Wykłady z algebry abstrakcyjnej

A. Paweł Wojda

17 października 2016

Spis treści

Wstęp **6**

1 Arytmetyka liczb całkowitych **11**
1.1 Liczby pierwsze . . . 11
1.2 Algorytm Euklidesa . . . 14
1.3 Zadania . . . 18

2 Grupy **19**
2.1 Funkcja φ Eulera . . . 21
2.2 Podgrupy . . . 23
2.3 Homorfizmy grup, grupy izomorficzne . . . 24
2.4 Grupy cykliczne . . . 26
2.5 Twierdzenie Cayleya . . . 29
2.6 Twierdzenie Lagrange'a . . . 30
2.6.1 Wnioski z twierdzenia Lagrange'a . . . 32
2.7 Grupa dihedralna . . . 33
2.8 Podgrupy normalne . . . 34
2.8.1 Podstawowe twierdzenie o izomorfizmie grup . . . 36
2.9 Sprzężenie podgrupy . . . 38
2.10 Grupy alternujące . . . 41
2.11 Zadania . . . 42

3 Arytmetyka modularna **45**
3.1 Twierdzenie Eulera i Małe Twierdzenie Fermata . . . 45
3.2 Chińskie twierdzenie o resztach – równania modularne . . . 46
3.3 Residua kwadratowe . . . 48
3.4 Zasady kryptografii . . . 50
3.4.1 Metoda Rabina . . . 51
3.4.2 Metoda RSA . . . 52
3.5 Zasady kryptografii . . . 54
3.5.1 Metoda Rabina . . . 55
3.5.2 Metoda RSA . . . 56

4 Działanie grupy na zbiorze **59**
4.1 Lemat Burnside'a 62
4.2 Grupa obrotów sześcianu 67
4.3 Zadania 68

5 Skończone grupy abelowe **69**
5.1 Twierdzenie Cauchy'ego dla grup abelowych 70
5.2 Zasadnicze twierdzenie o skończonych grupach abelowych 71
5.3 Zadania 75

6 Twierdzenia Sylowa **79**
6.1 Pierwsze twierdzenie Sylowa 79
6.1.1 Wnioski z pierwszego twierdzenia Sylowa 81
6.1.2 Twierdzenie o rozkładzie na orbity 82
6.2 Drugie twierdzenie Sylowa 84
6.3 Wnioski z Drugiego Twierdzenia Sylowa 85
6.4 Trzecie twierdzenie Sylowa 86
6.5 Wnioski z twierdzeń Sylowa 87
6.6 Zastosowanie w matematyce dyskretnej 88
6.6.1 Grafy samodopełniające 88
6.6.2 Twierdzenie Muzychuka 88
6.7 Zadania 92

7 Grupy rozwiązalne **95**
7.1 Komutatory i komutanty 97
7.2 Twierdzenia o izomorfizmie grup 99
7.3 Warunek konieczny i wystarczający rozwiązalności 101
7.4 Zadania 103

8 Pierścienie i ciała **105**
8.1 Przykłady pierścieni 106
8.2 Podpierścienie 107
8.3 Ideały 107
8.4 Ideały i pierścienie główne 109
8.5 Homomorfizmy pierścieni 109
8.6 Podzielność w pierścieniach 111
8.7 Charakterystyka pierścienia 114
8.8 Zadania 116

9 Pierścienie Gaussa **119**
9.1 Pierścienie wielomianów 121
9.2 Pierścienie główne 123
9.3 Pierścienie euklidesowe 125
9.4 Zasadnicze Twierdzenie Arytmetyki 127
9.5 Ciało ułamków pierścienia całkowitego 129
9.6 Homomorfizmy pierścieni 130

9.7 Wielomiany nad pierścieniami Gaussa 131
9.8 Twierdzenie Gaussa 134
9.9 Wielomiany nieprzywiedlne 134
9.10 Zadania 137

10 Wielomiany wielu zmiennych **139**
10.1 Wielomiany symetryczne 139
10.2 Twierdzenie Wilsona 141
10.3 Podstawowe twierdzenie o wielomianach symetrycznych 142
10.4 Zadania 146

11 Rozszerzenia ciał **147**
11.1 Ciało rozkładu wielomianu 150
11.2 Zasadnicze Twierdzenie Algebry 152
11.3 Rozszerzenia o skończoną liczbę elementów 155
11.4 Rozszerzenia skończone i algebraiczne 155
11.5 Rozszerzenia przestępne 161
11.6 Rząd ciała skończonego 163
11.7 Pochodne wielomianów i krotności pierwiastków 164
11.8 Ciało Galois rzędu p^n 165
11.9 Rozszerzenia ciał izomorficznych 169
11.10Zadania 172

12 Teoria Galois **175**
12.1 Grupy Galois 175
12.2 Grupa Galois rozszerzenia prostego 176
12.3 Wielomiany i ciała rozdzielcze 183
12.4 Twierdzenie o elemencie prymitywnym 187
12.5 Twierdzenie Dedekinda-Artina 190
12.6 Rozszerzenia Galois 194
12.6.1 Wnioski z twierdzenia o skończonym rozszerzeniu Galois 197
12.6.2 Zasadnicze twierdzenie teorii Galois 199
12.7 Zadania 203

13 Ewaryst Galois **205**

14 Wskazówki do wybranych zadań **207**
14.1 Rozdział 2 207
14.2 Rozdział 4 207
14.3 Rozdział 5 207
14.4 Rozdział 6 207
14.5 Rozdział 7 208
14.6 Rozdział 8 209
14.7 Rozdział 11 210
14.8 Rozdział 12 210

15 Oznaczenia **213**

Bibliografia **217**

Index **217**

Wstęp

Nazwa **algebra** pochodzi od tytułu dzieła arabskiego matematyka działającego w IX wieku w Bagdadzie, Muhammada Ibn Mussa Al Chwarizimi: *Hisab al-dżabr wal mukabala* (w transkrybcji polskiej, oczywiście). Algebra jest zniekształconym **al-dżabr** z owego tytułu[1]. Tytuł ten oznacza *Sztuka redukcji i przenoszenia*, zaś samo dzieło arabskiego matematyka dotyczyło rozwiązywania równań algebraicznych stopni pierwszego i drugiego. Al Chwarizimi był główną postacią znakomitej instytucji, którą był bagdadzki *Dom Nauki*, prekursor późniejszych uniwersytetów i instytucji naukowych. Nazwisko Al Chwarizimiego, także zniekształcone[2], stało się źródłem nazwy *algorytm*, tak ważnej we współczesnej matematyce i informatyce.
Zainteresowanych historią matematyki namawiam gorąco do przeczytania pięknej książki Marka Kordosa *Wykłady z historii matematyki*, dzięki której można poznać historię matematyki, prześledzić jak powstawała i zrozumieć jak bardzo niebanalnymi były, dla pozbawionych współczesnego formalizmu algebraicznego uczonych, działających we wcale niedawnej przeszłości wieków średnich, najprostsze operacje algebraiczne.

Poza aspektami historycznymi, warto w tym miejscu zwrócić uwagę na jeszcze jedną sprawę. Ta część algebry, która jest obiektem niniejszej książki, najczęściej nazywana jest *algebrą abstrakcyjną*. To piękna i dobra nazwa, która wyróżnia ten dział od *algebry liniowej*. Niestety przymiotnik *abstrakcyjna* sugruje też: *niekoniecznie potrzebna*. To oczywista nieprawda - nawet podczas tego wykładu, którego merytoryczna zawartość jest z konieczności bardzo ograniczona, będą okazje do poznania niektórych bardzo konkretnych zastosowań. Więcej zastosowań algebry abstrakcyjnej studenci matematyki (a także informatyki) poznają z pewnością z pewnością na innych przedmiotach (kodowanie, matematyka dyskretna, teoria algorytmów...).

Wykład algebry abstrakcyjnej jest prowadzony zazwyczaj po takich przedmiotach jak *Wstęp do matematyki* czy *Algebra liniowa*. Stąd nie definiuję tak znanych pojęć

[1] W językach angielskim i francuskim podobieństwo słowa *algebra* czy też *algèbre* do arabskiego oryginału jest znacznie wyraźniejsze niż w języku polskim.

[2] Tytuł dzieła Al Chwarizimiego przetłumaczony na łacinę brzmiał *Algorithmi de numero Indorum*, co miało znaczyć: *Al Chwarizimiego dzieło o liczbach indyjskich.* To właśnie dzieki temu dziełu Europa poznała dziesiątkowy system pozycyjny i liczbę zero, które matematycy arabscy przejęli od Hindusów.

jak zbiory liczbowe zaś podając definicje podstawowych struktur algebraicznych, takich jak grupa, pierścień czy ciało, robię to bardzo skrótowo, bez wielu przykładów, zakładając, że pojęcia te są czytelnikowi znane. Zakładam także, że relacje, szczególnie relacje równoważnościowe, klasy równoważności są znane czytelnikowi, podobnie jak zbiory $\mathbb{Z}_n$ i działania w tych zbiorach. Niektóre z powyższych pojęć opisane są w sposób przystępny, bardzo ładny a jednak z zachowaniem należytego rygoryzmu matematycznegoi w słynnej książce Couranta i Robbinsa [7]. Polecam wszystkim, także jako przykład, że można pięknie się zestarzeć - minęło 70 lat od pierwszego, amerykańskiego wydania tej książki.

Materiał tu zawarty starałem się ułożyć w taki sposób, by te jej części. które mają zastosowania później nie były od tych zastosowań zbytnio oddalone. Stąd właśnie po rozdziale o grupach pojawia się krótki rozdział o arytmetyce modularnej, gdzie znajduje zastosowanie twierdzenie Lagrange'a. Zaraz potem, w rozdziale piątym podaję zastosowanie twierdzenia chińskiego o resztach i twierdzeń Fermata i Eulera w kryptografii. Podobnie, o sprzężeniach podgrup i podgrupach normalnych mowa jest dopiero w rozdziale o siódmym o twierdzeniach Sylowa - po rozdziale o działaniach grup na zbiorach dlatego, że w dowodach tych twierdzeń działania grup na zbiorach stosowane są wielokrotnie.

Zdaję sobie sprawę, że umieszczenie na początku książki krótkiego rozdziału na temat pewnych, wybranych własności liczb całkowitych jest dyskusyjny. Wszystkie te własności wynikają natychmiast z dowodzonych w następnych rozdziałach, własności pierścieni. Jednak grupy (addytywne i multyplikatywne) $\mathbb{Z}_n$ i $\mathbb{Z}_n^*$, bardzo ważne ze względu na zastosowania w kryptografii i jako najwygodniejsze przykłady grup skończonych, występują już w rozdziale następnym (rozdział 2: Grupy).

Niniejsza książka jest adresowana przede wszystkim do studentów matematyki na Wydziale Matematyki Stosowanej AGH, dla których wykład z algebry prowadzę od kilku lat, choć mam nadzieję, że może być użyteczna nie tylko dla nich. Studenci mogli korzystać z kolejnych wersji tekstu, który był im udostępniany pocztą elektroniczną.

Istnieje bardzo wiele podręczników algebry, część z nich jest wymieniona w bibliografii na końcu *Wykładów ....* Są wśród nich książki zupełnie nowe i znakomite, wydane ostatnio (jak chociażby podręczniki Gilberta i Nicholsona [10], Nicholsona [16], Kostrykina [14],[15]), lub starsze (Birkhoff i MacLane [3], Birula-Białynicki [2], Opial [17]) o nieprzemijającej wartości. Jeśli jednak postanowiłem spisać moje wykłady to po to, żeby studenci mieli pomoc materiał w tej formie i układzie, który później jest wymagany podczas egzaminów. Poza tym, niektóre z książek zawartych w bibliografii nigdy nie zostały przetłumaczone na język polski. Książka Zdzisława Opiala mimo, że wykorzystywana była i jest przez studentów pewno wszystkich polskich uczelni[3] *Algebra Wyższa* nigdy nie została przyzwoicie wydana, nad czym należy ubolewać.

[3] W Krakowie nawet w antykwariatach, tak licznych w tym mieście, książka Opiala praktycznie się nie pojawia. Wynika to stąd, jak mnie poinformowano, iż biblioteka jednej z największych uczelni tego miasta ma nieformalną umowę z najważnieszymi antykwariatami, że jeśli tylko pojawia się egzemplarz tej książki jest rezerwowany i następnie kupowany przez bibliotekę. To ogromny sukces książki i jej autora, ale dowód także, że z polityką wydawnictw coś nie do końca jest tak.

