\coprod_{i\in I} G_i \stackrel{\text{def}}{=} \{(g_1, g_2, \ldots, g_n, \ldots) \colon \exists_m \, \forall_{i>m} \; g_i = e_i\}.$$

Iloczyn prosty jest więc zbiorem tych elementów iloczynu kartezjańskiego, których prawie wszystkie współrzędne są jedynkami odpowiednich grup. Grupa, która może być wyrażona jako suma prosta właściwych podgrup jest nazywana **rozkładalną**, w przeciwnym wypadku nosi ona nazwę **nierozkładalnej**.

Uwagi [edytuj kod]

Jeżeli $I = \{1, 2, \ldots, n\}$ jest zbiorem skończonym, to iloczyn prosty pokrywa się z iloczynem kartezjańskim grup, wówczas do jego oznaczenia stosuje się również zapis $G_1 \times G_2 \times \ldots \times G_n$.

Jeżeli jednak $I = \mathbb{N}$ jest zbiorem przeliczalnym, a G_i są nietrywialne dla nieskończenie wielu $i \in I$, to $\coprod G_i < \prod G_i$.

Suma prosta [edytuj kod]

Jeżeli rozważamy grupy A_i z addytywnym sposobem zapisu, to iloczyn prosty nazywa się wówczas **sumą prostą** i pisze

$$\bigoplus_{i\in I} A_i.$$

W algebrze abstrakcyjnej sumy proste grup uogólnia się na sumy proste przestrzeni liniowych, modułów i innych struktur, więcej w artykule o sumach prostych modułów.

Sam zapis jest przemienny, tzn. dla sumy prostej dwóch grup przemiennych $G = H \oplus K = K \oplus H$. Jest również łączny w sensie, że jeżeli $G = H \oplus K$ oraz $K = L \oplus M$, to $G = H \oplus (L \oplus M) = H \oplus L \oplus M$.

Jeżeli $G = H \oplus K$, to można udowodnić, że:

- dla dowolnych $h \in H,\ k \in K$ zachodzi $h + k = k + h$,
- dla dowolnych $g \in G$ istnieją jednoznacznie wyznaczone $h \in H,\ k \in K$ takie, że $g = h + k$,
- zachodzi skracanie sumy w ilorazie, tzn. $(H \oplus K)/K$ jest izomorficzna z H.

Fakty te uogólnia się łatwo na sumę prostą skończenie wielu grup.

Przykłady [edytuj kod]

- grupa wektorów na płaszczyźnie euklidesowej o współrzędnych rzeczywistych z dodawaniem jest iloczynem prostym grupy liczb rzeczywistych z dodawaniem przez samą siebie.

Iloczyn półprosty [edytuj kod]

Niech będą dane grupy N i D oraz homomorfizm $\varphi\colon D \to \mathrm{Aut}\ N$ grupy D w grupę automorfizmów grupy N.

Iloczynem półprostym (zewnętrznym) grup N i D za pośrednictwem φ, oznaczanym $N \rtimes_\varphi D$, nazywa się grupę składająca się z elementów $(n, d),\ n \in N, d \in D$ wraz z działaniem określonym wzorem

$$(n_1, d_1)(n_2, d_2) = (n_1\varphi_{d_1}(n_2), d_1 d_2)$$

oraz odwrotnością daną przez

$$(n, d)^{-1} = \left(\varphi_{d^{-1}}(n^{-1}), d^{-1}\right),$$

i elementem neutralnym

$$(e, 1)$$

gdzie $e \in N$ oraz $1 \in D$ są elementami neutralnymi.

Iloczyn półprosty wewnętrzny [edytuj kod]

Niech N będzie podgrupą normalną w G. **Dopełnieniem normalnym** D podgrupy N w G nazywamy zbiór spełniający warunki $N \cap D = \{e\}$ oraz $ND = G$ (równoważnie $DN = G$).

Grupę G nazywa się **iloczynem półprostym wewnętrznym** podgrup N i D, co oznacza $N \rtimes D$ wtedy i tylko wtedy, gdy D jest dopełnieniem normalnym N.

Jeżeli grupa G jest iloczynem półprostym wewnętrznym swoich podgrup N i D, to jest ona izomorficzna z iloczynem półprostym zewnętrznym $N \rtimes_\varphi D$ za pośrednictwem homomorfizmu $\varphi : D \to \mathrm{Aut}\, N$ określonego jako $\varphi_d(n) = dnd^{-1}$, czyli sprzężenie n przez d. Odwrotnie, iloczyn półprosty zewnętrzny $N \rtimes_\varphi D$ jest wewnętrznym iloczynem półprostym swoich podgrup $N \times \{1\}$ oraz $\{e\} \times D$, przy czym pierwsza z nich jest podgrupą normalną.

Uwagi [edytuj kod]

- $N \rtimes_\varphi D \equiv N \times D$ wtedy i tylko wtedy, gdy homomorfizm $\varphi\colon D \to \mathrm{Aut}\ N$ jest trywialny.
- $N \rtimes_\varphi D$ jest przemienna wtedy i tylko wtedy, gdy N, D są przemienne oraz $\varphi\colon D \to \mathrm{Aut}\ N$ jest trywialny.

Przykłady [edytuj kod]

- Grupa diedralna rzędu $2n$ jest iloczynem półprostym wewnętrznym $D_{2n} = \mathbb{Z}_n \ltimes \mathbb{Z}_2$.
- Grupa izometrii przestrzeni $\mathbb{R}^n$ jest iloczynem półprostym grupy obrotów oraz symetrii z grupą translacji.

Niech G będzie grupą, a X oznacza pewien zbiór, którego elementy nazywane *punktami* będą oznaczane pismem prostym. Wówczas (lewostronnym) **działaniem grupy** G *na zbiorze* X nazywa się funkcję dwuargumentową

$$G \times X \to X;\ (g,x) \mapsto g \cdot x$$

spełniającą następujące dwa aksjomaty:

- $(gh) \cdot x = g \cdot (h \cdot x),$
- $e \cdot x = x,$

gdzie g, h są dowolnymi elementami grupy G, element x należy do zbioru X, zaś e oznacza element neutralny w G. Zbiór X nazywa się wtedy (lewostronnym) G**-zbiorem**, co formalnie można oznaczać parą uporządkowaną (X, G); o grupie G mówi się zaś, że *działa* na X (z lewej strony).

Homomorfizm w grupę symetryczną [edytuj kod]

Powyższe dwa aksjomaty gwarantują, że dla każdego $g \in G$ funkcja przekształcająca $x \in X$ w $g \cdot x$ jest bijekcją φ_g zbioru X. Jeżeli nie prowadzi to do nieporozumień, wyznaczaną jednoznacznie przez element $g \in G$ bijekcję $\varphi_g(x)$ oznacza się niekiedy symbolem $g(x)$ lub nawet gx. Dlatego też działanie grupy może być zdefiniowane jako homomorfizm grupowy φ z G w grupę symetryczną $\mathrm{Sym}(X)$ wszystkich bijekcji X dany wzorem $\varphi(g) = \varphi_g$. Z tego też powodu dowolny homomorfizm $G \to \mathrm{Sym}(X)$ można nazywać działaniem grupy na zbiorze.

Działanie to przypisuje każdemu elementowi grupy permutację X w taki sposób, że

- permutacją X odpowiadającą elementowi neutralnemu G jest odwzorowanie tożsamościowe X;
- permutacją X odpowiadającą iloczynowi gh dwóch elementów tej grupy jest złożenie permutacji przypisanych do g oraz h.

Ponieważ każdy element w G reprezentowany jest jako permutacja, działanie grupy nazywa się także **reprezentacją permutacyjną**.

Stabilizator, orbita, punkt stały [edytuj kod]

Nazwy te nawiązują do intuicji astronomicznych/geometrycznych dotyczących badania ruchów. *Stabilizator elementu* należącego do zbioru to zbiór elementów grupy, które nie „poruszają" elementu, stąd *stabilizator* całego zbioru to te elementy, które „nie poruszają" elementów zbioru (*stabilizują* je). Inną nazwą stabilizatora jest *grupa izotropii* (*isos* – równy, jednakowy, *trópos* – zwrot, obrót, zob. izotropia). *Punkty stałe* to punkty, które nie są „poruszane" przez żaden element grupy, czyli stabilizowane przez całą grupę.

Orbita to zbiór punktów, do których można przejść z danego punktu przy działaniu grupy. Same orbity są rozłączne, a punkty mogą przechodzić wyłącznie na punkty należące do tej samej orbity (każdy punkt należy do pewnej orbity). Jeżeli działanie wyróżnia na zbiorze tylko jedną orbitę (dowolny punkt może przejść na każdy inny), to działanie nazywa się *wiernym* lub *efektywnym*; jest to równoważne temu, że wyłącznie element neutralny grupy stabilizuje zbiór. Ta dwoista charakteryzacja nie jest przypadkiem: stabilizator i orbity są ze sobą ściśle powiązane.

Definicje [edytuj kod]

Niech grupa G działa na zbiorze X oraz $x \in X$. Zapis działania $g \cdot x$ zostanie zarzucony na rzecz $g(x)$, co uwydatni sens oznaczeń poszczególnych obiektów.

Zbiór

$$G(x) = \{g(x)\colon g \in G\}$$

nazywa się **orbitą** elementu (wyznaczaną przez element) x; czasami oznacza się go również po prostu Gx (w nawiązaniu do oznaczenia działania jako gx).

Zbiór wszystkich orbit w X ze względu na działanie grupy G zapisuje się symbolem X/G i nazywa **ilorazem** działania; w kontekście geometrycznym obiekt ten może być nazywany **przestrzenią orbit**.

Zbiór

$$G_x = \{g \in G\colon g(x) = x\}$$

nazywa się **stabilizatorem** bądź **grupą izotropii** elementu x, który oznacza się również symbolem $\mathrm{Stab}(x)$. Zbiór wszystkich stabilizatorów elementów zbioru X nazywa się **stabilizatorem (zbioru)** bądź **grupą izotropii (zbioru)** i oznacza G_X lub $\mathrm{Stab}(X)$.