A. Paweł Wojda

Kraków

Notatki w zasadzie co roku są dostosowywane do tego o czym mówię na wykładach, co roku są więc trochę inne. Niemniej nowa ich edycja do wszystkich poprzednich różni się bardzo wyraźnie i jest tak dlatego, że służyć ma nie tylko studentom drugiego roku, ale także studentom lat starszych, dla których ob bieżącego prowadzę przedmiot obieralny *Algebra 2*. Tekst przeznaczony dla nich, dla studentów *Algebry 2* jest niebieski, choć nie jest to do końca konsekwentne, część tego niebieskiego tekstu w roku bieżącym wykładałem w ramach *Algebry*.
Tegoroczne *Notatki* dedykuję studentom, którzy jako pierwsi wysłuchali praktycznie całości tego tekstu: *dwum Krzysztofom (Blaszyńskiemu i Różańskiemu), Marlenie Ciężak, Sebastianowi Gwizdkowi, Jerzemu Konarskiemu, Hirkowi Kubicy, Agnieszce Michałek, Ani Nowak, Mateuszowi Rakowskiemu, Bartoszowi Sobolewskiemu, Marcinowi Stawiskiemu, dwum Kasiom (Szczepańskiej i Wójcik), Paulinie Wójcik i Szymonowi Wrzoskowi*. Wszyscy oni, mam wrażenie, bardzo uważnie wysłuchali wykładów (w zasadzie zajęcia miały charakter konwersatorium), uczestniczyli w nich aktywnie nie wahając się zadawać pytań. Dla mnie, jako wykładowcy, spotkania te były przyjemne i inspirujące, bardzo wszystkim wymienionym za nie dziękuję.

A. Paweł Wojda
Kraków, 2 stycznia 2014

Rozdział 1

Arytmetyka liczb całkowitych

Poniżej przypomnimy niektóre definicje i własności liczb całkowitych, które potrzebne nam będą w dalszym ciągu wykładu. Później zobaczymy, że twierdzenia, które podamy i udowodnimy w tym krótkim wprowadzeniu są bardzo szczególnymi przypadkami twierdzeń bardziej ogólnych. Niemniej warto już teraz o nich powiedzieć ponieważ będą nam bardzo szybko potrzebne oraz dlatego, że łatwiej będzie później dowody twierdzeń dotyczących struktur abstrakcyjnych zrozumieć.

1.1 Liczby pierwsze

Liczbami pierwszymi nazywamy liczby naturalne[1], których nie da się przedstawić w postaci iloczynu co najmniej dwóch liczb naturalnych różnych od 0 i 1. Czasami zbiór liczb pierwszych oznacza się przez $\mathbb{P} = \{2, 3, 5, 7, ...\}$. Znane były od starożytności. Dzięki swoim bardzo praktycznym zastosowaniom w teorii szyfrowania (o czym piszemy w rozdziale 3.5) stanowią bardzo atrakcyjny przedmiot badań. Liczby naturalne, które można przedstawić jako iloczyn co najmniej dwóch liczb naturalnych (różnych od 0 i 1) nazywamy *liczbami złożonymi*.
Szczególnie ważny dla nas jest podany przez Euklidesa znany fakt, że zbiór liczb pierwszych jest nieskończony.
Rzeczywiście, przypuśćmy, że $\mathbb{P} = \{p_1, p_2, ..., p_n\}$. Oznaczałoby to, że każda liczba naturalna różna od 0 i 1 jest podzielna przez co najmniej jedną z liczb $p_1, p_2, ..., p_n$. Zdefiniujmy liczbę

$$a = p_1 p_2 \cdot ... \cdot p_n + 1$$

a jest liczbą naturalną większą od każdej z liczb $p_1, p_2, ..., p_n$, która nie jest podzielna przez żadną z nich, bowiem reszta z dzielenia a przez p_i jest równa 1. Udowodniliśmy w ten sposób fakt znany już Euklidesowi.

[1] Za znane przyjmujemy zbiory liczbowe i ich oznaczenia. Warto uczynić jednak wyjątek dla zbioru liczb naturalnych $\mathbb{N}$, ponieważ bywa on definiowany w różnych książkach rozmaicie. Tu przez liczby naturalne rozumieć będziemy liczby całkowite nieujemne, a więc $\mathbb{N} = \{0, 1, 2, 3, ...\}$.

Twierdzenie 1.1 (Twierdzenie Euklidesa.) *Zbiór liczb pierwszych jest nieskończony.* ■

Znacznie więcej na temat liczności zbioru liczb pierwszych mówi twierdzenie udowodnione przez Eulera[2] w 1748 roku. Twierdzenie to podajemy tu z dowodem Paula Erdősa[3] z 1938 roku. W [1] można znaleźć więcej rozważań na temat rozmieszczenia liczb pierwszych (por. także [7]). W dowodzie występuje oznaczenie $\lfloor a \rfloor$ na cechę liczby rzeczywistej a, zwaną także **podłogą** liczby . Tak więc $\lfloor a \rfloor = \max\{x \in \mathbb{R} : x \leq a\}$. Przez analogię mówimy, że $\lceil a \rceil = min\{x \in \mathbb{R} : x \geq a\}$ jest sufitem liczby rzeczywistej a.

Twierdzenie 1.2 (Euler 1738) *Szereg $\sum_{p \in \mathbb{P}} \frac{1}{p}$ jest rozbieżny.*

Dowód (nie wprost). Przypuśćmy, że $\mathbb{P} = \{p_1, p_2, ...\}$ $(p_1 < p_2 < ...)$ jest zbiorem wszystkich liczb pierwszych i szereg

$$\sum_{n=1}^{\infty} \frac{1}{p_n}$$

jest zbieżny.
Wtedy istnieje takie $k \in \mathbb{N}$, że

$$\sum_{n \geq k+1} \frac{1}{p_n} < \frac{1}{2}$$

Nazwijmy liczby pierwsze

$$p_1, p_2, ..., p_k$$

małymi liczbami pierwszymi zaś

$$p_{k+1}, p_{k+2}, ...$$

dużymi liczbami pierwszymi.
Dla każdego naturalnego N prawdziwa byłaby nierówność

$$\sum_{n \geq k+1} \frac{N}{p_i} < \frac{N}{2} \tag{1.1}$$

Dla dowolnego $N \in \mathbb{N}$ oznaczmy przez

N_d - liczbę tych $n \leq N$ $(n \in \mathbb{N})$, które mają co najmniej jeden *duży dzielnik pierwszy* (czyli dzielnik pierwszy w zbiorze $\{p_{k+1}, p_{k+2}, ...\}$).

[2] Leonard Euler, 1707-1783.

[3] Pál Erdős, 1913-1996. Wybitny matematyk węgierski, autor bądź współautor rekordowej liczby naukowych prac naukowych (ponad 1500) a także bohater niezliczonej liczby anegdot i oryginalnych poglądów na wiele spraw. Wygłaszał pogląd, że Bóg ma *Księgę*, w której są zapisane najpiękniejsze dowody twierdzeń matematycznych. Ten pogląd Erdősa podsunął Aignerowi i Zieglerowi pomysł napisania *Dowody z Księgi*, która ma zawierać, zdaniem autorów, dowody z *Księgi*, o której myślał Erdős. Jednym z nich jest prezentowany tu dowód twierdzenia 1.2.

N_m - liczbę tych $n \leq N$ ($n \in \mathbb{N}$), które mają tylko małe dzielniki pierwsze.

Oczywiście

$$N_d + N_m = N$$

Wykażemy jednak, że przypuszczając, że szereg $\sum_{p\in\mathbb{P}} \frac{1}{p}$ jest zbieżny otrzymamy ostrą nierówność $N_d + N_m < N$ i to właśnie będzie szukana sprzeczność, która zakończy dowód twierdzenia 1.2.

Zauważmy, że

$\lfloor \frac{N}{p_i} \rfloor$ jest liczbą tych liczb naturalnych, które są podzielne przez liczbę p_i i nie są większe od N.[4]

Stąd i z nierówności (1.1) wynika następujące oszacowanie liczby N_d:

$$N_d \leq \sum_{i\geq k+1} \lfloor \frac{N}{p_i} \rfloor < \frac{N}{2}$$

Niech $n \leq N$, $n \in N_m$ (tak więc tym razem przypuszczamy, że liczba n ma tylko małe dzielniki). Zapiszmy n w postaci

$$n = a_n b_n^2$$

gdzie a_n jest iloczynem różnych, czywiście małych, dzielników pierwszych liczby n. Czynnik a_n nazwiemy *częścią bezkwadratową*, zaś b_n^2 *częścią kwadratową*. Takich części bezkwadratowych może być co najwyżej 2^k, bowiem różnych małych dzielników jest k, każdy z nich w a_n może pojawić się co najwyżej jeden raz.
Prawdziwe są nierówności

$$b_n \leq \sqrt{n} \leq \sqrt{N}$$

z których wynika, że różnych części kwadratowych jest co najwyżej $\sqrt{N}$.
Stąd

$$N_m \leq 2^k \sqrt{N} \tag{1.2}$$

Wybierzmy $N = 2^{2k+2}$ (pamiętamy, że do tego momentu rozumowania N było dowolną liczbą naturalną, możemy ją więc ustalić w dowolny sposób). Wówczas

$$2^k \sqrt{N} \leq \frac{N}{2} \tag{1.3}$$

a więc (na podstawie nierówności (1.2) i (1.3))

$$N_m \leq 2^k \sqrt{N} \leq \frac{N}{2}$$

i wobec $N_d < \frac{N}{2}$ otrzymujemy $N_d + N_m < N$, co kończy dowód. ■

[4]Rzeczywiście, przypuśćmy, że $N = qp_i + r$, gdzie $0 \leq r < p_i$. Wówczas $\lfloor \frac{N}{p_i} \rfloor = q$. Z drugiej zaś strony, liczbami naturalnymi niewiększymi od N i podzielnymi przez p_i są $p_i, 2p_i, 3p_i, ..., qp_i$. A więc tych liczb jest dokładnie q.

Twierdzenie 1.2 mówi więcej o liczności zbioru liczb pierwszych niż twierdzenie 1.1. Zbiór liczb pierwszych jest oczywiście przeliczalny jako podzbiór zbioru liczb naturalnych, jest więc z nim równoliczny. Można na jego liczność spojrzeć jednak nieco inaczej.
Przyjrzyjmy się wpierw zbiorowi liczb naturalnych $\mathbb{N}$ i porównajmy go z (również przeliczalnym) zbiorem $X = \{n^2 : n \in \mathbb{N}\}$. Fakt, że szereg $\sum_{n\in\mathbb{N}} \frac{1}{n}$ jest rozbieżny, zaś szereg $\sum_{n\in\mathbb{N}} \frac{1}{n^2}$ jest zbieżny można interpretować tak, że w zbiorze X, który powstaje z $\mathbb{N}$ przez *wyrzucenie* z niego niektórych elementów pozostaje co prawda nieskończona ilość elementów, ale już na tyle niewiele, że ich nieskończona suma jest zbieżna. W tym sensie twierdzenie 1.2 można interpretować tak, że liczb pierwszych jest nie tylko nieskończenie wiele, ale *istotnie więcej* niż liczb zbioru X kwadratów liczb naturalnych.
Jak się okazuje jednak *luki* pomiędzy kolejnymi liczbami pierwszymi mogą być dowolnie duże. Rzeczywiście, prawdziwe następujące twierdzenie.

Twierdzenie 1.3 *Niech $k \in \mathbb{N}$ i niech $n_0 = 2 \cdot 3 \cdot 5 \cdot ... \cdot p$ będzie iloczynem wszystkich liczb pierwszych mniejszych od $k+2$. Wówczas liczby $n_0 + 2, n_0 + 3, ..., n_0 + (k+1)$ nie są liczbami pierwszymi.*

Dowód. Z definicji liczby n_0 wynika, że zarówno n_0 jak i dowolne i spełniające nierówności $2 \leq i \leq k+1$ są podzielne przez jedną z liczb pierwszych $2, 3, 5, ..., p$. ■
Na koniec rozważań o liczbach pierwszych dwa znane twierdzenia, których dowodów tutaj nie podamy. Pierwsze z nich znane jest jako Postulat Bertranda[5].

Twierdzenie 1.4 (Postulat Bertranda) *Dla dowolnego $n \in \mathbb{N}$ istnieje liczba pierwsza p spełniająca $n < p \leq 2n$.*

Chyba najdokładniej opisuje gęstość zbioru liczb pierwszych w zbiorze liczb naturalnych słynne twierdzenie znane jako Twierdzenie o Liczbach Pierwszych[6] udowodnione niezależnie przez Hadamarda[7] i Vallée de la Poussina[8]

Twierdzenie 1.5 (Twierdzenie o Liczbach Pierwszych)

$$\lim_{n\to\infty} \frac{|\{p \leq n : p \textit{ jest liczbą pierwszą }\}|}{\frac{n}{\ln n}} = 1$$

1.2 Algorytm Euklidesa

Poniższe **twierdzenie o dzieleniu liczb całkowitych** powinno być doskonale znane.

[5] Joseph Bertrand (1822-1900), matematyk francuski. Jego słynny postulat został w 1850 roku udowodniony przez P.L. Czebyszewa i później niezależnie przez Ramanujana. W [1] można znaleźć dowód Erdősa postulatu Bertranda.

[6] Rozkład liczb pierwszych w zbiorze liczb naturalnych fascynował najbardziej znanych matematyków. Wystarczy powiedzieć, że problemem asymptotycznego zachowania się liczności zbioru liczb pierwszych zajmowali się między innymi Legendre, Euler, Gauss i Dirichlet. W pewien sposób ukoronowaniem tych poszukiwań jest właśnie Twierdzenie o Liczbach Pierwszych.

[7] J.S. Hadamard (1865-1963).

[8] Ch. J. de la Vallée-Poussin (1866-1962).

Twierdzenie 1.6 (O dzieleniu liczb całkowitych.) *Dla dowolnych liczb całkowitych a i b, $b > 0$, istnieją jednoznacznie wyznaczone liczby $q, r \in \mathbf{Z}$ takie, że*

$$a = bq + r \tag{1.4}$$

przy czym $0 \leq r < b$.

Dowód. Zdefiniujmy liczbę q wzorem $q = \max\{q' \in \mathbb{Z} : bq' \leq a\}$. Łatwo zauważyć, że nasze q jest dobrze określone (to znaczy istnieje dla dowolnych a, b całkowitych takich, że $b > 0$).
Niech $r = a - bq$. Wykażemy, że tak zdefiniowane liczby całkowite q i r spełniają warunki twierdzenia.
Rzeczywiście, r jest nieujemne i równość (1.4) jest oczywista. Należy jednak sprawdzić, że $r < b$. Zauważmy, że gdyby $r \geq b$, wówczas prawdziwe byłyby związki

$$bq < b(q+1) = bq + b \leq bq + r = a$$

Tak więc $q+1$ spełniałoby $b(q+1) \leq a$, co sprzeczne jest ze sposobem wyboru q jako największej liczby całkowitej dla której $bq \leq a$.
Pozostaje udowodnić, że q i r spełniające tezę twierdzenia są jedyne. Przypuśćmy, że $a = bq_1 + r_1$, $a = bq_2 + r_2$, przy czym $0 \leq r_1, r_2 < b$. Wówczas prawdziwa byłaby równość

$$bq_1 + r_1 = bq_2 + r_2$$

a więc

$$b(q_2 - q_1) = r_1 - r_2$$

A więc $r_1 - r_2$ byłoby krotnością b. Ponieważ jednak $|r_1 - r_2| < b$, $r_1 - r_2$ jest równe zeru, a więc $r_1 = r_2$. Stąd otrzymujemy, że $b(q_2 - q_1) = 0$, co wobec założenia, że b jest dodatnie daje, że i $q_1 = q_2$. ■

Liczby q oraz r zdefiniowane wzorem w twierdzeniu 1.6 nazywamy, odpowiednio, **ilorazem** i **resztą** dzielenia a przez b.

Dla dowolnych liczb całkowitych a, b, które nie są równocześnie równe zeru, zbiór liczb naturalnych, które dzielą zarówno a jak i b jest skończony. Stąd istnieje największa liczba w tym zbiorze. Liczbę tę nazywamy **największym wspólnym dzielnikiem** a i b i oznaczamy przez NWD(a, b).

Wykażemy teraz istotną dla nas własność występujących w twierdzeniu 1.6 liczb a, b i r.

Fakt 1.7 NWD(a, b) = NWD(b, r).

Rzeczywiście, oznaczmy d = NWD(a, b) oraz c = NWD(b, r). Skoro d dzieli a oraz b, dzieli także r (najlepiej widać ten fakt po napisaniu wzoru (1.4) w postaci $r = a - bq$). Ponieważ zaś c jest największym wspólnym dzielnikiem b i r, d dzieli c. Równie łatwo dowodzimy, że $c|d$, skąd już natychmiast wynika fakt 1.7.

Algorytm Euklidesa

Niech $a, b \in \mathbb{Z}$, $a, b \neq 0$.
Tworzymy rekurencyjnie ciąg (r_n):
$r_0 = a, \quad r_1 = b$
$r_{n-1} = q_n r_n + r_{n+1}$, gdzie $0 \leq r_{n+1} < r_n$.
Zauważmy, że skoro dla każdego n dla którego $r_n > 0$ zachodzi $0 \leq r_{n+1} < r_n$, ciąg (r_n) jest skończony, istnieje takie $k > 1$, że r_k 0 oraz $r_{k+1} = 0$. Mamy więc ciąg k równości:

$$\begin{cases} r_0 = q_1 r_1 + r_2 & r_2 < r_1 \\ r_1 = q_2 r_2 + r_3 & r_3 < r_2 \\ \ldots & \\ r_{k-2} = q_{k-1} r_{k-1} + r_k & r_k < r_{k-1} \\ r_{k-1} = q_k r_k & \end{cases} \tag{1.5}$$

Na mocy faktu 1.7 mamy: $\mathrm{NWD(r_0, r_1)} = \mathrm{NWD(r_1, r_2)} = \ldots = \mathrm{NWD(r_{k-2}, r_{k-1})} = \mathrm{NWD(r_{k-1}, r_k)} = \mathrm{r_k}$. To oznacza, że prawdziwe jest następujące twierdzenie.

Twierdzenie 1.8 *Niech $a, b \in \mathbb{Z}$, $a, b \neq 0$. Istnieje takie k całkowite, że $r_k \neq 0$ oraz $r_{k+1} = 0$ (gdzie ciąg (r_n) jest wyznaczony przy pomocy algorytmu Euklidesa). Co więcej, mamy wówczas $r_k =$*$\mathrm{NWD}(a, b)$.

Oczywiście algorytm Euklidesa kończy się w liczbie kroków ograniczonej przez $|b|$ i w tym sensie jest to algorytm szybki, efektywny[9].

Twierdzenie 1.9 *Niech a i b będą liczbami całkowitymi, nie równymi równocześnie zero. Wówczas*

$$\mathrm{NWD(a, b)} = min\{d > 0 : d = ax + by, \quad x, y \in \mathbb{Z}\}$$

Dowód. Niech $A = \{d > 0 : d = \alpha a + \beta b, \alpha, \beta \in \mathbb{Z}\}$. Zauważmy, że $A \neq \emptyset$ oraz, że $\min A$ istnieje. Oznaczmy $d = \min A$. Oczywiście $d \in A$, a więc istnieją takie α i β, że $d = \alpha a + \beta b$. Wykażemy wpierw, że $d|a$. Rzeczywiście, przypuśćmy, że

$$a = qd + r$$

gdzie $d > r > 0$. Wówczas

$$0 < r = a - qd = a - q(\alpha a + \beta b) = a(1 - q\alpha) + b(-q\beta) < d$$

A to sprzeczne z definicją d jako najmniejszego elementu zbioru A[10].
W identyczny sposób dowodzimy, że $d|b$.

[9] Za algorytm *szybki* uważa się taki, który kończy działanie po czasie ograniczonym przez funkcję wielomianową *wielkości problemu*. W naszym przypadku rozsądnym jest przyjąć, że wielkość problemu, to $|b|$.

[10] A ma element najmniejszy (jak nie widzisz dlaczego, pomyśl nad uzasadnieniem, to nietrudne!), nie musimy się więc tu zajmować *subtelną* różnicą pomiędzy elementem najmniejszym a minimalnym elementem tego zbioru.

Załóżmy teraz, że pewna liczba całkowita c dzieli zarówno a jak b. Wówczas c dzieli $d = \alpha a + \beta b$, co kończy dowód faktu, że d jest największym wspólnym dzielnikiem a i b. ■

Korzystając ze ciągu związków (1.5) oraz faktu, że r_k jest największym wspólnym dzielnikiem a i b, można w inny sposób udowodnić twierdzenie 1.9. Co więcej, widać także, że algorytm Euklidesa pozwala efektywnie wyrazić NWD(a, b) jako liniową kombinację liczb a i b.

Jeśli NWD(a, b) = 1, wówczas mówimy, że a **i** b **są względnie pierwsze** i piszemy (a, b)= 1 lub $a \perp b$.

Wniosek 1.10 *Liczby całkowite a i b są względnie pierwsze wtedy i tylko wtedy gdy istnieją $\alpha, \beta \in \mathbb{Z}$ takie, że*

$$\alpha a + \beta b = 1$$

Co więcej, α i β dadzą się wyznaczyć przy pomocy algorytmu Euklidesa.

1.3 Zadania

Zadanie 1.1 Dla podanych liczb całkowitych a, b wskaż $q, r \in \mathbb{Z}$ takie, że $a = bq + r, 0 \leq r < b$.

1. $a = 17, b = 3$
2. $a = 3, b = 13$
3. $a = -34, b = 16$

Zadanie 1.2 Wykorzystując algorytm Euklidesa, dla podanych liczb całkowitych a, b znajdź $d = \mathrm{NWD(a, b)}$ oraz takie $\alpha, \beta \in \mathbb{Z}$, że $d = \alpha a + \beta b$.

1. $a = 246, b = 348$
2. $a = 105, b = 800$

Zadanie 1.3 Udowodnij, że jeśli $a, b, c \in \mathbb{N} - \{0\}$ i $c \equiv a \mod b$, wówczas $\mathrm{NWD(a, b)} = \mathrm{NWD(b, c)}$.
Wskazówka. Wykorzystaj definicję NWD *liczb całkowitych i fakt, że* $c = qb + a$ *dla pewnego* $q \in \mathbb{N}$.

Zadanie 1.4 Wskaż liczby a i b nieposiadające największego wspólnego dzielnika.

Zadanie 1.5 Zdefiniuj największy wspólny dzielnik $\mathrm{NWD(a, b, c)}$ trzech liczb całkowitych a, b i c.

- Czy jest prawdą, że $\mathrm{NWD(a, b, c)} = 1$ wtedy i tylko wtedy gdy każde dwie z liczb a, b i c są względnie pierwsze?
- Czy jest prawdą, że

$$\mathrm{NWD(a, b, c)} = \mathrm{NWD(a, NWD(b, c))}$$

- Udowodnij, że $d = \mathrm{NWD(a, b, c)}$ jest najmniejszą dodatnią liczbą całkowitą taką, że $d = \alpha a + \beta b + \gamma c$, gdzie $\alpha, \beta, \gamma \in \mathbb{Z}$.

Zadanie 1.6 Udowodnij, że dwie kolejne liczby całkowite są względnie pierwsze.

Rozdział 2

Grupy

Definicja 2.1 *Zbiór G z działaniem łącznym $*$, posiadającym element neutralny w G i taki, że każdy element w G ma element odwrotny nazywamy* **grupą**.
O grupie G mówimy, że jest **przemienna** *(lub* **abelowa***) jeśli działanie $*$ jest przemienne.*

Przykład 2.1 Z łatwością można sprawdzić, że poniższe stuktury są grupami.

S_X *(zbiór permutacji zbioru X z działaniem składania funkcji).*

$\mathbb{Z}$ *(zbiór liczb całkowitych),* $\mathbb{Q}$ *(zbiór liczb wymiernych),* $\mathbb{R}$ *(zbiór liczb rzeczywistych),* $\mathbb{C}$ *(zbiór liczb zespolonych) z działaniem dodawania.*

$\mathbb{Q}^+$ *(zbiór liczb wymiernych dodatnich) z działaniem mnożenia.*

$\mathbb{Z}_n$ *z działaniem dodawania modulo n.*

$\mathbb{Z}_5^* = \mathbb{Z}_5 - \{0\}$ *z działaniem mnożenia modulo* 5.