Punkt x nazywa się **punktem stałym**, jeżeli spełnia on warunek

$$G(x) = \{x\}, \text{ czyli } g(x) = x \text{ dla każdego } g \in G,$$

co jest równoważne

$$G_x = G.$$

Zbiór punktów stałych wyznaczanych przez element g oznacza się X^g, a zbiór wszystkich punktów stałych jest zapisywany jako X^G.

Własności [edytuj kod]

Orbity

Własności grupy gwarantują, że zbiór orbit w X tworzy podział tego zbioru ze względu na działanie grupy G. Relacja równoważności wyznaczająca ten podział dana jest wzorem

$$x \sim y \iff \exists_{g \in G}\ g(x) = y,$$

a orbity są klasami abstrakcji tej relacji, a więc dwa elementy są uważane za równoważne wtedy i tylko wtedy, gdy oba wyznaczają tę samą orbitę (leżą w jednej orbicie), tzn. $G(x) = G(y)$.

Stabilizatory

Stabilizator G_x punktu x jest podgrupą w G. Wynika to z faktu, iż wraz ze stałą na pewnym punkcie bijekcją wyznaczaną przez dany element do stabilizatora należy bijekcja do niej odwrotna, która również jest stała na pewnym punkcie oraz tego, iż złożenie dwóch bijekcji stałych na danym punkcie również jest stałe na tym punkcie. Zwykle nie jest to jednak podgrupa normalna. Grupa G działa na X w sposób wolny wtedy i tylko wtedy, gdy wszystkie stabilizatory są trywialne.

Stabilizator $\mathrm{Stab}(X)$ całego zbioru to przecięcie wszystkich stabilizatorów elementów tego zbioru, gdyż przecięcie podgrup danej grupy również jest jej podgrupą. Tłumaczy to nazwę „grupa izotropii".

Stabilizator zbioru X można zdefiniować jako zbiór $\{g \in G\colon \forall_{x \in X}\ g(x) = x\}$. Innymi słowy są to te elementy grupy g, które wyznaczają przekształcenia tożsamościowe na zbiorze X, czyli $\varphi_g = \mathrm{id}$. Wynika stąd, że $\mathrm{Stab}(X)$ jest podgrupą normalną w G jako jądro homomorfizmu $\varphi\colon G \to \mathrm{Sym}(X)$.

Twierdzenie [edytuj kod]

Niech będzie dane dla ustalonego $x \in X$ przekształcenie $G \to X$ dane wzorem $g \mapsto g(x)$. Obrazem tego odwzorowania jest orbita wyznaczana przez punkt x, a koobraz jest zbiorem wszystkich warstw lewostronnych stabilizatora G_x. Zwykłe twierdzenie o ilorazie teorii grup daje naturalną bijekcję między grupą ilorazową G/G_x a $G(x)$. Bijekcja ta dana jest wzorem $hG_x \mapsto h(x)$. Wynik ten znany jest w literaturze angielskiej jako „twierdzenie o orbitach i stabilizatorach" (ang. *orbit-stabilizer theorem*) lub „twierdzenie o klasyfikacji G-orbit" (ang. *classification of G-orbits*).

Zliczanie elementów

Powyższe twierdzenie wraz z twierdzeniem Lagrange'a daje

$$|G(x)| = [G\colon G_x] = |G|/|G_x|.$$

Dla G i X są skończonych dodatkowo zachodzi

$$|G(x)| = [G\colon G_x].$$

Wynik ten stosuje się szczególnie często podczas zliczania elementów zbioru.

Sprzężenie stabilizatorów

Należy zauważyć, że jeżeli dwa elementy x, y należą do tej samej orbity, to ich podgrupy stabilizujące G_x, G_y są izomorficzne (lub sprzężone). Dokładniej: jeśli $y = g(x)$, to $G_y = gG_xg^{-1}$. O punktach mających sprzężone podgrupy stabilizujące mówi się, że mają ten sam *typ orbity*.

Lemat Burnside'a

Wynikiem blisko związanym z powyższym twierdzeniem jest lemat Burnside'a:

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|\,,$$

gdzie X^g to zbiór punktów stałych wyznaczanych przez element g. Z wyniku tego korzysta się głównie, gdy tak G jak i X są skończone, można go wówczas interpretować następująco: liczba orbit jest równa średniej liczbie punktów stałych przypadających na jeden element grupy.

Zbiór różnic formalnych skończonych G-zbiorów tworzy pierścień nazywany pierścieniem Burnside'a, gdzie dodawanie odpowiada sumie rozłącznej, a mnożenie iloczynowi kartezjańskiemu.

Reprezentacja grupy [edytuj kod]

Osobny artykuł: reprezentacja grupy.

Macierz A kwadratowa stopnia $n \in \mathbb{N}$ nad ciałem K wyznacza przekształcenie liniowe przestrzeni liniowej K^n w siebie. Pełną grupę liniową $\mathrm{GL}(n, K)$ można traktować zatem jako grupę przekształceń zbioru K. Każdy homomorfizm $\varphi\colon G \to \mathrm{GL}(n, K)$ wyznacza działanie grupy G na przestrzeni K^n. Działania te nazywa się **reprezentacjami** grupy G w przestrzeni K^n. Jeśli φ jest różnowartościowy, to reprezentację nazywa się **wierną**.

Działania grupy na sobie [edytuj kod]

Osobne artykuły: klasa sprzężoności i centralizator oraz normalizator.

Działanie dowolnej grupy G na sobie przez mnożenie z lewej strony jest regularne, a więc i wierne. Każda grupa może być więc zanurzona w grupie symetrycznej własnych elementów $\mathrm{Sym}(G)$. Jest to wynik znany jako twierdzenie Cayleya.

Innym ważnym działaniem grupy na sobie, bardzo pomocnym podczas badania jej struktury, jest działanie poprzez tzw. automorfizmy wewnętrzne (sprzężenia), określone wzorem

$$g \cdot x = gxg^{-1}.$$

Automorfizm $a_x(g) = gxg^{-1}$ zapisywany jest też często jako x^g, gdyż zachowuje się on, zgodnie ze swoim oznaczeniem, tak jak potęga.

Orbitami tego działania są zbiory $x^G = \{x^g\colon g \in G\}$ nazywane **klasami sprzężoności (klasami elementów sprzężonych)**, natomiast stabilizator $G_x = \{g \in G\colon gxg^{-1} = x\}$ nazywa się **centralizatorem** elementu x i oznacza $\mathrm{C}_G(x)$ lub krótko: $\mathrm{Z}(x)$; są to wszystkie elementy grupy G przemienne z elementem x. Stabilizator $\mathrm{C}_G(G)$ całego zbioru nazywa się **centrum** grupy i oznacza się symbolem $\mathrm{Z}(G)$; są to te elementy, które są przemienne z dowolnym elementem grupy.

Równanie klas [edytuj kod]

Niech G będzie grupą skończoną działającą na zbiorze skończonym X, a $x_1, \ldots, x_n$ będą reprezentantami wszystkich orbit w zbiorze X. Ponieważ zbiór X rozpada się na rozłączne orbity:

$$X = \bigcup_{i=1}^{n} G_{x_i},$$

to prawdą jest, iż moc zbioru X jest równa sumie mocy poszczególnych orbit, czyli sumie indeksów stabilizatorów w grupie (zob. wniosek):

$$|X| = \sum_{i=1}^{n} [G\colon G_{x_i}].$$

Równanie to nazywa się często **równaniem klas**, można je wyprowadzić wprost z twierdzenia o stabilizatorach i orbitach. Równanie klas jest narzędziem dowodzenia wielu twierdzeń w teorii grup skończonych. Można je wykorzystać także w dowodzie twierdzenia Cauchy'ego i twierdzenia Sylowa (zob. zastosowania równania dla klas sprzężoności).

Reprezentacja grupy [edytuj kod]

Osobny artykuł: reprezentacja grupy.

Macierz A kwadratowa stopnia $n \in \mathbb{N}$ nad ciałem K wyznacza przekształcenie liniowe przestrzeni liniowej K^n w siebie. Pełną grupę liniową $\mathrm{GL}(n, K)$ można traktować zatem jako grupę przekształceń zbioru K. Każdy homomorfizm $\varphi\colon G \to \mathrm{GL}(n, K)$ wyznacza działanie grupy G na przestrzeni K^n. Działania te nazywa się **reprezentacjami** grupy G w przestrzeni K^n. Jeśli φ jest różnowartościowy, to reprezentację nazywa się **wierną**.

Działania grupy na sobie [edytuj kod]

Osobne artykuły: klasa sprzężoności i centralizator oraz normalizator.

Działanie dowolnej grupy G na sobie przez mnożenie z lewej strony jest regularne, a więc i wierne. Każda grupa może być więc zanurzona w grupie symetrycznej własnych elementów $\mathrm{Sym}(G)$. Jest to wynik znany jako twierdzenie Cayleya.

Innym ważnym działaniem grupy na sobie, bardzo pomocnym podczas badania jej struktury, jest działanie poprzez tzw. automorfizmy wewnętrzne (sprzężenia), określone wzorem

$$g \cdot x = gxg^{-1}.$$

Automorfizm $a_x(g) = gxg^{-1}$ zapisywany jest też często jako x^g, gdyż zachowuje się on, zgodnie ze swoim oznaczeniem, tak jak potęga.

Orbitami tego działania są zbiory $x^G = \{x^g\colon g \in G\}$ nazywane **klasami sprzężoności (klasami elementów sprzężonych)**, natomiast stabilizator $G_x = \{g \in G\colon gxg^{-1} = x\}$ nazywa się **centralizatorem** elementu x i oznacza $\mathrm{C}_G(x)$ lub krótko: $\mathrm{Z}(x)$; są to wszystkie elementy grupy G przemienne z elementem x. Stabilizator $\mathrm{C}_G(G)$ całego zbioru nazywa się **centrum** grupy i oznacza się symbolem $\mathrm{Z}(G)$; są to te elementy, które są przemienne z dowolnym elementem grupy.