Najczęściej działania w grupach oznaczamy przez $+$ lub $\cdot$ czyli tak, jak dodawanie lub mnożenie liczb. O grupie, w której działanie jest oznaczone przez $+$ mówimy, że jest **grupą addytywną**, zaś o grupie, w której działanie jest oznaczone przez $\cdot$ mówimy, że jest **grupą multiplikatywną**[1]. Element neutralny w grupie oznaczany jest zwykle przez e lub e_G (jeśli grupa nazywa się G). Jeśli grupa jest multiplikatywna, wówczas element neutralny będzie także oznaczany przez 1 lub 1_G, zaś jeśli grupa jest addytywna przez 0 lub 0_G.

Powyżej zauważyliśmy, że zbiór $\mathbb{Z}_5^* = \mathbb{Z}_5 - \{0\}$ z działaniem mnożenia (a dokładniej: z działaniem indukowanym w $\mathbb{Z}_5$ przez mnożenie w zbiorze $\mathbb{Z}$) jest grupą. Równie łatwo jednak zauważyć, że $\mathbb{Z}_8 - \{0\}$ już grupą multiplikatywną nie jest. Rzeczywiście, w zbiorze $\{1, 2, 3, 4, 5, 6, 7\}$ reszt z dzielenia przez 8 zachodzi $2 \cdot 4 \equiv 0 \pmod 8$, a stąd łatwo wynika, że ani 2 ani 4 nie mają ze względu na mnożenie elementów odwrotnych.

[1] Słownik ortograficzny podaje jedynie pisownię *multiplikatywna* choć w przeszłości używano raczej pisowni *multyplikatywna*. Stąd w niniejszej książce mogą pojawić się obie pisownie.

Stąd pytanie: czy usuwając ze zbioru $\mathbb{Z}_8$ pewną liczbę elementów, można otrzymać grupę z działaniem mnożenia? Okazuje się, że tak. Co więcej, dla dowolnego $n \in \mathbb{N}$ znajdziemy maksymalny podzbiór $\mathbb{Z}_n^* \subset \mathbb{Z}_n$, który jest grupą multiplikatywną.

Twierdzenie 2.1 *Niech $n \in \mathbf{N}^*$ i niech $a \in \mathbf{Z}_n$. a jest elementem odwracalnym ze względu na działanie mnożenia w $\mathbf{Z}_n$ wtedy i tylko wtedy, gdy liczby a i n są względnie pierwsze.*

Przykład 2.2 $(\mathbf{Z}_{10}, \cdot)$ *oczywiście nie jest grupą (elementem neutralnym dla mnożenia jest* 1*, nie istnieje element odwrotny do elementu* 2*). Co więcej, także* $(\mathbf{Z}'_{10}, \cdot)$*, gdzie* $\mathbf{Z}' = \mathbf{Z} - \{0\}$*, nie jest grupą. Grupą przemienną natomiast jest* $(\mathbf{Z}^*_{10}, \cdot)$*, gdzie* $\mathbf{Z}^*_{10} = \{1, 3, 7, 9\}$.

Dowód twierdzenia 2.1. Przypuśćmy, że liczba całkowita a jest odwracalna w $\mathbb{Z}_n$.[2] Wówczas istnieje $b \in \mathbb{Z}$ takie, że $ba \equiv 1 \pmod{n}$, czyli $ba = 1 + kn$ dla pewnego k całkowitego. Wtedy $ba + (-k)n = 1$ i $a \perp n$ na mocy wniosku 1.10.
Jeśli $a \perp n$ wówczas, znowu na mocy wniosku 1.10, istnieją α i β całkowite takie, że $\alpha a + \beta n = 1$. Stąd zaś wynika, że $\alpha a \equiv 1 \pmod{n}$, czyli α jest elementem odwrotnym do a modulo n. ■

Definicja 2.2 *Niech $n \in \mathbf{N}$. Definiujemy*

$$\mathbf{Z}_n^* = \{a \in \mathbf{Z}_n : a \perp n\}.$$

Twierdzenie 2.2 *Niech $n \in \mathbf{N}$. Wówczas $(\mathbf{Z}_n^*, \cdot)$ jest grupą przemienną.*

Dowód. Wobec twierdzenia 2.1 oraz faktu, że istnienie elementu nautralnego dla mnożenia (to oczywiście 1) oraz łączność mnożenia są do sprawdzenia bardzo łatwe, sprawdzimy tylko, że mnożenie jest rzeczywiście działaniem zamkniętym w $\mathbb{Z}_n^*$.
Niech $a, b \in \mathbb{Z}_n^*$. Wiemy (znowu na mocy wniosku 1.10), że wówczas istnieją takie całkowite liczby s, t, u oraz v, że

$$sa + tn = 1$$

$$ub + vn = 1$$

Stąd

$$1 = (su)ab + n\alpha$$

gdzie $\alpha = tub + tvn + sav$. Z wniosku 1.10 wynika natychmiast, że $ab \perp n$ ■

W dalszym ciągu, za każdym razem gdy pisać będziemy $\mathbb{Z}_n$ myśleć będziemy o grupie $\mathbb{Z}_n$ z działaniem dodawania, natomiast przez $\mathbb{Z}_n^*$ rozumieć będziemy grupę $\mathbb{Z}_n^*$ z działaniem mnożenia. Tak więc powiemy, że elementem odwrotnym do 4 w $\mathbb{Z}_5^*$ jest 4, zaś w $\mathbb{Z}_5$ elementem odwrotnym do 4 jest 1.

[2] Oczywiście liczby całkowite nie są elementami $\mathbb{Z}_n$, natomiast są elementami $\mathbb{Z}_n$ ich klasy modulo n.

2.1 Funkcja φ Eulera

Większość przykładów grup, o których była do tej pory mowa a także będzie mowa w dalszym ciągu, to grupy o skończonej liczbie elementów. Takie grupy nazywamy *grupami skończonymi*. Liczbę elementów grupy skończonej nazywamy *rzędem grupy*. Rząd grupy G oznaczamy przez $|G|$.
Oczywiście rzędem grupy $\mathbb{Z}_n$ jest n. Grupy $\mathbb{Z}_5^*$, $\mathbb{Z}_8^*$ i $\mathbb{Z}_{10}^*$ są rzędu 4.

Niech $n \in \mathbf{N}$. Przez $\varphi(n)$ oznaczamy liczbę takich liczb naturalnych nie większych od n, które z n są względnie pierwsze. Można tę definicję zapisać wzorem

$$\varphi(n) = |\{k \in \mathbb{N} : k \leq n, k \perp n\}|$$

Funkcję $\varphi : \mathbf{N} \to \mathbf{N}$ tak zdefiniowaną nazywamy **funkcją Eulera**[3].

Następne twierdzenie wynika bezpośrednio z twierdzenia 2.2.

Twierdzenie 2.3 (O rzędzie $\mathbf{Z}_n^*$) *Dla każdej liczby naturalnej $n \geq 2$*

$$\varphi(n) = |\mathbf{Z}_n^*|.$$

Przykład 2.3 (Własności funkcji Eulera) *Niech p będzie liczbą pierwszą. Z łatwością można sprawdzić następujące związki.*

- $\varphi(p) = p - 1$,
- $\varphi(p^2) = p^2 - p$,
- $\varphi(p^n) = p^n - p^{n-1}$
- *Jeśli także q jest pierwsze, to* $\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$.

Zanim podamy i udowodnimy wzór na wartość $\varphi(n)$, wykażemy następujące twierdzenie.

Twierdzenie 2.4 (Formuła Sita[4] lub **Zasada Włączania i Wyłączania)** *Niech $A_1, A_2, ..., A_n$ będą zbiorami skończonymi. Wówczas zachodzi wzór*

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} (-1)^{k+1} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}| \tag{2.1}$$

Dowód. Przedstawimy indukcyjny dowód twierdzenia 2.4. Twierdzenie jest oczywiście prawdziwe dla $n = 1$, jednak w drugim kroku indukcyjnym będzie my korzystać z prawdziwości formuły sita dla $n = 2$ to znaczy z faktu

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| \tag{2.2}$$

[3]Leonard Euler 1707-1783.

[4]Dokładniej: "sita Eratostenesa". Eratostenes, (276-194 p.n.e) był kustoszem Biblioteki Aleksandryjskiej i jednym z największych umysłów starożytności. Sito Eratostenesa służyło do "odsiewania" liczb pierwszych od "plew" innych liczb (por. twierdzenie 2.5 i wniosek 2.6). Innym osiągnięciem Eratostenesa była próba zmierzenia promienia Ziemi przez porównanie długości cieni rzucanych w południe przez dwie tyczki: jednej ustawionej w Aleksandrii, drugiej zaś w Syene (dzisiejszy Asuan). Wynik jaki otrzymał różnił sie tylko o 1% od nam znanego.

Rzeczywiście, w sumie $|A_1| + |A_2|$ elemanty zbioru $A_1 \cap A_2$ liczone są dwukrotnie i stąd wynika wzór (2.2).
Przypuśćmy, że wzór (2.6) jest prawdziwy dla pewnego $n \geq 2$. Wykażemy, że jest prawdziwy dla liczności sumy $n+1$ zbiorów czyli, że

$$|A_1 \cup A_2 \cup ... \cup A_n \cup A_{n+1}| = \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n+1} (-1)^{k+1} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}| \quad (2.3)$$

Na mocy (2.2)

$$|A_1 \cup A_2 \cap ... \cup A_n \cup A_{n+1}| = |(A_1 \cup A_2 \cup ... \cup A_n) \cup A_{n+1}| =$$
$$= |A_1 \cup A_2 \cup ... \cup A_n| + |A_{n+1}| - |(A_1 \cup A_2 \cup ... \cup A_n) \cap A_{n+1}|$$
$$= |A_1 \cup A_2 \cup ... \cup A_n| + |A_{n+1}| - |(A_1 \cap A_{n+1}) \cup ... \cup (A_n \cap A_{n+1})|$$

Stosując teraz formułę sita dla sumy n zbiorów (dwukrotnie: do $|A_1 \cup A_2 \cup ... \cup A_n|$ i do $|(A_1 \cap A_{n+1}) \cup ... \cup (A_n \cap A_{n+1})|$) otrzymujemy

$$|A_1 \cup A_2 \cap ... \cup A_n \cup A_{n+1}| =$$
$$= \sum_{1 \leq i_1 < ... < i_n \leq n} (-1)^{k+1} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}| +$$
$$+ |A_{n+1}| - \sum_{1 \leq j_1 < ... < j_k \leq n} (-1)^{k+1} |A_{j_1} \cap ... \cap A_{j_k} \cap A_{n+1}|$$

Zauważmy teraz, że w składniku $\sum_{1 \leq i_1 < ... < i_n \leq n} (-1)^{k+1} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}|$ występują wszystkie tę składniki prawej strony wzoru (2.3), w których nie występuje zbiór A_{n+1}, zaś składnik

$$|A_{n+1}| - \sum_{1 \leq j_1 < ... < j_k \leq n} (-1)^{k+1} |A_{j_1} \cap ... \cap A_{j_k} \cap A_{n+1}|$$

to suma wszsytkich składników wzoru (2.3), w których A_{n+1} jest jednym z czynników iloczynu zbiorów. Co więcej

$$- \sum_{1 \leq j_1 < ... < j_k \leq n} (-1)^{k+1} |A_{j_1} \cap ... \cap A_{j_k} \cap A_{n+1}| = \sum_{1 \leq j_1 < ... < j_k \leq n} (-1)^{k+2} |A_{j_1} \cap ... \cap A_{j_k} \cap A_{n+1}|$$

a więc przed każdym składnikiem postaci $|A_{j_1} \cap ... \cap A_{j_k} \cap A_{n+1}|$ pojawia się znak równy -1 do potęgi równej *liczba zbiorów* $+1$. ■

Tak jak to zapowiedzieliśmy, twierdzenie 2.4 pozwoli nam udowodnić wzór na wartości funkcji Eulera dla dowolnych liczb naturalnych.

Twierdzenie 2.5 *Niech $n = p_1 ... p_t$, gdzie p_i są różnymi liczbami pierwszymi dla $i = 1, ..., t$. Wówczas*

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - ... \frac{n}{p_t} + \frac{n}{p_1 p_2} + ... + \frac{n}{p_{t-1} p_t} - \frac{n}{p_1 p_2 p_3} - ... - \frac{n}{p_{t-2} p_{t-1} p_t} + ... + \frac{(-1)^t n}{p_1 p_2 ... p_t}$$
$$= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_t}\right)$$

Dowód. Chwila refleksji wystarczy, żeby zrozumieć dlaczego zachodzi wzór

$$n - \frac{n}{p_1} - \frac{n}{p_2} - ... \frac{n}{p_t} + \frac{n}{p_1 p_2} + ... + \frac{n}{p_{t-1} p_t} - \frac{n}{p_1 p_2 p_3} - ... - \frac{n}{p_{t-2} p_{t-1} p_t} + ... + \frac{(-1)^t n}{p_1 p_2 ... p_t}$$

$$= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_t}\right)$$

(każdy składnik postaci $\frac{1}{p_{i_1} ... p_{i_k}}$ bierze się z wyboru $\frac{1}{p_{i_1}}, ..., \frac{1}{p_{i_k}}$ i $n - k$ jedynek w nawiasach po prawej stronie równości).
Pozostaje więc wykazać, że

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - ... \frac{n}{p_t} + \frac{n}{p_1 p_2} + ... + \frac{n}{p_{t-1} p_t} - \frac{n}{p_1 p_2 p_3} - ... - \frac{n}{p_{t-2} p_{t-1} p_t} + ... \pm \frac{(-1)^t n}{p_1 p_2 ... p_t}$$

Dla dowolnego $i = 1, 2, ..., t$ oznaczmy teraz przez A_i zbiór tych liczb naturalnych niewiększych od n, które są podzielne przez p_i. Zbiór liczb niewiększych od n i względnie pierwszych z n jest równy

$$\Phi(n) = \{1, 2, ..., n\} - \bigcup_{i=1,...,t} A_i$$

Łatwo zaobserwować, że

$$|A_{j_1} \cap A_{j_2} \cap ... \cap A_{j_l}| = \frac{n}{p_{j_1} ... p_{j_l}}$$

Stąd zaś i z formuły sita (twierdzenie 2.4) nasze twierdzenie wynika już bardzo łatwo:

$$\varphi(n) = |\Phi(n)| = n - |\bigcup_{i=1,...,t} A_i| = n + \sum_{1 \le j_1 < ... < j_k \le t} (-1)^k \frac{n}{p_{j_1} ... p_{j_k}}$$

■

Przykład 2.4 $\varphi(42) = \varphi(2 \cdot 3 \cdot 7) = 12$

Dobrym ćwiczeniem i sprawdzianem zrozumienia dowodu twierdzenia 2.5 będzie dla czytelnika samodzielne udowodnienie poniższego wniosku (dowód jest dokładnie taki sam jak powyższy).

Wniosek 2.6 *Wzór na φ z twierdzenia 2.6 pozostaje identyczny jeśli położymy $n = p_1^{a_1} \cdot ... \cdot p_t^{a_t}$ gdzie $p_1 < ... < p_t$ są liczbami pierwszymi, $a_1, ..., a_t \in \mathbb{N} - \{0\}$.*

2.2 Podgrupy

Niech $(G; *)$ będzie grupą, $H \subset G$. Jeśli $(H; *)$ (a dokładniej: $(H, *|_{H \times H})$) jest grupą, wówczas mówimy, że H jest podgrupą grupy G. Piszemy wtedy $H \le G$.

Jeśli w pewnej grupie G zbiór H jest podgrupą, to $H \neq \emptyset$, bowiem do H należy wtedy element neutralny e. Co więcej, dla dowolnych $a, b \in H$ mamy $a * b^{-1} \in H$.
Z drugiej strony, jeśli H jest niepustym podzbiorem grupy G takim, że dla dowolnych $a, b \in H$ spełniony jest warunek

$$a * b^{-1} \in H \tag{2.4}$$

wówczas spełnione są w H warunki grupy dla działania $*$. Rzeczywiście.

- $e \in H$. Skoro $H \neq \emptyset$, istnieje pewien element $c \in H$. Z warunku (2.4) dla $c = a = b$ otrzymujemy $c * c^{-1} = e \in H$.
- Dla dowolnego $c \in H$, biorąc w (2.4) $a = e, b = c$ mamy $a*b = e*c^{-1} = c^{-1} \in H$, a więc dla każdego elementu należącego do H także element do niego odwrotny należy do H.
- Dla dowolnych elementów $c, d \in H$ wstawiając $a = c$ oraz $b = d^{-1}$ we wzorze (2.4) otrzymamy $c * d \in H$. Tak więc działanie $*$ jest w H zamknięte.
- Działanie $*$ w H jest łączne, bo jest łączne w nadzbiorze G zbioru H.

Udowodniliśmy w ten sposób następujący, wygodny warunek konieczny i wystarczający by podzbiór grupy był podgrupą.

Twierdzenie 2.7 *Niech G będzie grupą z działaniem $*$. Niepusty podzbiór H zbioru G jest podgrupą wtedy i tylko wtedy, gdy dla dowolnych elementów $a, b \in H$ zachodzi $a * b^{-1} \in H$.* ■

Przykład 2.5 Można sprawdzić, że zbiór D'_n wszystkich izometrii n-kąta foremnego z działaniem składania jest grupą. Każda z tych izometrii jest albo obrotem o krotność kąta $\frac{2\pi}{n}$ albo symetrią względem osi zawierającej środek n-kąta. Zbiór wszystkich n obrotów, oznaczany przez O_n jest podgrupą grupy D_n. Elementy podgrupy O_n nazywane są *izometriami właściwymi* (por. podrozdział 2.7).

2.3 Homorfizmy grup, grupy izomorficzne

Funkcja $h : G_1 \to G_2$ jest *homomorfizmem* grupy $(G_1, *)$ w grupę $(G_2, \circ)$ jeśli $h(x * y) = h(x) \circ h(y)$ dla dowolnych $x, y \in G_1$.
Homomorfizm h jest:

- **monomorfizmem**, jeśli h jest injekcją,
- **epimorfizmem**, jeśli h jest surjekcją,
- **izomorfizmem**, jeśli h jest bijekcją.

W tym ostatnim przypadku mówimy, że grupy G i H są **izomorficzne**.

Grupy izomorficzne będziemy, w pewnym sensie, identyfikowali. Algebraiczne własności grup izomorficznych są bowiem identyczne. Bierze się to stąd, że wyniki działania w grupie G_1 przenoszą się, przez izomorfizm właśnie, na wyniki działania w grupie G_2 (i na odwrót, przez izomorfizm odwrotny). Dla przykładu, jeśli w grupie G_1 elementem odwrotnym do a jest element b wówczas, jak łatwo sprawdzić, elementem odwronym do $h(a)$ jest $h(b)$.

Przykład 2.6 *Przyjrzyjmy się następującym przykładom grup o czterech elementach (tabele, w których przedstawione są działania w tych grupach nazywane są* tabelami Cayleya[5]*).*

$(\mathbb{Z}_4, +)$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

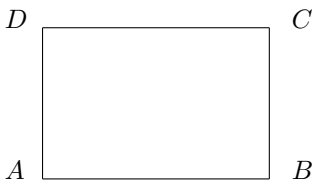
$(\mathbb{Z}_5^*, \cdot)$. $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(\mathbb{Z}_8^*, \cdot)$. *Oczywiście* $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$.

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Grupa Kleina. *To grupa izometrii prostokąta* $ABCD$.[6]



[5] Arthur Cayley, 1821-1895.
[6] Felix Klein, 1849-1925.

W grupie tej są cztery elementy:

Identyczność: e.

Obrót o π*, czyli permutacja:* $\sigma = (A, C)(B, D)$.

Symetria względem osi pionowej: $\tau = (A, B)(C, D)$.

Symetria względem osi poziomej: $\rho = (A, D)(B, C)$

$\circ$	e	σ	τ	ρ
e	e	σ	τ	ρ
σ	σ	e	ρ	τ
τ	τ	ρ	e	σ
ρ	ρ	τ	σ	e

Z łatwością można sprawdzić, że $h : \mathbb{Z}_4 \to \mathbb{Z}_5^*$ zdefiniowane równościami: $h(0) = 1, h(1) = 2, h(2) = 4$ i $h(3) = 3$ jest izomorfizmem grupy $\mathbb{Z}_4$ na $\mathbb{Z}_5^*$.
Nie trudniej wykazać, że grupy Kleina i $\mathbb{Z}_8^*$ są izomorficzne, natomiast grupy $\mathbb{Z}_5^*$ i $\mathbb{Z}_8^*$ izomorficzne nie są.

Działania w grupach $\mathbb{Z}_4$ i $\mathbb{Z}_5^*$ mają identyczne własności, podobnie jak działania w grupie $\mathbb{Z}_8$ i grupie Kleina. Dla przykładu, skoro w $\mathbb{Z}_8^*$ każdy element jest do siebie odwrotny i grupa ta jest izomorficzna z grupą Kleina, także w grupie Kleina każdy element jest swoją odwrotnością.

2.4 Grupy cykliczne

Dla dowolnego elementu g multyplikatywnej grupy G i liczby całkowitej n można zdefiniować *n-tą potęgę elementu* g, w następujący sposób.

$g^0 = e$ (gdzie e jest elementem neutralnym grupy G),

$g^{n+1} = g^n \cdot g$, jeśli n jest nieujemne,

$g^n = (g^{-1})^{-n}$, jeśli $n < 0$.

Oczywiście dla dowolnego n całkowitego g^n jest także elementem grupy G.
Potęgom w grupach multyplikatywnych odpowiadają *krotności* w grupach addytywnych. Niech H będzie grupą addytywną, $a \in H$, $n \in \mathbb{Z}$.

$0a = 0$ (przez 0 z lewej strony równości rozumiemy tu liczbę 0, zaś po prawej stronie równości tak samo pisane 0 oznacza element neutralny grupy H),

$(n + 1)a = na + a$ dla n dodatnich,

$na = (-n)(-a)$ dla n ujemnych.

Wszystkie własności grup multyplikatywnych mają w tym kontekście swoje odpowiedniki dla notacji addytywnej.

Definicja 2.3 (Rząd elementu grupy) *Najmniejszą dodatnią liczbę całkowitą n taką, że*

$$g^n = e \tag{2.5}$$

nazywamy **rzędem** *elementu g grupy, jeśli n (całkowite dodatnie) spełniające (2.5) nie istnieje, wówczas mówimy, że rzędem g jest ∞.*
Rząd elementu g oznaczamy przez $|g|$.

Twierdzenie 2.8 *Jeśli grupa G jest skończona, $g \in G$, wówczas rząd elementu g jest skończony.*

Dowód. Rozważmy ciąg (nieskończony)

$$e = g^0, g^1, g^2, g^3, ...$$

Skoro zbiór G ma skończoną liczbę elementów, w ciągu tym pewne elementy muszą się powtarzać, to znaczy istnieją $k, n \in \mathbb{N}$ takie, że

$$g^k = g^n \tag{2.6}$$

dla $k \neq n$. Załóżmy, że $0 \leq k < n$ i na dodatek, że n jest najmniejszą liczbą naturalną. dla której spełniony jest związek (2.6), przy czym $0 \leq k < n$. Mnożąc obie strony (2.6) przez g^{-1} otrzymujemy

$$g^{k-1} = g^{n-1}$$

To stoi w sprzeczności z wyborem n jako najmniejszej liczby naturalnej, dla której zachodzi równość postaci (2.6) chyba, że $k = 0$. Wtedy jednak mamy $g^0 = g^n$ co oznacza, że n jest poszukiwanym rzędem elementu g. ■

Twierdzenie 2.9 *Jeśli w grupie skończonej G zbiór $S \neq \emptyset$ jest zamknięty ze względu na działanie grupowe $(*)$, to S stanowi podgrupę G.*

Dowód. Przypuśćmy, że podzbiór $S \subset G$ jest zamknięty ze względu na działanie $*$. Oczywiście wystarczy wykazać, że element neutralny w G, powiedzmy e, należy do S a także, że dla dowolnego $a \in S$ element a^{-1} także jest elementem zbioru S. Na mocy twierdzenia 2.8 istnieje taka liczba naturalna n, że $a^n = e$. Stąd oczywiście $e \in S$ (zauważmy, że skoro zbiór S jest niepusty, jakiś element a do S należy, a więc do S należy także e). Co więcej, mamy $e = a^n = a^{n-1} * a = a * a^{n-1}$, a więc element a^{n-1} jest odwrotny do a i to należy do zbioru S. ■

Definicja 2.4 (Generator grupy, grupa cykliczna) *Mówimy, że element g jest* **generatorem** *grupy G z działaniem $*$, jeżeli każdy element grupy G można otrzymać jako wynik działania $*$ na elementach g i g^{-1}.*
Jeśli grupa zawiera generator g, to nazywamy ją cykliczną i piszemy $G =< g >$.