Równanie klas [edytuj kod]

Niech G będzie grupą skończoną działającą na zbiorze skończonym X, a $x_1, \ldots, x_n$ będą reprezentantami wszystkich orbit w zbiorze X. Ponieważ zbiór X rozpada się na rozłączne orbity:

$$X = \bigcup_{i=1}^{n} G_{x_i},$$

to prawdą jest, iż moc zbioru X jest równa sumie mocy poszczególnych orbit, czyli sumie indeksów stabilizatorów w grupie (zob. wniosek):

$$|X| = \sum_{i=1}^{n} [G\colon G_{x_i}].$$

Równanie to nazywa się często **równaniem klas**, można je wyprowadzić wprost z twierdzenia o stabilizatorach i orbitach. Równanie klas jest narzędziem dowodzenia wielu twierdzeń w teorii grup skończonych. Można je wykorzystać także w dowodzie twierdzenia Cauchy'ego i twierdzenia Sylowa (zob. zastosowania równania dla klas sprzężoności).

Twierdzenie Sylowa

Twierdzenia Sylowa – twierdzenia teorii grup autorstwa Petera Sylowa[1], czasem formułowane jako jedno *twierdzenie Sylowa*. Wynik ten jest częściowym odwróceniem twierdzenia Lagrange'a (rząd podgrupy jest dzielnikiem rzędu danej grupy), a zarazem uogólnieniem twierdzenia Cauchy'ego (o istnieniu podgrupy rzędu będącego liczbą pierwszą dzielącym rząd danej grupy).

Twierdzenia [edytuj kod]

Zobacz też: p-grupa.

Niech p będzie liczbą pierwszą, która ponadto jest względnie pierwsza z liczbą naturalną r (tzn. największy wspólny dzielnik $\mathrm{nwd}(p,r)=1$). Niech G będzie grupą rzędu $|G|=p^k r$, gdzie k jest pewną nieujemną liczbą całkowitą; dowolną jej podgrupę rzędu p^i, gdzie $i=1,\ldots,k$ nazywa się *p-podgrupą* tej grupy, przy czym podgrupy rzędu p^k nazywane są *p-podgrupami Sylowa*.

Pierwsze twierdzenie Sylowa

W grupie G istnieje (co najmniej jedna) p-podgrupa Sylowa.

Drugie twierdzenie Sylowa

Wszystkie p-podgrupy Sylowa grupy G są sprzężone, tzn. dla dowolnych p-podgrup Sylowa H,K grupy G istnieje taki automorfizm wewnętrzny φ_g tej grupy ($\varphi_g(a)=gag^{-1}$), że $\varphi[H]=K$.

Trzecie twierdzenie Sylowa

Liczba s_p wszystkich p-podgrup Sylowa grupy G przystaje do jedynki modulo p, tzn. $s_p \equiv 1 \bmod p$ (czyli p jest dzielnikiem s_p-1, tj. $p|s_p-1$).

Wnioski [edytuj kod]

Z twierdzenia Lagrange'a wynika, że p-podgrupa Sylowa jest jej maksymalną (w sensie zawierania) p-podgrupą, a jej indeks równy r nie jest podzielny przez p, innymi słowy $s_p|r$. Z drugiego twierdzenia wynika, że warunek $s_p=1$ jest równoważny normalności (a nawet charakterystyczności) p-podgrupy Sylowa[2]. Z pierwszego i drugiego twierdzenia Sylowa wynika, że jeżeli H jest p-podgrupą Sylowa w G, zaś K jest p-podgrupą normalną w G, to istnieje taki element $g \in G$, dla którego K jest podgrupą normalną w gHg^{-1}.

Jeżeli p jest dzielnikiem rzędu $|G|$ grupy G, to w grupie tej istnieje element rzędu p (tzw. twierdzenie Cauchy'ego); ponadto s_p dzieli wtedy $|G|$. Jeżeli każdy element $g \in G$ ma rząd postaci p^k, to G jest p-grupą. Jeśli $p>q$ oraz $|G|=pq$, gdzie p,q są pewnymi liczbami pierwszymi, to w G istnieje podgrupa normalna rzędu p; jeżeli q nie dzieli ponadto $p-1$, to grupa G jest cykliczna. W szczególności jeśli q nie dzieli $p-1$ oraz p nie dzieli $q-1$, to jedyną grupą rzędu pq jest suma prosta grup cyklicznych o rzędach p i q.

Grupa prosta [edytuj]

Grupa prosta – nietrywialna grupa nie mająca właściwych podgrup normalnych, czyli jedynymi grupami normalnymi są w niej grupa trywialna i ona sama.

Przykład [edytuj kod]

- Grupa cykliczna $\mathbf{Z}_3$ jest prosta. Jeśli H jest podgrupą tej grupy, to jej rząd (liczba elementów) musi być dzielnikiem 3 (rzędu G). Ponieważ 3 jest liczbą pierwszą, jej jedynymi dzielnikami są 1 i 3, więc H jest albo trywialna albo równa G. Przykładem grupy która nie jest prosta jest $\mathbf{Z}_{12}$. Podgrupa składająca się z elementów 0, 4 i 8 jest podgrupą rzędu 3 i jest dzielnikiem normalnym $\mathbf{Z}_{12}$, ponieważ jest przemienna.
- Podobnie grupa addytywna $\mathbf{Z}$ (wszystkich liczb całkowitych) nie jest prosta – zbiór liczb parzystych jest jej nietrywialną podgrupą normalną.
- Analogiczne rozumowanie można zastosować do wszystkich grup przemiennych, i pokazać że jedynymi grupami przemiennymi, które są proste, są grupy cykliczne o liczbie elementów będącej liczbą pierwszą.
- Grupy Mathieu.

Klasyfikacja [edytuj kod]

Klasyfikacja nieprzemiennych grup prostych jest znacznie bardziej skomplikowana. Najmniejszą z takich grup jest grupa alternująca $\mathbf{A}_5$ i można pokazać że każda grupa prosta rzędu 60 jest z nią izomorficzna.

Grupy proste stanowią "klocki" z których zbudowane są wszystkie grupy skończone, w podobnym znaczeniu jak liczby pierwsze stanowią klocki z których zbudowane są wszystkie liczby naturalne. Klasyfikacja skończonych grup prostych, zakończona w 1982 roku, jest jednym z największych dotychczas zrealizowanych projektów w matematyce.

Twierdzenie Feita–Thompsona mówi, że każda grupa nieparzystego rzędu jest rozwiązalna. Wynika z tego że każda skończona grupa prosta jest grupą cykliczną o rzędzie pierwszym albo ma rząd parzysty.

Istnieją różne nieskończone grupy proste: przykładami takich grup są proste grupy Liego i grupy Thompsona T i V.

Grupa rozwiązalna

Grupa rozwiązalna – w matematyce, jest to grupa, dla której istnieje ciąg subnormalny o abelowych faktorach (przemiennych ilorazach).

Nazwa pojęcia ma swoje źródło w teorii Galois, skąd pochodzi – pierwiastki wielomianu o współczynnikach z pewnego ciała można wyrazić za pomocą *pierwiastników* (elementów ciała połączonych działaniami dodawania, odejmowania, mnożenia, dzielenia i pierwiastkowania dowolnego stopnia naturalnego), gdy tzw. *grupa Galois* ciała rozkładu danego wielomianu jest rozwiązalna. Twierdzenie Abela-Ruffiniego mówi, że grupy Galois ciała rozkładu wielomianów stopnia większego od 4 nie muszą być rozwiązalne, tzn. wśród wielomianów rzeczywistych dowolnego stopnia większego niż 4 istnieją wielomiany, których pierwiastki nie dają się przedstawić za pomocą pierwiastników. Przykładem może być następujący wielomian piątego stopnia: $x^5 - x - 1$.

Definicja

Grupa G jest **rozwiązalna**, gdy istnieje ciąg podgrup

$$\{1\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_{k-1} \subseteq H_k = G,$$

takich, że dla każdego $1 \leqslant i \leqslant k$ są spełnione warunki:

- H_{i-1} jest podgrupą normalną H_i
- grupa ilorazowa H_i/H_{i-1} jest abelowa.

Warunki równoważne [edytuj kod]

Czasami jako definicję podaje się również następujący, równoważny warunek:

Grupa G jest rozwiązalna wtedy i tylko wtedy, gdy $G^{(n)} = \{1\}$ dla pewnej liczby n,

gdzie $G^{(n)}$ oznacza n-tą pochodną grupy G. Najmniejszą taką liczbę n nazywa się **stopniem rozwiązalności** grupy G.

Jeżeli grupa G jest skończona, to jest ona rozwiązalna wtedy i tylko wtedy, gdy faktory ciągu kompozycyjnego grupy G są grupami cyklicznymi rzędu, będącego liczbą pierwszą. Równoważność ta wynika z twierdzenia Jordana-Höldera.

Własności

- Podgrupa grupy rozwiązalnej jest rozwiązalna.
- Jeśli $H \lhd G$ i grupa G jest rozwiązalna, to iloraz G/H również jest grupą rozwiązalną.
- Jeżeli $H \lhd G$ oraz grupy H i G/H są rozwiązalne, to G również jest grupą rozwiązalną.
- Obraz homomorficzny grupy rozwiązalnej jest grupą rozwiązalną.
- Iloczyn prosty grup rozwiązalnych jest grupą rozwiązalną.

Grupa nilpotentna [edytuj]

Grupa nilpotentna – w teorii grup, intuicyjnie grupa „prawie" abelowa. Grupy nilpotentne pojawiają się w teorii Galois, a także w zagadnieniach związanych z klasyfikacją grup, również grup Liego.

Definicja [edytuj kod]

Grupę G nazywamy **nilpotentną**, jeżeli istnieje ciąg podgrup normalnych $\{e\} = G_0 \leqslant G_1 \leqslant G_2 \ldots \leqslant G_n = G$, że:

1. $G_i \triangleleft G,\ i = 0, \ldots, n$
2. grupy ilorazowe G_{i+1}/G_i są podgrupami centrum $Z(G/G_i)$ dla $i = 0, 1, 2, \ldots, n-1$.

Jeśli istnieje ciąg o tej własności to nazywamy go **ciągiem centralnym grupy** G. Najmniejsze n dla którego grupa G jest nilpotentna, nazywamy **stopniem nilpotentności** i oznacza $\operatorname{nil}\ G$.

Uwaga [edytuj kod]

Następujące warunki są równoważne:

1. Ciąg $\{e\} = G_0 \leqslant G_1 \leqslant G_2 \ldots \leqslant G_n = G$ jest centralny.
2. Ciąg $\{e\} = G_0 \leqslant G_1 \leqslant G_2 \ldots \leqslant G_n = G$ jest normalny oraz $[G_{i+1}, G] \leqslant G_i,\ i = 0, 1, \ldots, n-1$.
3. $[G_{i+1}, G] \leqslant G_i,\ i = 0, 1, \ldots, n-1$.

Przykłady [edytuj kod]

Grupą nilpotentną jest na przykład:

- dowolna grupa przemienna,
- grupa multiplikatywna macierzy postaci $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, gdzie a, b, c są elementami pewnego ciała,
- grupa kwaternionów Q_8, ma centrum rzędu 2 ($Z(Q_8) = \{1, -1\}$); ciąg centralny tej grupy to $\{1\},\ \{1, -1\}, Q_8$, zatem jest to grupa nilpotentna drugiego stopnia nilpotentności,
- każdy produkt prosty skończonej liczby p-grup,
- dyskretna grupa Heisenberga.
- każda grupa G rzędu p^k, gdzie p jest liczbą pierwszą jest nilpotentna oraz $\operatorname{nil} G \leqslant k$.

Własności [edytuj kod]

- Każda grupa nilpotentna jest rozwiązalna.
- Jeżeli komutant grupy G jest zawarty w jej centrum, to grupa jest nilpotentna.
- grupy permutacji S_n nie są nilpotentne dla $n > 2$.
- Każda podgrupa grupy nilpotentnej klasy n jest grupą nilpotentną klasy co najwyżej n, co więcej to samo dotyczy obrazu homomorficznego grupy nilpotentnej.
- Następujące zdania są równoważne dla grup skończonych:
  - G jest nilpotentna.
  - Jeżeli H jest właściwą podgrupą G, to H jest właściwą podgrupą normalną normalizatora $N(H)$.
  - Każda maksymalna podgrupa właściwa G jest normalna.
  - G jest sumą prostą swoich podgrup Sylowa.
- Ostatnie stwierdzenie może być uogólnione na grupy nieskończone: jeżeli G jest nilpotentna, to każda podgrupa Sylowa G_p grupy G jest normalna, a suma prosta tych podgrup Sylowa jest podgrupą wszystkich elementów skończonego rzędu w G (zob. podgrupa torsyjna).
- Jeśli grupa $G/Z(G)$ jest nilpotentna stopnia n, to G jest nilpotentna stopnia $n+1$.

Skończone grupy przemienne [edytuj kod]

Twierdzenie o klasyfikacji skończonych grup przemiennych mówi, że każda skończona grupa przemienna może być wyrażona jako suma prosta podgrup cyklicznych rzędu będącego potęgą liczby pierwszej. Jest to przypadek szczególny twierdzenia o klasyfikacji skończenie generowanych grup przemiennych w przypadku, gdy rozważana grupa ma beztorsyjną rangę równą zeru.

Grupa $\mathbb{Z}_{mn}$ jest izomorficzna z iloczynem prostym $\mathbb{Z}_m$ przez $\mathbb{Z}_n$ wtedy i tylko wtedy, gdy m i n są względnie pierwsze.

Dlatego można zapisać dowolną skończoną grupę abelową G jako iloczyn prosty postaci

$$\mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_u}$$

na dwa różne sposoby:

- gdzie liczby $k_1, \cdots, k_u$ są potęgami liczb pierwszych
- gdzie k_1 dzieli k_2, które dzieli k_3 i tak dalej, aż do k_u.

Na przykład $\mathbb{Z}_{15}$ może być wyrażona jako suma prosta dwóch podgrup cyklicznych rzędów odpowiednio 3 i 5: $\mathbb{Z}_{15} \simeq \{0, 5, 10\} \oplus \{0, 3, 6, 9, 12\}$. To samo można powiedzieć o dowolnej grupie przemiennej rzędu 15, co prowadzi do ciekawego wniosku, iż wszystkie grupy przemienne rzędu 15 są izomorficzne.

Innym przykładem jest fakt, że każda grupa abelowa rzędu 8 jest izomorficzna z $\mathbb{Z}_8$ (liczby całkowite od 0 do 7 z dodawaniem modulo 8), $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ (nieparzyste liczby całkowite od 1 do 15 z mnożeniem modulo 16) bądź $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Zobacz też listę małych grup zawierającą skończone grupy przemienne rzędu 16 lub mniejszego.

Teoria pierścieni [edytuj kod]

W teorii pierścieni elementy odwrotne względem dodawania nazywane są *elementami przeciwnymi*. Ponieważ elementy pierścienia z działaniem dodawania tworzą grupę, to dla każdego elementu pierścienia istnieje element do niego przeciwny, zatem każdy z nich jest odwracalny względem tego dodawania. Zwyczajowo nazwę *element odwrotny* rezerwuje się dla elementu odwrotnego względem mnożenia. Ponieważ nie każdy element ma element do niego odwrotny względem mnożenia, to uzasadnione jest wyróżnianie tych elementów, które mają swoje odwrotności – właśnie one nazywane są *elementami odwracalnymi* lub dla odróżnienia od ogólnie pojętych elementów odwracalnych *jednościami* (nie należy mylić z jedynką, która w danym pierścieniu z jedynką jest jedna).

Dla danego pierścienia z jedynką $(R, +, \cdot, 0, 1)$ element $a \in R$ nazywa się **odwracalnym** lub **jednością**, jeśli jest dzielnikiem jedynki:

$$\exists_{b \in R}\ a \cdot b = b \cdot a = 1.$$

Grupa elementów odwracalnych [edytuj kod]

Zbiór elementów odwracalnych danego pierścienia oznacza się symbolem R^* lub $U(R)$. Ponieważ zbiór ten zawiera jedynkę (elementem do niej odwrotnym jest ona sama) oraz dla $a, b \in R^*$ jest $ab^{-1} \in R^*$, to $(R^*, \cdot, 1)$ jest grupą.

Pierścień (z jedynką) R jest pierścieniem z dzieleniem wtedy i tylko wtedy, gdy $R^* = R \setminus \{0\}$.

Element nilpotentny [edytuj]

Element nilpotentny lub **nilpotent** pierścienia R - element x pierścienia R o tej własności, że

$$x^n = 0$$

dla pewnej liczby naturalnej n. W każdym pierścieniu 0 (element neutralny dodawania) jest elementem nilpotentnym.

Własności [edytuj kod]

Twierdzenie. Niezerowy element nilpotentny jest dzielnikiem zera.

Dowód. Niech $x \in P$ będzie niezerowym elementem nilpotentnym pierścienia P. Oznacza to, że dla pewnego $n \in \mathbb{N}$ zachodzi $x^n = 0$. Ponieważ, z założenia, element x jest niezerowy, to $n > 1$. Oznacza to, że

$$x^n = xx^{n-1} = 0$$

co dowodzi tezy.

Twierdzenie. Suma dwóch elementów nilpotentnych, które są ze sobą przemienne, jest także elementem nilpotentnym.

Dowód. Niech P będzie pierścieniem przemiennym, a $x, y \in P$ dwoma elementami nilpotentnymi. Oznaczmy przez $m, n \in \mathbb{N}$ liczby takie, że $x^m = 0$ i $y^n = 0$. Ponieważ, z założenia, elementy x i y są ze sobą przemienne, to możemy zastosować wzór Newtona dla wyrażenia $(x+y)^{m+n}$, otrzymując

$$(x+y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k}$$

Dla $0 \leqslant k < m$ zachodzi $m+n-k > n$, czyli $y^{m+n-k} = 0$ i składniki odpowiadające tym indeksom k są zerami. Pozostałe składniki odpowiadają $k \geqslant m$, czyli w tym przypadku $x^k = 0$. Oznacza to, że wszystkie składniki w powyższej sumie są zerami, a więc i cała suma jest zerem. Element $x+y$ jest więc elementem nilpotentnym.

Wniosek. W pierścieniu przemiennym suma dowolnych dwóch elementów nilpotentnych jest elementem nilpotentnym.

Twierdzenie. W pierścieniu przemiennym z jedynką suma elementu nilpotentnego i elementu odwracalnego jest elementem odwracalnym.

Pierścienie i moduły [edytuj kod]

Twierdzenia o izomorfizmie zachodzą również dla modułów nad ustalonym pierścieniem R (a więc również i dla przestrzenie liniowe nad ustalonym ciałem). Należy jedynie zamienić pojęcia „grupa" na „R-moduł", „podgrupa" i „podgrupa normalna" na „podmoduł", a „grupa ilorazowa" na „moduł ilorazowy".

W przypadku przestrzeni liniowych pierwsze twierdzenie o izomorfizmie nosi nazwę twierdzenia o rzędzie.

Twierdzenia o izomorfizmie zachodzą także dla pierścieni, homomorfizmów pierścieni i ideałów. W tym przypadku należy zamienić pojęcia „grupa" na „pierścień", „podgrupa" na „podpierścień" i „podgrupa normalna" na „ideał", a „grupa ilorazowa" na „pierścień ilorazowy".

We wspomnianych dwóch przypadkach notacja supremum to „$H + K$", nie zaś „HK".

Ogólnie [edytuj kod]

Aby uogólnić ten wynik na algebrę uniwersalną, podgrupy normalne muszą być zastąpione kongruencjami.