Przykład 2.7 1 *(a także* -1*) jest generatorem grupy* $\mathbf{Z}$ *(addytywnej grupy liczb całkowitych).*
2 *jest generatorem (multyplikatywnej) grupy* $\mathbf{Z}_5^*$.
Łatwo się przekonać, że ani grupa addytywna $\mathbb{Q}$*, ani grupa multyplikatywna* $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ *nie jest cykliczna.*
Grupa $(\mathbf{Z}_4, +)$ *jest cykliczna, grupa Kleina nie.*
$\mathbb{Z}_5^* =< 2 >$.

Twierdzenie 2.10 *Jeżeli* G *jest multyplikatywną grupą skończoną,* $g \in G$*, wówczas istnieje* $n \in \mathbf{N}$ *takie, że* $g^n = g^{-1}$

Dowód. Na mocy twierdzenia 2.8 g ma rząd skończony, a więc istnieje $k \in \mathbb{N}$ takie, że $g^k = e$. Stąd wynika, że $g^{k-1} \cdot g = g \cdot g^{k-1} = e$, a więc, że $g^{-1} = g^{k-1}$ (gdzie k jest rzędem elementu g). ■

Twierdzenie 2.11 *Każda grupa cykliczna jest przemienna.*

Dowód. Rzeczywiście, przypuśćmy, że $a, b \in G$, gdzie G jest grupą cykliczną, generowaną przez element $g \in G$. Wówczas istnieją takie $k, l \in \mathbb{Z}$, że $a = g^k, b = g^l$. Wobec tego

$$ab = g^k g^l = g^{k+l} = g^{l+k} = g^l g^k = ba$$

■

Twierdzenie 2.12 *Każda skończona grupa cykliczna* G *jest izomorficzna z* $(\mathbf{Z}_n, +)$*, gdzie* n *jest rzędem grupy* G*.* [7]

Dowód. Czytelnikowi pozostawiony jest nietrudny dowód faktu, że jeśli grupa multyplikatywna G rzędu n jest cykliczna, zaś $g \in G$ jest jej generatorem, wówczas funkcja $F : G \ni g^k \to k \in \mathbb{Z}_n$ jest izomorfizmem grup G i $\mathbb{Z}_n$. ■

18.10.2011

Podobnie jak, z dokładnością do izomorfizmu, $\mathbb{Z}_n$ jest jedyną grupą cykliczną rzędu n, tak grupa addytywna $\mathbb{Z}$ jest jedyną, z dokładnością do izomorfizmu, grupą cykliczną nieskończoną.

Twierdzenie 2.13 *Każda nieskończona grupa cykliczna jest izomorficzna z* $(\mathbf{Z}; +)$.

Dowód. Rzeczywiście, niech $a \in G$ będzie generatorem grupy nieskończonej G. Wówczas dla dowolnych całkowitych k, m, $k \neq m$ zachodzi $a^k \neq a^m$ (łatwo widać, że w przeciwnym przypadku zbiór G byłby skończony). Funkcja $f : G \ni a^n \to n \in \mathbb{Z}$ jest, jak łatwo sprawdzić, izomorfizmem grupy (multyplikatywnej) G na grupę $\mathbb{Z}$. ■

Oczywiście stąd wynika, że każda grupa cykliczna jest przeliczalna, choć jest to dość oczywiste także bez odwoływania się do twierdzenia 2.13.

[7] Inaczej: jedyną, z dokładnością do izomorfizmu, grupą skończoną o n elementach jest $(\mathbf{Z}_n, +)$.

Twierdzenie 2.14 *Każda podgrupa grupy cyklicznej jest cykliczna.*

Dowód. Przypuśćmy, że G jest grupą multyplikatywną, w której g jest generatorem i niech H będzie podgrupą grupy G. Jeśli H jest podgrupą trywialną, $H =< 1 >$, wówczas H jest generowana przez element neutralny 1. Przypuśćmy więc, że w H poza elementem neutralnym (jedynką) istnieją inne elementy. Skoro G jest grupą generowaną przez g, zaś $H \subset G$, wszystkie elementy H są postaci $h = g^k, k \in \mathbb{Z}$. Załóżmy teraz, że k_0 jest najmniejszą liczbą całkowitą dodatnią taką, że $g^{k_0} \in H$, a więc

$$k_0 = \min\{k \in \mathbb{Z}^+ : g^k \in H\} \tag{2.7}$$

Niech g^m będzie dowolnym elementem podgrupy H. Wykażemy, że $g^m = (g^{k_0})^l$ dla pewnego l całkowitego. Inaczej mówiąc udowodnimy, że m jest krotnością k_0. Rzeczywiście, przypuśćmy, że tak nie jest. Wówczas $m = qk_0 + r, q, r \in \mathbb{Z}, 0 < r < k_0$. Mamy

$$g^r = g^{m-qk_0} = g^m \cdot g^{-qk_0} = g^m (g^{k_0})^{-q} \tag{2.8}$$

Wiemy, że $g^m \in H$ oraz $g^{k_0} \in H$. Wobec tego $(g^{k_0})^{-q} \in H$, $g^m \cdot (g^{k_0})^{-q} \in H$ i na mocy (2.8) mamy $g^r \in H$. To jednak jest sprzeczne z założeniem (definicja k_0 dana wzorem 2.7), że k_0 jest najmniejszą liczbą całkowitą dodatnią taką, że $g^{k_0} \in H$. Ta sprzeczność kończy dowód twierdzenia 2.14. ■

2.5 Twierdzenie Cayleya

Okazuje się, że tak jak dla grup cyklicznych wskazaliśmy powyżej bardzo dobrze nam znane modele, tak i dla dowolnych grup, niekoniecznie cyklicznych, także można wskazać uniwersalny model.

Definicja 2.5 (Grupa transformacji) *Dowolną podgrupę grupy permutacji $S(X)$ nazywamy* grupą transformacji.

Twierdzenie 2.15 (Tw. Cayleya) *Dowolna grupa jest izomorficzna z pewną grupą tranformacji.*

Dowód. Niech $(G, *)$ będzie dowolną grupą. Dla dowolnego $a \in G$ rozważmy następujące odwzorowanie f_a:

$$G \ni x \to f_a(x) = a * x \in G$$

f_a jest permutacją zbioru G, bowiem z równości $f_a(x) = f_a(y)$ wynika $a * x = a * y$ a stąd, po wymnożeniu lewostronnie przez a^{-1}, otrzymujemy $x = y$, a więc f_a jest injekcją. Jest także surjekcją, bo równanie $a*x = y$ ma dla każdego $y \in G$ rozwiązanie (równe $a^{-1}y$).
Niech teraz T będzie zbiorem wszystkich tak zdefiniowanych funkcji.

$$T = \{f_a : a \in G\}$$

Z łatwością można sprawdzić, że

$$f_a \circ f_b = f_{a*b} \tag{2.9}$$

dla dowolnych $a, b \in G$.
Jak widzieliśmy powyżej, T jest pewnym zbiorem permutacji zbioru G. Wykażemy, że T jest podgrupą grupy $S(G)$ wszystkich permutaci zbioru G (to będzie poszukiwana grupa transformacji izomorficzna z G).
Oczywiście T jest podzbiorem niepustym (bo G jako grupa jest zbiorem niepustym). Niech $f_a, f_b \in T$, gdzie $a, b \in G$. Zauważny, że $f_a \circ f_b^{-1} = f_{a*b^{-1}} \in T$ i T jest podgrupą na mocy twierdzenia 2.7. Stąd i ze wzoru (2.9) oczywiście wynika, że przyporządkowanie

$$\mathcal{C} : G \ni a \to f_a \in T$$

jest homomorfizmem grup.
$\mathcal{C}$ jest injekcją ($\mathcal{C}(a) = \mathcal{C}(b) \Rightarrow f_a(x) = f_b(x)$, czyli $a * x = b * x$ dla każdego $x \in G$, w szczególności dla $x = e$ otrzymujemy $a = b$) oraz surjekcją (z definicji zbioru T), a więc izomorfizmem. ■

Przykład 2.8 Jak już widzieliśmy, grupa Kleina jest izomorficzna z podgrupą grupy $S(\{A, B, C, D\})$ składającą się z następujących permutacji:

$$id_{\{A,B,C,D\}}; (A, C)(B, D); (A, B)(C, D); (A, D)(B, C)$$

2.6 Twierdzenie Lagrange'a

Przyjrzyjmy się przykładowi grupy $\mathbb{Z}_{25}^*$. Korzystając z twierdzenia 2.5 z łatwością można sprawdzić, że rząd tej grupy jest równy 20. Przykładami podgrup $\mathbb{Z}_{25}^*$ są $H_1 = \{1, 7, 18, 24\}$, $H_2 = \{1, 6, 11, 16, 21\}$ i $H_3 = \{1, 24\}$. Rzędy tych podgrup to, odpowiednio, 4, 5 i 2, a więc podzielniki rzędu grupy $\mathbb{Z}_{25}^*$.

Twierdzenie 2.16 (Lagrange'a) *Niech H będzie podgrupą grupy skończonej G, $a = |H|, b = |G|$. Wówczas $a|b$.*

Dowód twierdzenia Lagrange'a wynika z kilku lematów, które przedstawiamy poniżej. Wpierw jednak użyteczna definicja.

Definicja 2.6 (Przystawanie modulo półgrupa) *Niech H będzie podgrupą grupy G, $a, b \in G$. Mówimy, że a* przystaje do b modulo H *(piszemy $a \equiv b \ (mod\ H)$) jeżeli $ab^{-1} \in H$.*

Lemat 2.17 *Jeżeli H jest podgrupą G wówczas relacja przystawania modulo H jest w G relacją równoważności.*

Dowód lematu 2.17 pozostawiony jest do samodzielnego wykonania jako zadanie 2.11. ■

Lemat 2.18 *Niech G będzie dowolną grupą, zaś H jej podgrupą. Wówczas klasą elementu neutralnego grupy G modulo H jest zbiór H.*

Dowód. Rzeczywiście, jeśli przez $[g]_H$ oznaczymy klasę elementu g grupy G modulo H, wówczas

$$[e]_H = \{h \in G : h \equiv e \ (mod\ H)\} = \{h \in G : g * e^{-1} \in H\} = \{g \in G : g \in H\} = H$$

■

Warto zwrócić uwagę na lemat następny, bowiem będziemy z niego wielokrotnie korzystać w przyszłości.

Lemat 2.19 *Niech G będzie dowolną grupą, zaś H jej podgrupą. Wówczas klasą elementu $g \in G$ modulo H jest zbiór $Hg = \{hg | h \in H\}$.*

Dowód.

$$[g]_H = \{h \in G : h * g^{-1} \in H\} = \{h \in G | h \in Hg\} = Hg$$

(warto zadać sobie trud dokładnego sprawdzenia, czy dobrze rozumiemy ten bardzo krótki dowód). ■

Klasa równoważności Ha dla relacji przystawania modulo podgrupa H nazywamy **warstwami modulo** H lub prawostronnymi klasami przystawania modulo H.

Lemat 2.20 *Niech G będzie dowolną grupą, zaś H jej podgrupą, $a \in G$. Wówczas klasa Ha jest równoliczna z H.*

Dowód. Oczywiście dla dowolnego $h \in H$ mamy $h * a \in Ha$. Zdefiniujmy funkcję

$$F : H \ni h \to h * a \in Ha$$

Wystarczy teraz wykazać, że funkcja F jest bijekcją.