Krótko, jeżeli A jest algebrą uniwersalną, to **kongruencją** na A jest relacja równoważności Φ określona na A, która jest podalgebrą, gdy jest ona rozpatrywana jako podzbiór $A \times A$ (z działaniami określonymi po współrzędnych). Zbiór klas równoważności A/Φ może być przekształcony w algebrę tego samego typu poprzez zdefiniowanie działań na reprezentantach; będą one dobrze określone, ponieważ Φ jest podalgebrą $A \times A$.

Pierwsze twierdzenie [edytuj kod]

Jeżeli A, B są algebrami, a f homomorfizmem z A do B, to relacja równoważności Φ określona na A wzorem

$a \sim b \iff f(a) = f(b)$ jest kongruencją na A, zaś algebra A/Φ jest izomorficzna z obrazem f, czyli podalgebrą w B.

Drugie twierdzenie [edytuj kod]

Dla danej algebry A i jej podalgebry B oraz kongruencji określonej na A, niech $[B]\Phi$ będzie podzbiorem A/Φ wyznaczanym przez wszystkie klasy kongruencji zawierające element z B. Symbol Φ_B będzie oznaczał przecięcie Φ (rozpatrywane jako podzbiór $A \times A$) z $B \times B$. Wówczas $[B]\Phi$ jest podalgebrą A/Φ, a Φ_B jest kongruencją na B i wreszcie algebra $[B]\Phi$ jest izomorficzna z algebrą B/Φ_B.

Trzecie twierdzenie [edytuj kod]

Niech A będzie algebrą, a Φ oraz Ψ będą dwoma relacjami kongruencji określonymi na A, gdzie Ψ zawiera się w Φ. Wówczas Φ wyznacza kongruencję Θ na A/Ψ określoną wzorem

$[a]_\Psi \sim [b]_\Psi \iff a \sim_\Phi b$, a A/Φ jest izomorficzna z $(A/\Psi)/\Theta$.

Dla każdego pierścienia całkowitego P (zatem i struktur takich jak pierścień liczb całkowitych czy pierścień wielomianów o współczynnikach całkowitych) można zdefiniować ciało nazywane **ciałem ułamków**. Definiuje się je jako zbiór klas abstrakcji relacji równoważności $\sim$ określonej w iloczynie kartezjańskim $P \times P^*$ w następujący sposób:

$$[a, b] \sim [c, d] \iff ad = bc.$$

W zbiorze tym wprowadza się również działania dodawania i mnożenia:

$$[a, b] + [c, d] = [ad + bc, bd],$$
$$[a, b] \cdot [c, d] = [ac, bd].$$

Jak wspomniano wcześniej, ciało ułamków pierścienia liczb całkowitych jest izomorficzne z ciałem liczb wymiernych.

Istotność założenia całkowitości pierścienia [edytuj kod]

Jeżeli pierścień przemienny ma dzielniki zera, to nie można skonstruować na nim ciała ułamków: jeśli $xy = 0$ dla niezerowych $x, y \in P$, to

$$[1, 1] \sim [x, x] = [x, 1] \cdot [1, x] \sim [xy, y] \cdot [1, x] = [0, y] \cdot [1, x] \sim [0, 1] \cdot [1, x] = [0, x] \sim [0, 1],$$

czyli

$$[1, 1] \sim [0, 1],$$

stąd zaś dla dowolnego

$$[a, b] = [a, b] \cdot [1, 1] \sim [a, b] \cdot [0, 1] = [0, b] \sim [0, 1],$$

więc jest tylko jedna klasa abstrakcji – klasa $[0, 1]$, a z definicji ciało ma przynajmniej dwa różne elementy.

Dla pierścieni nieprzemiennych tworzenie ułamków bardzo się komplikuje.

Chińskie twierdzenie o resztach mówi, że układ kongruencji:

$$x \equiv y_1 \pmod{n_1},$$
$$x \equiv y_2 \pmod{n_2},$$
...
$$x \equiv y_k \pmod{n_k},$$

gdzie $y_1, y_2, \ldots, y_k$ są dowolnymi liczbami całkowitymi, a liczby $n_1, n_2, \ldots, n_k$ to liczby parami względnie pierwsze), spełnia dokładnie jedna liczba

$$1 \leqslant x \leqslant n_1 \cdot n_2 \cdot n_3 \cdot \ldots \cdot n_k$$ [1].

Jest to jedno z najważniejszych twierdzeń w teorii liczb i kryptografii.

Algorytm rozwiązywania układu kongruencji [edytuj kod]

Istnieje algorytm wyliczania x na podstawie takiego układu równań.

Mianowicie, niech

$$M = n_1 \cdot n_2 \cdot n_3 \cdot \ldots \cdot n_k$$

oraz $M_i = M / n_i$ ($i \leq k$). Wówczas na podstawie założenia n_i oraz M_i są względnie pierwsze, tzn. korzystając z rozszerzonego algorytmu Euklidesa istnieją takie liczby całkowite f_i, g_i ($i \leq k$), że

$$f_i n_i + g_i M_i = 1.$$

Niech $e_i = g_i M_i$ ($i \leq k$). Wówczas

$$e_i \equiv 1 \pmod{n_i}$$

oraz

$$e_i \equiv 0 \pmod{n_j}$$

gdy $j \neq i$. Wtedy x zdefiniowany wzorem

$$x = \sum_{i=1}^{k} y_i e_i$$

spełnia powyższy układ kongruencji, jest to jedno z rozwiazań - pozostałe różnią się o wielokrotność M.

Przykład [edytuj kod]

Dany jest układ kongruencji:

$$x \equiv 3 \pmod{4},$$
$$x \equiv 4 \pmod{5},$$
$$x \equiv 1 \pmod{7}.$$

Używając metody generowania kolejnych wielokrotności (która jest mało wydajnym algorytmem, aczkolwiek prawdopodobnie najlepszym do obliczania ręcznie):

Ogólne rozwiązanie pierwszego równania to 3 + 4*i*

Znajdujemy najmniejsze takie *i*, że *x* = 3 + 4*i* spełnia drugie równanie:

3 (0), 7 (1), 11 (2), 15 (3), 19 (4).

Najmniejsze takie *i* to 4.

Z dwóch pierwszych równań otrzymujemy zatem kongruencję *x* ≡ 19 (mod 20).

Ogólne rozwiązanie dwóch pierwszych równań to 19 + (4 · 5)*j*.

Znajdujemy najmniejsze takie *j*, że *x* = 19 + 20*j* spełnia trzecie równanie:

19 (0), 39 (1), 59 (2), 79 (3), 99 (4).

Czyli najmniejsze rozwiązanie to 99, a ogólne 99 + (4 · 5 · 7)*k*.

Uogólnienie [edytuj kod]

Niech *R* będzie pierścieniem przemiennym z jedynką, a $I_1, I_2, \ldots, I_n$ jego ideałami. Jeśli są one parami względnie pierwsze, tj.

$$I_i + I_j = R,\ (i \neq j,\ i,j \leqslant n),$$

to naturalny homomorfizm

$$\phi\colon R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

zdefiniowany przez warstwy elementu względem ideałów

$$\phi(a) = (a + I_1, a + I_2, \ldots, a + I_n)$$

jest epimorfizmem.

Wersja dla liczb wynika z zastosowania twierdzenia do pierścienia liczb całkowitych, będącego pierścieniem ideałów głównych.

Dziedzina całkowitości [edytuj]

Dziedzina całkowitości – niezerowy pierścień przemienny z jedynką bez (właściwych) dzielników zera. Pierścienie te są uogólnieniem pierścienia liczb całkowitych i stanowią one naturalny kontekst do badania podzielności ze względu na dość regularne reguły przeprowadzania rachunków; najistotniejszą ich własnością jest tzw. *prawo skracania*.

Nieprzemienne dziedziny całkowitości nazywa się **dziedzinami**, wiele pozycji jednak się nimi nie zajmuje (ograniczając się do klasy pierścieni przemiennych), nazywając dziedziny całkowitości w skrócie również *dziedzinami*. Inną nazwą dziedziny całkowitości, pochodzącą od Langa, jest **pierścień całkowity**.

Własności [edytuj kod]

- Niech R będzie dziedziną całkowitości. Jeżeli $a, b, c \in R$, przy czym $c \neq 0$, to zachodzi własność skracania: jeśli $ac = bc$, to $a = b$.
- Każde ciało jest dziedziną całkowitości.
- Każda skończona dziedzina całkowitości jest ciałem.

Dowód: Wystarczy wykazać, że dowolny element jest odwracalny. Rozważmy dla danego elementu a jego iloczyny ze wszystkimi elementami pierścienia: $aa_1, aa_2, \ldots, aa_n$. Gdyby wśród nich nie było jedynki, to pewien element występowałby dwa razy (co najmniej) dla iloczynów z różnymi elementami. Jednak wówczas $ab = ac$ i z własności skracania: $b = c$.

Definicję można rozszerzyć na dziedziny całkowitości; dział teorii pierścieni zajmujący się badaniem podzielności w pierścieniach nazywa się teorią podzielności. Jeżeli $x|y$ i $y|x$, to elementy x oraz y nazywa się *stowarzyszonymi*. Relacja stowarzyszenia zdefiniowana wzorem

$$x \sim y \iff x|y \wedge y|x$$

jest relacją równoważności. Można to wyrazić również następująco:

$$x \sim y \iff x = cy,$$

gdzie c jest elementem odwracalnym (*jednością*; w istocie są to dzielniki jedynki), tzn. intuicyjnie: elementy stowarzyszone „różnią się" o czynnik odwracalny. Jest to równoważne stwierdzeniu, iż jeżeli $x|y$, to dla dowolnej liczby w takiej, że $w \sim x$ zachodzi również $w|y$. Jest to powód dla którego wyróżnia się tradycyjnie w zbiorze dzielników pewne elementy (np. liczby dodatnie wśród liczb całkowitych): wtedy jeden z dzielników reprezentuje inne z nim stowarzyszone (w liczbach całkowitych odwracalne są wyłącznie 1 oraz -1). W ten sposób *dzielniki właściwe* można opisać jako dzielniki, które nie stowarzyszone z daną liczbą i nie będące przy tym jednościami. *Dzielniki nierozkładalne* to dzielniki niebędące jednością, który nie ma dzielników właściwych.

Największy dzielnik elementu x, który jest równocześnie dzielnikiem y nazywa się *największym wspólnym dzielnikiem* tych elementów, przy czym jest on określony z dokładnością do stowarzyszenia.

Relację podzielności można zdefiniować w dowolnej półgrupie. Jeżeli ma ona element zerowy, to każdy element jest dzielnikiem zera (w szczególności w liczbach całkowitych 0 jest wielokrotnością dowolnej liczby i każda liczba jest jej dzielnikiem).

Pierścień z jednoznacznością rozkładu [edytuj]

Pierścień z jednoznacznością rozkładu (pierścień Gaussa, UFD, od ang. *unique factorization domain*) – pierścień przemienny, którego każdy element nieodwracalny może być przedstawiony jako iloczyn elementów pierwszych w *jednoznaczny* sposób, tzn. jednoznaczny co do permutacji czynników. Pierścienie te uogólniają pierścień liczb całkowitych w ten sposób, że spełniają one także tezę podstawowego twierdzenia arytmetyki.

Poniższy ciąg zawierań zbiorów obrazuje pewne szczególne przypadki pierścieni z jednoznacznością rozkładu:

pierścienie z jednoznacznością rozkładu ⊃ dziedziny ideałów głównych ⊃ pierścienie euklidesowe ⊃ **ciała**

Definicja [edytuj kod]

Dziedzina całkowitości R nazywana jest **pierścieniem z jednoznacznością rozkładu** wtedy i tylko wtedy, gdy

- dla dowolnego niezerowego elementu nieodwracalnego $a \in R$ istnieją elementy nierozkładalne $a_1, a_2, \ldots, a_n \in R$ takie, że $a = a_1 \cdot a_2 \cdot \ldots \cdot a_n$.
- jeżeli $a_1 \cdot a_2 \cdot \ldots \cdot a_n = b_1 \cdot b_2 \cdot \ldots \cdot b_m$, gdzie wszystkie elementy a_i, b_i są nierozkładalne, to $m = n$ i istnieje permutacja π taka, że $a_i \sim b_{\pi(i)}$, to znaczy elementy te są stowarzyszone.

Własności [edytuj kod]

- Jeżeli *R* jest pierścieniem z jednoznacznością rozkładu, to istnieje w nim największy wspólny dzielnik.
- Twierdzenie Gaussa: Jeżeli *R* jest pierścieniem z jednoznacznością rozkładu, pierścień wielomianów *R[x]* również jest pierścieniem z jednoznacznością rozkładu.
- W pierścieniu z jednoznacznością rozkładu każdy element nierozkładalny jest pierwszy.

Pierścień ideałów głównych [edytuj]

Pierścień ideałów głównych (także **pierścien główny**) - w algebrze pierścień całkowity, którego każdy ideał jest ideałem głównym.

Własności [edytuj kod]

- Każdy pierścień główny jest pierścieniem noetherowskim ponieważ każdy jego ideał jest generowany przez zbiór jednoelementowy, a zatem skończony.
- Każdy pierścień główny jest pierścieniem z jednoznacznością rozkładu.
- Każde dwa elementy a, b pierścienia ideałów głównych P mają największy wspólny dzielnik $\mathrm{NWD}(a, b)$, który daje się zapisać w postaci $ax + by$ dla pewnych $x, y \in P$.
- W pierścieniu ideałów głównych P element $q \in P$ jest nierozkładalny wtedy i tylko wtedy, gdy ideał generowany przez ten element, (q) jest maksymalny, czyli wtedy i tylko wtedy, gdy pierścień ilorazowy $P/(q)$ jest ciałem.
- W pierścieniu ideałów głównych każdy ideał pierwszy jest maksymalny.

Przykłady [edytuj kod]

Pierścieniami głównymi są:

- pierścień liczb całkowitych,
- pierścień wielomianów o współczynnikach w dowolnym ciele,
- dowolne ciało,
- każdy pierścień Euklidesa.

Dziedzina Euklidesa [edytuj]

(Przekierowano z Pierścień euklidesowy)

Dziedzina Euklidesa (albo **pierścień Euklidesa**, **pierścień euklidesowy**) – w teorii pierścieni najbardziej ogólny typ pierścieni, w którym możliwe jest wyznaczenie największego wspólnego dzielnika za pomocą algorytmu Euklidesa.

Definicja [edytuj kod]

Dziedzinę całkowitości R nazywa się *dziedziną Euklidesa* (albo *pierścieniem Euklidesa*, *pierścieniem euklidesowym*), jeżeli istnieje taka funkcja

$$N\colon R \to \mathbb{N}$$

(nazywana *normą*), że

- $N(0) = 0$,
- dla dowolnych $a, b \in R$, gdzie $b \neq 0$, istnieją takie $q, r \in R$, że

  $a = bq + r$

  oraz zachodzi jeden z warunków: $r = 0$ lub $N(r) < N(b)$.

Czasami dodatkowo przyjmuje się również, że:

- $N(a) \leq N(ab)$ dla $a, b \in R$,

jednak nie jest to konieczne: każda dziedzina całkowitości R która może być wyposażona w funkcję M spełniającą pierwsze dwa warunki, może być również wyposażona w funkcję N spełniającą również trzeci warunek. Istotnie, dla $a \neq 0$ można zdefiniować $N(a)$ wzorem

$$N(a) = \min_{x \in R \setminus \{0\}} M(xa).$$

Własności [edytuj kod]

Każdy pierścień Euklidesa jest pierścieniem ideałów głównych.

Dowód. Każdy pierścień Euklidesa jest z definicji dziedziną całkowitości. Należy wykazać, że jeżeli I jest ideałem w pierścieniu Euklidesa R, to $I = bR$ dla pewnego $b \in R$. Jeżeli $I = \{0\}$, $I = 0R$. Niech $b \in I$, $b \neq 0$ w przypadku, gdy $I \neq \{0\}$. Bez straty ogólności, można przyjąć, że $v(b)$ jest minimalne, tzn. $v(b) \leq v(a)$ dla każdego niezerowego $a \in R$. Twierdzimy, że $I = bR$. Ponieważ, $b \in I$, zachodzi inkluzja $bR \subseteq I$, należy zatem wykazać inkluzję przeciwną. Niech $a \in R$. Istniają zatem takie $q, r \in R$, że $a = qb + r$. Ponieważ $v(b)$ jest minimalne, $r = 0$, czyli zachodzi równość $a = qb$, tj. $a \in bR$, co dowodzi inkluzji $I \subseteq bR$.

Istnieją pierścienie ideałów głównych, których nie da się wyposażyć w normę (tj. nie są pierścieniami euklidesowymi). Przykładem takiego pierścienia, jest

$$\mathbb{Z}\left[\tfrac{1+\sqrt{19}\mathrm{i}}{2}\right].$$

Największy wspólny dzielnik dwóch niezerowych elementów pierścienia Euklidesa można odnaleźć przy pomocy algorytmu Euklidesa. Jeżeli R jest pierścieniem Euklidesa, $a, b \in R \setminus \{0\}$ to można utworzyć taki ciąg równości

$$\begin{cases} a = bq_1 + r_1 \\ b = r_1q_2 + r_2 \\ r_1 = r_2q_3 + r_3 \\ r_2 = r_3q_4 + r_4 \\ \ldots, \end{cases}$$

aby

$$N(b) > N(r_1) > N(r_2) > \ldots.$$

Ciąg taki (jako malejący ciąg liczb całkowitych dodatnich) musi być skończony, zatem dla pewnej liczby naturalnej k zachodzi równość $r_{k+1} = 0$. Dla najmniejszego takiego k reszta r_k jest największym wspólnym dzielnikiem elementów $a, b \in R$. Zatem, jeśli można wyznaczyć $q_1, q_2, \ldots$ i $r_1, r_2, \ldots$, to można wyznaczyć największy wspólny dzielnik a i b.

Przykłady [edytuj kod]

Pierścieniami Euklidesa są:

- Pierścień liczb całkowitych z normą $N(x) = |x|$,
- Pierścień $\mathbb{Z}[i]$ liczb całkowitych Gaussa wraz z normą $N(z) = a^2 + b^2$, gdzie $z = a + bi$,
- Pierścień $\mathbb{Z}[e^{2\pi i/3}]$ liczb całkowitych Eisensteina z normą $N(z) = a^2 + b^2 - ab$, gdzie $z = a + b \cdot e^{2\pi i/3}$,
- Pierścień wielomianów $F[x]$ nad dowolnym ciałem F wyposażony z normę $N(f)$ = stopień wielomianu f jest pierścieniem Euklidesa. Dokładniej, własność ta charakteryzuje ciała pośród pierścieni, gdyż dla dowolnego pierścienia R następujące warunki są równoważne:
  - R jest ciałem,
  - Pierścień wielomianów $R[x]$ jest pierścieniem Euklidesowym,
  - Pierścień wielomianów $R[x]$ jest pierścieniem ideałów głównych.
- Niech p będzie liczbą pierwszą oraz niech T_p oznacza rodzinę liczb wymiernych postaci m/n dla których p nie dzieli n. Rodzina T_p jest podpierścieniem ciała liczb wymiernych. Każdy element pierścienia T_p może być zapisany w postaci $p^k\ell / n$, gdzie p nie dzieli ani ℓ ani n. Funkcja v dana wzorem $v(p^k\ell / n) = k$ dla $p^k\ell / n \neq 0$ jest normą, tzn. T_p jest pierścieniem Euklidesa.