- Jeśli $F(h) = F(h')$ wówczas $h * a = h' * a$. Stąd wynika, że $h = h'$ a więc F jest injekcją.
- Niech $g \in Ha$. Wówczas $g = h * a$, gdzie h jest pewnym elementem H. To zaś oznacza, że $F(h) = g$, udowodnlśmy więc, że F jest surjekcją. ■

Dowód twierdzenia Lagrange'a. Wiemy, że jeśli mamy w zbiorze zdefiniowaną relację równoważnościową, wówczas klasy równoważności względem tej relacji tworzą podział zbioru, to znaczy są parami rozłączne i ich suma daje cały zbiór. W naszym przypadku wiemy dodatkowo, że klasy te są równoliczne (każda z nich ma liczność klasy elementu neutralnego, czyli zbioru H). Możemy więc napisać

$$|G| = |H| \cdot (\text{liczba klas równoważności}) \tag{2.10}$$

Stąd natychmiast wynika, że rząd $|H|$ podgrupy H dzieli rząd $|G|$ grupy G. ■

Liczba klas równoważności względem relacji przystawania modulo podgrupa jest parametrem zwanym *indeksem podgrupy* H w grupie G. Oznaczamy ten parametr przez $\mathrm{Ind}_G(H)$. Wzór (2.10) przyjmie wtedy postać

$$|G| = |H| \cdot \mathrm{Ind}_G(H) \tag{2.11}$$

2.6.1 Wnioski z twierdzenia Lagrange'a

Zbiór wszystkich prawostronnych warstw grupy G modulo podgrupa H oznacza się często przez $G : H$ lub przez G/H, mamy więc

$$G : H = \{Ha : a \in G\}$$

Wzór (2.10), który wykazaliśmy dowodząc twierdzenia Lagrange'a możemy zapisać w postaci następującego wniosku.

Wniosek 2.21 *Jeżeli H jest podgrupą grupy skończonej G, wówczas*

$$|G : H| = \frac{|G|}{|H|}$$

■

Wiemy już, że każdy element g grupy skończonej generuje podgrupę o elementach

$$g^0 = e, g^1 = g, g^2, ..., g^{k-1}$$

której rząd k jest równy rzędowi tego elementu. Stąd natychmiastowy wniosek.

Wniosek 2.22 *Każdy element grupy skończonej G ma rząd będący dzielnikiem rzędu grupy G.*

Jeśli grupa skończona G ma rząd, który jest liczbą pierwszą, wówczas na mocy twierdzenia Lagrange'a ma tylko dwie podgrupy: G i podgrupę której jedynym elementem jest jej element neutralny.

Wniosek 2.23 *Jeśli rząd grupy G jest liczbą pierwszą, to G jest cykliczna. Co więcej, każdy element grupy G, który nie jest elementem neutralnym, jest jej generatorem.*

Wniosek 2.24 *Jedynymi, z dokładnością do izomorfizmu, grupami grupami rzędu* 4 *są $\mathbf{Z}_4$ i grupa Kleina.*

Dowód. Niech G będzie grupą rzędu 4. Jeśli w G jest cykliczna wówczas, na mocy wniosku 2.12, G jest izomorficzna z $\mathbb{Z}_4$. Przypuśćmy więc, że G grupą cykliczną nie jest. Wtedy każdy element grupy, który nie jest elementem neutralnym jest, na mocy

wniosku 2.22 rzędu 2. Co więcej, jeśli oznaczymy przez e, a, b, c wszystkie elementy grupy G, przy czym e oznacza element neutralny wówczas $a \cdot b = c$ - iloczyn[8] dwóch elementów (a i b) różnych od elementu neutralnego jest równy trzeciemu elementowi (oznaczyliśmy go przez c). Rzeczywiście, gdyby $a \cdot b = a$ wówczas powymnożeniu tej równości z lewes strony przez a^{-1} otrzymalibyśmy $b = e$ a to sprzeczne z założeniem, że $b \neq e$. Teraz już niemal oczywistym jest, że G jest izomorficzna z grupą Kleina. ■

Jeszcze łatwiej niż wniosek 2.24 można udowodnić, że jedynymi grupami k elementowymi dla $k = 1, 2, 3$ są $\mathbb{Z}_k$. Stąd i z wniosku 2.24 wynika, że wszystkie grupy rzędu co najwyżej 4 są przemienne.

Podobnie jak zdefiniowaliśmy relację przystawania modulo podgrupa H (zależnością $a \equiv b \Leftrightarrow ab^{-1} \in H$), można zdefiniować relację *lewostronnego przystawania modulo podgrupa* H zależnością $aL_Hb \Leftrightarrow a^{-1}b \in H$. Także relacja L_H jest relacją równoważności a jej klasami równoważności są, jak łatwo można się przekonać, zbiory postaci $[a]_{L_H} = aH$ (zwane *lewostronnymi warstwami modulo podgrupa* H).

2.7 Grupa dihedralna

Grupą diherdalną nazywamy grupę multyplikatywną

$$D_n = \{1, a, a^2, ..., a^{n-1}, b, ba, ba^2, ..., ba^{n-1}\}$$

gdzie

- $|a| = n, |b| = 2$,
- $aba = b$,
- $|D_n| = 2n$

– założenie, że $|D_n| = 2n$ oznacza, że $b \notin < a >$. Sprawdzenie, że zbiór D_n z multyplikatywnym działaniem spełniającym podane wyżej warunki rzeczywiście jest grupą pozostawione jest jako zadanie 2.7.

Twierdzenie 2.25 *Dla dowolnej liczby pierwszej p, każda grupa rzędu $2p$ jest albo izomorficzna z grupą cykliczną albo z grupą dihedralną D_p.*

Dowód. Niech G będzie grupą rzędu $2p$. Jeśli $p = 2$ wówczas $|G| = 4$ i G jest albo izomorficzna z $\mathbb{Z}_4$ albo izomorficzna z grupą Kleina (wniosek 2.24). Możemy więc założyć, że $p > 2$ i w konsekwencji $2 \perp p$.
Załóżmy, że G nie jest grupą cykliczną. Wykażemy, że jest izomorficzna z D_p.

Skoro G nie jest grupą cykliczną, każdy jej element jest albo rzędu p albo rzędu 2 (na mocy wniosku 2.22). Gdyby każdy element G był rzędu 2, wtedy grupa G byłaby przemienna (zadanie 2.10). Wówczas dla dowolnych $x, y \in G$ ($x \neq y; x, y \neq 1$) zbiór $\{1, x, y, xy\}$ byłby, jak łatwo sprawdzić, podgrupą rzędu 4, a to jest niemożliwe

[8] Stosujemy tu multyplikatywną konwencję oznaczania działania w grupie G.

bowiem $4 \not| |G|$.
W G istnieją więc elementy rzędu p. Oznaczmy przez g element rzędu p i przez H podgrupę generowaną przez g ($H =< g >$). Ponieważ $|H| = p$ każdy element podgrupy H różny od 1 jest rzędu p. Wiemy także, że $H \neq G$ i istnieje w G element nie należący do H.
Wykażemy następujący fakt.

Fakt 2.26 *Każdy element nie należący do H jest rzędu 2.*

Dowód faktu 2.26. Niech $h \in G - H$. Wiemy, że $|G| = 2p$. $|H| = |Hh| = p$, $H \cap Hh = \emptyset$ i stąd

$$H \cup Hh = G$$

Gdyby $h^2 \in Hh$ wówczas mielibyśmy $h^2 = fh$ dla pewnego $f \in H$ i wobec tego $h \in H$, sprzeczność. Stąd $h^2 \in H$ i wobec tego, $|h^2| = p$ lub $h^2 = 1$.Ponieważ p jest liczbą pierwszą nieparzystą, gdyby $|h^2| = p$ mielibyśmy

$$h = h^{p+1} = (h^2)^{\frac{p+1}{2}} \in H$$

a to jest sprzeczne z wyborem h.
Wiemy więc, że w G istnieją zarówno elementy rzędu p, jak i elementy rzędu 2.
Niech $a, b \in G$, $|a| = n, |b| = 2$. Ponieważ $G = H \cup bH$, mamy

$$G = \{1, a, ..., a^{p-1}, b, ba, ..., ba^{p-1}\}$$

Wiemy także, że $|a| = p$, $|b| = 2$. Skoro $ba \notin H$ mamy $|ba| = 2$ a więc

$$aba = (b^{-1}ba)(ba) = b^{-1}(ba)^2 = b^{-1} = b$$

To oznacza, że grupy G i D_n są izomorficzne. ■

2.8 Podgrupy normalne

Już wiemy (dowiedzieliśmy sie tego przy okazji dowodu twierdzenia Lagrange'a), że dla dowolnej podgrupy H grupy multyplikatywnej G relacja:

$$aRb \Longleftrightarrow ab^{-1} \in H \tag{2.12}$$

jest równoważnościowa. Klasą równoważności dowolnego elementu $a \in G$ dla tej relacji jest zbiór

$$Ha = \{ha | h \in H\}$$

zwany **warstwą prawostronną** elementu a.
Podobnie można zdefiniować **warstwę lewostronną** elementu a:

$$aH = \{ah | h \in H\}$$

Z łatwością można sprawdzić, że warstwy lewostronne są klasami równoważności dla relacji (także równoważnościowej) L zdefiniowanej w G wzorem $aLb \iff a^{-1}b \in H$ (gdzie H jest podgrupą G).

Przykład. Warstwy (lewo- i prawostronne) dla podgrupy $\{id, (12)\}$ grupy S_3 permutacji zbioru $\{1, 2, 3\}$.

Twierdzenie 2.27 *Jeśli grupa G jest przemienna, to dla dowolnej podgrupy H i $a \in G$*

$$aH = Ha$$

Definicja 2.7 *Mówimy, że podgrupa H grupy G jest* **normalna** *(lub* **niezmiennicza***), jeśli dla dowolnego $a \in G$ i dla dowolnego $b \in H$ zachodzi $aba^{-1} \in H$. Piszemy wtedy*

$$H \trianglelefteq G$$

Twierdzenie 2.28 *Podgrupa H grupy G jest normalna wtedy i tylko wtedy gdy dla każdego $a \in G$*

$$aH = Ha$$

Dowód. Rzeczywiście, przypuśćmy wpierw, że H jest podgrupą normalną grupy G, $a \in G$ i $x \in aH$. Skoro $x \in aH$, istnieje takie $d \in H$, że $x = ad$. Możemy wówczas napisać $x = ad(a^{-1}a) = (ada^{-1})a$. Ponieważ podgrupa H jest normalna, mamy $ada^{-1} \in H$, a wobec tego $x \in Ha$.
Wykazaliśmy więc, że $aH \subset Ha$. Faktu, że $Ha \subset aH$ dowodzimy analogicznie.
Przypuśćmy teraz, że $aH = Ha$ dla dowolnego elementu $a \in G$. Wykażemy, że podgrupa H jest normalna.
Niech $b \in H$ i $a \in G$. Wówczas oczywiście $ab \in aH$, a ponieważ $aH = Ha$ zachodzi także $ab \in Ha$. Istnieje więc takie $c \in H$, że $ab = ca$. Stąd już natychmiast wynika, że $aba^{-1} = c \in H$, co kończy dowód. ■

Twierdzenie 2.28 jest równoważne następującemu wnioskowi.

Wniosek 2.29 *Podgrupa H grupy G jest normalna wtedy i tylko wtedy gdy*

$$aHa^{-1} = H$$

dla dowolnego elementu $a \in G$.

Z twierdzenia 2.28 wynika, że jeżeli H jest podgrupą normalną grupy G, wówczas relacje, R i L zdefiniowane powyżej są identyczne. Zamiast pisać wtedy aRb czy też aLb będziemy pisać $a \overset{H}{\equiv} b$ (mówimy w takiej sytuacji, że **element** a **grupy** G **przystaje modulo** H **do elementu** b).