4.8 Pierścienie faktorialne

Wprowadzimy teraz kolejny typ pierścieni, który za wzorzec własności przyjmuje znane nam Zasadnicze Twierdzenie Arytmetyki — jak pamiętamy mówi ono o tym, że każdą liczbę całkowitą (poza zerem i jednościami) można przedstawić w jednoznaczny sposób jako iloczyn liczb pierwszych. Odpowiednikami liczb pierwszych w ogólnej sytuacji staną się elementy nierozkładalne.

Definicja 4.8.1 (rozkład jednoznaczny). *Jeśli P jest pierścieniem całkowitym, to mówimy, że element $a \in P$ ma rozkład jednoznaczny, gdy:*

(1) *element a jest nierozkładalny lub można go zapisać jako skończony iloczyn elementów nierozkładalnych (rozkład skończony),*

(2) *jeśli element a ma dwa rozkłady na elementy nierozkładalne $a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$, to $r = s$ oraz istnieje taka permutacja $\sigma \in S_r$, że $q_i \sim p_{\sigma(i)}$ dla $i = 1, \ldots, r$.*

Wprowadzimy teraz definicję tytułowego pierścienia faktorialnego.

Definicja 4.8.2 (pierścień faktorialny). *Całkowity pierścień P nazywamy* ***pierścieniem faktorialnym*** *(dziedziną z jednoznacznością rozkładu, pierścieniem Gaussa), jeśli każdy niezerowy element nieodwracalny tego pierścienia posiada rozkład jednoznaczny.*

Przykład 4.8.3. *W pierścieniu $\mathbb{Z}[i\sqrt{3}]$ elementy 4 i $2 - 2i\sqrt{3}$ nie mają NWD.*

Dzielnikami 4 są $\pm 1, \pm 4, \pm 2, \pm(1+i\sqrt{3}), \pm(1-i\sqrt{3})$. Wspólne dzielniki obu liczb: $\pm 1, \pm 2, \pm(1+i\sqrt{3})$ $\pm(1 - i\sqrt{3})$.

Jednak 2 nie dzieli ± 1, i 2 nie dzieli $\pm(1 \pm i\sqrt{3})$ ale też $1 + i\sqrt{3}$ nie dzieli ± 2.

Przedstawimy teraz fundamentalne własności takiego pierścienia.

Twierdzenie 4.8.1 (charakteryzacja pierścienia faktorialnego). *Jeśli P jest pierścieniem całkowitym, w którym każdy niezerowy element nieodwracalny posiada rozkład skończony, to następujące warunki są równoważne:*

(1) *każdy niezerowy element nieodwracalny posiada rozkład jednoznaczny,*

(2) *dla dowolnych $a, b \in P^*$ mamy $NWW(a, b) \neq \varnothing$,*

(3) *dla dowolnych $a, b \in P^*$ mamy $NWD(a, b) \neq \varnothing$,*

(4) *ideał generowany przez element nierozkładalny w tym pierścieniu jest ideałem pierwszym.*

Rozszerzenie ciała [edytuj]

(Przekierowano z Rozszerzenia ciał)

Rozszerzenie ciała - w teorii ciał jest to większe w sensie inkluzji ciało zawierające dane ciało. Na przykład, ciało liczb rzeczywistych jest rozszerzeniem ciała liczb wymiernych; ciało liczb zespolonych jest rozszerzeniem ciał liczb rzeczywistych (więc także wymiernych). Rozszerzenia ciał są centralnym pojęciem teorii Galois. Wyróżnia się wiele rodzajów rozszerzeń ciał ze względu na ich własności.

Każde rozszerzenie L ciała K jest przestrzenią liniową nad K. Wymiar tej przestrzeni oznacza się przez $[L:K]$ i nazywa **stopniem rozszerzenia** $L \supset K$.

Rozszerzenie ciała o pierwiastki wielomianu [edytuj kod]

Z teorii równań algebraicznych wynika, że każdy niesprzeczny układ równań nad ciałem K ma rozwiązanie w pewnym ciele L. W szczególności, jeżeli f jest wielomianem o współczynnikach z ciała K, to istnieje rozszerzenie L ciała K, które zawiera pierwiastek a wielomianu f.

Mówimy, że ciało L jest **rozszerzeniem ciała** K **o pierwiastek** a wielomianu $f \in K[x]$ wtedy i tylko wtedy, gdy $L = K(a)$[1].

Dla przykładu, ciało liczb zespolonych jest rozszerzeniem ciała liczb rzeczywistych o pierwiastek wielomianu $h(x) = x^2 + 1$.

Jeśli L jest rozszerzeniem ciała K oraz $a \in L$, to

$$K(a) = \{\tfrac{f(a)}{g(a)} \in L\colon\ f, g \in K[x], g(a) \neq 0\}.$$

Rozszerzenie o pierwiastek danego wielomianu nie jest wyznaczone jednoznacznie w przypadku gdy wielomian jest rozkładalny. W przypadku gdy dany wielomian jest nierozkładalny, to rozszerzenia wyznacza się z dokładnością do izomorfizmu.

Ciało rozkładu wielomianu [edytuj kod]

Mówimy, że ciało L jest ciałem rozkładu wielomianu $f \in K[x]$ wtedy i tylko wtedy, gdy wielomian f rozkłada się w pierścieniu $L[x]$ na czynniki liniowe oraz

$$L = K(a_1, \ldots, a_m),$$

gdzie $a_1, \ldots, a_m$ są wszystkimi pierwiastkami f w ciele L.

Dla każdego wielomianu stopnia dodatniego istnieje jego ciało rozkładu. Dowolne dwa ciała rozkładu tego wielomianu są izomorficzne.

Rozszerzenie algebraiczne [edytuj kod]

Zobacz też: element algebraiczny.

Rozszerzenie L ciała K nazywamy **algebraicznym** wtedy i tylko wtedy, gdy każdy element $a \in L$ jest algebraiczny nad K.

Dla przykładu, każdy element ciała skończonego jest algebraiczny nad podciałem prostym, zawartym w tym ciele.

Dla rozszerzenia $L \supseteq K$ i $a \in L$ następujące warunki są równoważne

- a jest algebraiczny nad K,
- $K[a] = K(a)$,
- $[K(a) : K] < \infty$.

Stopień rozszerzenia $K(a) \supseteq K$ nazywa się **stopniem elementu algebraicznego** $a \in K$. Stopień ten jest równy stopniowi wielomianu nierozkładalnego $f \in K[x]$ takiemu, że $f(a) = 0$, a także minimalnemu stopniowi niezerowego wielomianu $f \in K[x]$ takiego, że $f(a) = 0$

Rozszerzenie rozdzielcze [edytuj kod]

Zobacz też: element rozdzielczy.

Rozszerzenie L ciała K nazywamy **rozdzielczym** wtedy i tylko wtedy, gdy każdy element $a \in L$ jest rozdzielczy nad K.

Jeśli ciało K ma charakterystykę równą 0, to każde jego rozszerzenie algebraiczne jest rozdzielcze. W szczególności, każde algebraiczne rozszerzenie ciała liczb wymiernych jest rozdzielcze.

Rozszerzenie czysto przestępne [edytuj kod]

Rozszerzenie L ciała K nazywamy **czysto przestępnym** wtedy i tylko wtedy, gdy istnieje zbiór algebraicznie niezależny $A \subseteq L$, taki że $K(A) = L$.

Rozszerzenia skończone [edytuj kod]

Rozszerzenie L ciała K nazywa się **skończonym** wtedy i tylko wtedy, gdy ma skończony stopień, tzn. $[L : K] < \infty$.

Każde rozszerzenie skończone jest algebraiczne. Jeśli $K_2 \supseteq K_1 \supseteq K$ jest ciągiem rozszerzeń ciał, to rozszerzenie $K_2 \supseteq K$ jest skończone wtedy i tylko wtedy, gdy rozszerzenia $K_2 \supseteq K_1$ i $K_1 \supseteq K$ są skończone. Ponadto

$$[K_2 : K] = [K_2 : K_1] \cdot [K_1 : K].$$

Rozszerzenie normalne [edytuj kod]

Osobny artykuł: Rozszerzenie normalne.

Rozszerzenie L ciała K nazywamy **normalnym** wtedy i tylko wtedy, gdy jest algebraiczne i dla każdego $b \in L$ wielomian nierozkładalny $f \in K[x]$, którego pierwiastkiem jest b rozkłada się w $L[x]$ na czynniki liniowe.

Element algebraiczny [edytuj]

Element algebraiczny - uogólnienie pojęcia liczby algebraicznej na rozszerzenia dowolnych ciał. Liczby algebraiczne to elementy algebraiczne ciała liczb zespolonych nad ciałem liczb wymiernych.

Definicja [edytuj kod]

Niech K będzie podciałem ciała L. Element $a \in L$ nazywamy **elementem algebraicznym** nad K wtedy i tylko wtedy, gdy istnieje niezerowy wielomian o współczynnikach z ciała K, którego pierwiastkiem jest a.

Element nie będący algebraicznym nad K nazywamy **elementem przestępnym** nad K w ciele L.

Własności [edytuj kod]

- Zbiór wszystkich elementów ciała L algebraicznych nad K tworzy ciało, zwane **rozszerzeniem algebraicznym** ciała K.
- Jeśli $a \in L$ jest elementem algebraicznym nad K, to $K(a) = K[a] = \{f(a) \in L\colon f \in L[x]\}$ (por. oznaczenia w artykule rozszerzenia ciał)
- Dla każdego elementu algebraicznego $a \in L$ nad K istnieje dokładnie jeden unormowany wielomian pierwszy p_a o współczynnikach z ciała K (tj. element pierwszy w pierścieniu $K[x]$), którego pierwiastkiem jest a. Wielomian p_a nazywamy **wielomianem minimalnym** elementu algebraicznego a. Zachodzi $[F(a) : F] = \deg p_a$. Stopień ten nazywamy **stopniem elementu algebraicznego** a.

Element nazywa się pierwotny, jeśli każdy element ciała jest jego potęgą.

Rozszerzenie normalne [edytuj]

Rozszerzenie normalne - rozszerzenie ciała takie, że dla każdego elementu, który należy do rozszerzenia, a nie należy do ciała, każdy wielomian nierozkładalny, którego ten element jest pierwiaskiem, rozkłada się na czynniki liniowe w pierścieniu wielomianów o współczynnikach z rozszerzenia. Rozszerzenia normalne odgrywają dużą rolę w teorii Galois.

Definicja [edytuj kod]

Rozszerzenie L ciała K nazywamy **normalnym** wtedy i tylko wtedy, gdy jest algebraiczne i dla każdego $b \in L$ wielomian nierozkładalny $f \in K[x]$, którego pierwiastkiem jest b rozkłada się w $L[x]$ na czynniki liniowe.

Warunki równoważne [edytuj kod]

Niech L będzie skończonym rozszerzeniem ciała K. Następujące warunki są równoważne.

1. L/K jest rozszerzeniem normalnym.
2. L jest ciałem rozkładu pewnego wielomianu o współczynnikach z ciała K.
3. Dla każdego zanurzenia $\varphi: L \to \overline{K}$
   $\varphi(L) = L$,

gdzie $\overline{K}$ oznacza algebraiczne domknięcie ciała K.

Własności [edytuj kod]

Jeśli K, M, L są ciałami oraz $K \subseteq M \subseteq L$, a ponadto rozszerzenie L/K jest normalne, to rozszerzenie L/M również.

Przykłady [edytuj kod]

- Rozszerzenie $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ jest normalne, bo jest ciałem rozkładu wielomianu $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$.

Ciało skończone [edytuj]

Ciało skończone lub **ciało Galois** – w teorii ciał ciało skończonego rzędu, tj. o skończonej liczbie elementów; druga z nazw pochodzi od nazwiska francuskiego matematyka Évariste'a Galois, który znacząco przyczynił się do rozwoju badań nad ciałami skończonymi oraz wskazał ich zastosowanie w tzw. teorii Galois dającej m.in. rozstrzygającą odpowiedź na pytania dotyczące możliwości wykonania bądź nie klasycznych konstrukcji w geometrii euklidesowej, czy też zgrabnie uzasadniającej brak ogólnych wzorów na pierwiastki wielomianów wyższych stopni.

W artykule za naturalne uważa się dodatnie liczby całkowite, ciało proste o p elementach (tzn. rzędu p) oznaczane będzie zamiennie jednym z symboli $\mathbf{F}_p$ oraz $\mathbb{Z}/(p)$; inną stosowaną notacją jest $\mathrm{GF}(p)$ (od ang. Galois field, *ciało Galois).*

Konstrukcja i własności [edytuj kod]

Zobacz też: wielomian i pierścień wielomianów.

Niech p będzie liczbą pierwszą, a π będzie unormowanym (monicznym) wielomianem nierozkładalnym stopnia n należącym do $\mathbf{F}_p[x]$ (tj. zmiennej x o współczynnikach z ciała $\mathbf{F}_p$). Pierścień $\mathbf{F}_p[x]/(\pi)$ jest wtedy ciałem rzędu p^n[1]. Każde ciało skończone ma rząd wyrażający się naturalną potęgą liczby pierwszej[2], a ponadto jest izomorficzne z $\mathbf{F}_p[x]/(\pi)$ dla pewnej liczby pierwszej p i unormowanego wielomianu nierozkładalnego π należącego do $\mathbf{F}_p[x]$[3][4][5].

Dowolne ciało skończone można opisać jako ciało rozkładu wielomianu wyłącznie w zależności od rzędu ciała: ciało skończone o rzędzie p^n będącym potęgą liczby pierwszej jest ciałem rozkładu wielomianu ${}_xp^n - {}_x$ nad ciałem $\mathbf{F}_p$[6]; wynika stąd, że ciała skończone tego samego rzędu są izomorficzne[7][8]. Wychodząc stąd można dowieść istnienia ciał skończonych dowolnego rzędu będącego potęgą liczby pierwszej:

Twierdzenie

Dla dowolnych liczb pierwszej p i naturalnej n istnieje ciało rzędu p^n.

Ciało algebraicznie domknięte [edytuj]

Ciało algebraicznie domknięte F to takie ciało, w którym każdy wielomian stopnia co najmniej pierwszego jednej zmiennej ma pierwiastek w F.

Równoważnie można je zdefiniować jako ciało, które nie ma nietrywialnych rozszerzeń algebraicznych: z tego, że K jest rozszerzeniem algebraicznym F, wynika, że $K = F$.

Każde ciało jest podciałem pewnego ciała algebraicznie domkniętego. Za przykład niech posłuży ciało liczb rzeczywistych. Ciało to nie jest algebraicznie domknięte: wielomian $w(x) = x^2 + 1$ nie ma pierwiastków w tym ciele.

Rozszerzenie ciała F, które jest algebraiczne i jest ciałem algebraicznie domkniętym, nazywamy **domknięciem algebraicznym** ciała F.

Na przykład domknięciem algebraicznym ciała liczb rzeczywistych jest ciało liczb zespolonych (dla powyższego wielomianu pierwiastkami w ciele liczb zespolonych są i oraz $-i$).

Ponieważ dla każdego ciała F istnieje jego rozszerzenie K będące ciałem algebraicznie domkniętym, a zbiór elementów algebraicznych nad F należących do K jest rozszerzeniem algebraicznym F oraz ciałem algebraicznie domkniętym, dla każdego ciała istnieje jego algebraiczne domknięcie.

Twierdzenie mówiące o tym, że ciało liczb zespolonych jest ciałem algebraicznie domkniętym nazywa się "zasadniczym twierdzeniem algebry" i pociąga za sobą istotne konsekwencje, jak chociażby fakt, że każdą macierz o współczynnikach zespolonych można sprowadzić do postaci Jordana.

Jedną z najważniejszych własności ciał algebraicznie domkniętych jest twierdzenie Hilberta o zerach:

Jeśli F jest ciałem algebraicznie domkniętym, to dla każdych liczb naturalnych n, m i dla dowolnych wielomianów $f_1(X_1, X_2, \ldots, X_n), \ldots, f_m(X_1, X_2, \ldots, X_n)$ o współczynnikach z ciała F następujące warunki są równoważne:

- układ równań $f_1(X_1, X_2, \ldots, X_n) = 0, \ldots, f_m(X_1, X_2, \ldots, X_n) = 0$ ma rozwiązanie w F;
- ideał $(f_1(X_1, X_2, \ldots, X_n), \ldots, f_m(X_1, X_2, \ldots, X_n))$ jest ideałem właściwym pierścienia wielomianów $F[X_1, X_2, \ldots, X_n]$.

Innymi słowy, taki układ równań nie ma rozwiązań wtedy i tylko wtedy, gdy jest sprzeczny, tzn. gdy istnieją wielomiany $g_1(X_1, X_2, \ldots, X_n), \ldots, g_m(X_1, X_2, \ldots, X_n)$ o współczynnikach z ciała F takie, że

$$g_1 \cdot f_1 + \cdots + g_m \cdot f_m = 1.$$

Domknięcie algebraiczne ciała $\mathbb{Z}_p$ [edytuj kod]

Nie istnieją ciała skończone, algebraicznie domknięte. Oznacza to, że istnieją ciała nieskończone o skończonej charakterystyce. Przykładem takiego ciała może być algebraiczne domknięcie ciała $GF(3) = \mathbb{Z}_3 = \{0, 1, 2\}$:

Dla każdego $k = 1, 2, \ldots$ istnieje jedyne ciało $GF(3^k)$ o 3^k elementach. Na przykład, ciało $GF(3^2)$ można reprezentować jako $\mathbb{Z}_3(\sqrt{2}) = \{0, 1, 2,\ \alpha,\ \alpha+1,\ \alpha+2,\ 2\alpha,\ 2\alpha+1,\ 2\alpha+2\}$, gdzie $\alpha^2 = 2$.

Dla każdego $m, n \in \mathbb{N} \setminus \{0\}$, $GF(3^m) \subseteq GF(3^n)$ wtedy i tylko wtedy, gdy m jest dzielnikiem liczby n. Więc dla każdego m, n można znaleźć skończone ciało C zawierające $GF(3^m)$ i $GF(3^n)$, np ciało $GF(3^{mn})$. Z tego możemy wywnioskować, że suma wszystkich ciał $GF(3^n)$ jest znowu ciałem, które oznaczamy $\overline{\mathbb{Z}}_3$.

Każdy wielomian z współczynnikami w ciele $\overline{\mathbb{Z}}_3$ ma w rzeczywistości współczynniki w pewnym ciele skończonym $GF(3^n)$, więc ma pierwiastek w pewnym skończonym rozszerzeniu ciała $GF(3^n)$; to rozszerzenie musi być ciałem skończonym o charakterystyce 3, tzn. pewnym ciałem $GF(3^{n'}) \subseteq \overline{\mathbb{Z}}_3$.

Więc ciało $\overline{\mathbb{Z}}_3$ (zbiór nieskończony ale przeliczalny) jest algebraicznie domknięte.

Domknięcie algebraiczne ciała liczb wymiernych [edytuj kod]

Domknięcie algebraiczne $\overline{\mathbb{Q}}$ ciała liczb wymiernych $\mathbb{Q}$ nazywamy ciałem liczb algebraicznych. Jest ono (przeliczalnym) podciałem ciała liczb zespolonych; elementy ciała $\overline{\mathbb{Q}}$ nazywamy liczbami algebraicznymi; pozostałe liczby zespolone nazywamy liczbami przestępnymi. Georg Cantor udowodnił, że ciało $\overline{\mathbb{Q}}$ jest przeliczalne, a ciała $\mathbb{R}$ i $\mathbb{C}$ są nieprzeliczalne. Dowód Cantora. używając metody z nowego przez jego stworzonej teorii monogości, był nową konstrukcją liczb przestępnych; Liouville w 1844 r. znalazł liczby przestępne używając metody z teorii liczb.