Twierdzenie 2.30 *Niech H będzie podgrupą grupy multyplikatywnej G. H jest podgrupą normalną wtedy i tylko wtedy gdy relacja R (zdefiniowana wzorem $aRb \Leftrightarrow ab^{-1} \in H$) jest zgodna z działaniem grupowym grupy G.*

Dowód. Przypuśćmy, że H jest podgrupą normalną grupy G, $a \stackrel{H}{\equiv} b$ oraz $c \stackrel{H}{\equiv} d$. Wówczas istnieją takie α i β, że $ab^{-1} = \alpha \in H$ i $cd^{-1} = \beta \in H$. Stąd zaś łatwo wynika, że $ac = \alpha(b\beta b^{-1})bd$. Skoro $\beta \in H$ i H jest podgrupą normalną, zachodzi $b\beta b^{-1} \in H$. Mamy więc $(ac)(bd)^{-1} = \alpha(b\beta b^{-1}) \in H$, co oznacza, że $ac \stackrel{H}{\equiv} bd$ a więc udowodniliśmy, że relacja przystawania modulo podgrupa normalna H jest zgodna z działaniem grupowym w G.
Załóżmy teraz, że relacja R jest zgodna z działaniem grupowym. Skorzystamy z twierdzenia 2.28 by wykazać, że podgrupa H jest normalna.
Niech $b \in Ha$. Wówczas oczywiście bRa. Wiemy także, że $a^{-1}Ra^{-1}$ (relacja R jest zwrotna). Ze zgodności R z działaniem grupowym wynika, że $(a^{-1}b)R(a^{-1}a)$, czyli $(a^{-1}bRe)$. Stąd zaś łatwo wywnioskować, że $a^{-1}b \in H$ i wobec tego $b \in aH$. Wykazaliśmy, że $Ha \subset aH$, dla dowolnego $a \in G$. Podobnie wykazać można, że $aH \subset Ha$. Stąd wynika że $aH = Ha$ dla dowolnego $a \in G$ i dowód wynika z twierdzenia 2.28. ■

Zgodność relacji przystawania modulo podgrupa H, gdy H jest podgrupą normalną oznacza, że w zbiorze ilorazowym G/H można zdefiniować działanie w ten sposób, że iloczynem klas jest klasa iloczynu. Inaczej mówiąc: poprawnie zdefiniowane jest wtedy działanie na klasach zdefiniowane wzorem:

$$(Ha) \cdot (Hb) := H(ab)$$

Z łatwością można wykazać, że wówczas G/H z tak określonym działaniem jest grupą (zwaną **grupą ilorazową**).

Twierdzenie 2.31 *Niech H będzie podgrupą normalną grupy G i niech $F \leq G$. Wówczas $FH = \{ab | a \in F, b \in H\}$ jest podgrupą grupy G.*

Dowód. Rzeczywiście, wystarczy sprawdzić, że gdy $a_1, a_2 \in F, b_1, b_2 \in H$, wówczas $(a_1b_1)(a_2b_2)^{-1} \in FH$.

$$(a_1b_1)(a_2b_2)^{-1} = a_1(b_1b_2^{-1})a_2^{-1}$$

Ponieważ podgrupa H jest normalna, istnieje taki element $b \in H$, że $(b_1b_2^{-1})a_2^{-1} = a_2^{-1}b$, stąd

$$a_1(b_1b_2^{-1})a_2^{-1} = a_1a_2^{-1}b \in FH$$

co dowodzi, że FH jest podgrupą grupy G. ■

Już najmniejsza nieprzemienna grupa S_3 dostarcza przykładu, że założenie twierdzenia 2.31, iż jedna z grup F, H jest normalna, jest istotne.

2.8.1 Podstawowe twierdzenie o izomorfizmie grup

Niech $h : G \to H$ będzie homomorfizmem gruy G w grupę H. W obu grupach działanie oznaczamy multiplikatywnie a elementy neutralne w obu grupach przez, odpowiednio 1_G i 1_H. Przez Ker h oznaczmy zbiór

$$\text{Ker } h = \{a \in G : h(a) = 1_H\}$$

Zbiór ten nazywać będziemy **jądrem homomorfizmu** h. Nietrudno udowodnić (por. zadanie 2.15), że jądro homomorfizmu grup jest podgrupą normalną grupy G. Zapiszmy ten fakt jako twierdzenie.

Twierdzenie 2.32 *Niech $h : G \to H$ będzie homomorfizmem grup. Wówczas Ker h jest podgrupą normalną grupy G.*

Niech $k : G \ni a \to (\text{Ker } h)a \in G/\text{Ker } h$. Oczywiście k jest homomorfizmem grup (nazywanym **homomorfizmem kanonicznym**). Zdefiniujmy następujące odwzorowanie

$$\bar{h} : G/(\text{Ker } h) \ni (\text{Ker } h)a \to h(a) \in H \tag{2.13}$$

Udowodnimy, że $\bar{h}$ jest izomorfizmem grup. Nim to jednak zrobimy musimy wykazać, że odwzorowanie $\bar{h}$ jest dobrze określone. Rzeczywiście, możemy mieć $Ha = Hb$ dla dwóch, niekoniecznie równych elementów a i b grupy G. Żeby nasze odwzorowanie miało sens musimy wtedy mieć $\bar{h}(Ha) = \bar{h}(Hb)$.
Przypomnijmy jednak sobie, że elementy Ha i Hb są wtedy klasami równoważności relacji $aRb \Leftrightarrow ab^{-1} \in \text{Ker } h$ czyli $h(ab^{-1}) = 1_H$ a więc $h(a) = h(b)$, co oznacza, że nasze odwzorowanie, 're nasze odwzorowanie $\bar{h} : (\text{Ker } h)a \to \bar{h}((\text{Ker } h)a) = h(a)$ ma sens. Mamy także

$$\begin{array}{rcll} \bar{h}(((\text{Ker } h)a)((\text{Ker } h)b)) & = & \bar{h}((\text{Ker } h)(ab)) & \text{z def. mnożenia w } G/(\text{Ker } h) \\ & = & h(ab) & \text{z definicji } \bar{h} \\ & = & h(a)h(b) & \text{bo } h \text{ jest homomorfizmem} \\ & = & \bar{h}((\text{Ker } h)a)\bar{h}((\text{Ker } h)b) & \text{z definicji } \bar{h} \end{array}$$

skąd wynika, że $\bar{h}$ jest homomorfizmem grup. Nietrudno sprawdzić, że $\bar{h}$ jest także bijekcją, a więc izomorfizmem.
Zauważmy, że dla dowolnego $a \in G$ zachodzi wzór

$$h(a) = \bar{h}(k(a))$$

Wykazaliśmy tym samym twierdzenie zwane **Podstawowym** (lub **Pierwszym**) **Twierdzeniem o Izomorfizmie Grup**[9].

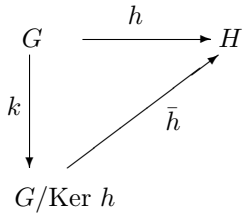
Twierdzenie 2.33 *Każdy epimorfizm grup $h : G \to H$ można zapisać w postaci $h = \bar{h} \circ k$ gdzie $\bar{h}$ jest izomorfizmem przyporządkowującym każdej warstwie $(Ker\ h)a$ grupy ilorazowej $G/Ker\ h$ element $h(a) \in H$, zaś k homomorfizmem kanonicznym przyporządkowującym każdemu elementowi $a \in G$ jego warstwę $(Ker\ h)a$.*

Często wykorzystuje się następującą postać tego twierdzenia.

Wniosek 2.34 *Niech $h : G \to H$ będzie epimorfizmem grup. Wówczas grupy $G/Ker\ h$ i H są izomorficzne.*

[9] To samo twierdzenie nazywane jest czasami *Podstawowym (Pierwszym) Twierdzeniem o Homomorfizmie Grup*. Tyle nazw dla twierdzenia o mało skomplikowanym dowodzie jest uzasadnione jego rozlicznymi zastosowaniami.

Twierdzenie 2.33 wygodnie jest zilustrować na diagramie. Wzór $h(a) = \bar{h}(k(a))$ interpretujemy na tym diagramie mówiąc, że *jest przemienny*[10].



2.9 Sprzężenie podgrupy

Sprzężeniem elementu a grupy G nazywamy każdy element b postaci $b = xax^{-1}$, gdzie $x \in G$ (dokładniej, mówimy wtedy, że b jest *sprzężeniem* a *przez* x. Z łatwością można wykazać, że relacja ρ zdefiniowana przez

$$a\rho b \text{ jeśli } b \text{ jest sprzężeniem } a$$

jest relacją równoważności (por. zadanie 2.17).

Sprzężeniem zbioru A zawartego w grupie G przez element $a \in G$ nazywamy zbiór aAa^{-1}.

Twierdzenie 2.35 *Jeśli H jest podgrupą grupy G, $g \in G$, wówczas gHg^{-1} jest podgrupą grupy G.*

Rzeczywiście, niech $a, b \in gHg^{-1}$. Wówczas istnieją $h, f \in h$ takie, że $a = ghg^{-1}, b = gfg^{-1}$. Wtedy $ab^{-1} = (ghg^{-1})(gfg^{-1}) = g(hf)g^{-1} \in gHg^{-1}$. ■

W związku z twierdzeniem 2.35 sprzężenie podgrupy $H \leq G$ będziemy nazywali także *podgrupą sprzężoną* H w G (przez element a).

Przykład 2.9 *Niech O_{AG} będzie podgrupą obrotów sześcianu wokół osi łączącej wierzchołki A i G (oznaczenia jak w przykładzie 4.2). Inaczej mówiąc $O_{AG} = \{id, \sigma_1 = (A)(G)(B,E,D)(C,F,H), \sigma_2 = (A)(G)(B,D,E)((C,H,F)\}$. Oznaczmy przez $\tau = (A,B,F,E)(D,C,G,H)$ - obrót wokół osi łączącej środki ścian przeciwległych o wierzchołkach A,B,F,E i D,C,G i H o $\pi/2$. Sprzężeniem O_{AG} przez τ jest*

$$\tau O_{AG}\tau^{-1} = \{id, (B)(H)(A,C,F)(G,E,D), (B)(H)(A,F,C)(D,E,G)\} = O_{BH}$$

a więc podgrupa obrotów wokół osi przechodzącej przez wierzchołki B i H.

Dowód następnego twierdzenia pozostawiamy czytelnikowi, jako łatwe ćwiczenie.

[10] To stąd, że z G do H można równoważnie dojść na dwa sposoby: bezpośrednio lub przez $G/\text{Ker } h$.

Twierdzenie 2.36 *Niech G będzie grupą i H podgrupą grupy G. H jest podgrupą normalną grupy G wtedy i tylko wtedy gdy $gHg^{-1} = H$ dla każdego $g \in G$.* ■

Normalizatorem podgrupy[11] H w grupie G nazywamy zbiór

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

Normalizator dowolnej podgrupu H zawiera H a co za tym idzie $N_G(H) \neq \emptyset$. Niech $a, b \in N_G(H)$. Wówczas

$$(ab^{-1})H(ab^{-1})^{-1} = (ab^{-1})H(ba^{-1}) = a(b^{-1}Hb)a^{-1}$$

Łatwo zauważyć (mnożąc równość $bHb^{-1} = H$ przez b^{-1} z lewej i przez b z prawej strony), że $b^{-1}Hb = H$ (dla $b \in N_G(H)$). A więc

$$(ab^{-1})H(ab^{-1})^{-1} = aHa^{-1} = H$$

Udowodniliśmy w ten sposób, że dla dowolnych $a, b \in N_G(H)$ także $ab^{-1} \in N_G(H)$. Oznacza to, na mocy twierdzenia 2.7, że $N_G(H) \leq G$.
Bardzo podobnie można udowodnić, że H jest podgrupą normalną $N_G(H)$. Co więcej, $N_G(H)$ zawiera *wszystkie* elementy $g \in G$ takie, że $gHg^{-1} = H$ (czyli $gH = Hg$). $N_G(H)$ jest więc największą podgrupą taką, że H jest jej podgrupą normalną. Warto zapisać te fakty w postaci następującego twierdzenia.

Twierdzenie 2.37 *Normalizator $N_G(H)$ podgrupy H w grupie G jest największą (ze względu na zawieranie) podgrupą grupy G, której H jest podgrupą normalną.* ■

Będziemy wykrzystywać twierdzenie następujące.

Twierdzenie 2.38 *Niech G będzie grupą skończoną, $H \leq G$. Liczba sprzężeń podgrupy H jest równa $|G : N_G(H)|$.*

Dowód. $G : N_G(H)$ jest zbiorem klas modulo $N_G(H)$, czyli $G : N_G(H) = \{N_G(H)a : a \in G\}$. Zbiór sprzężeń podgrupy H to $C = \{aHa^{-1} : a \in G\}$. Zauważmy, że $C = \{a^{-1}Ha : a \in G\}$. Zdefiniujmy funkcję ϕ ze zbioru C w zbiór $G : N_G(H)$ następującym wzorem

$$\phi : C \ni a^{-1}Ha \longrightarrow N_G(H)a \in G : N_G(H)$$

Wykażemy kolejno, że ϕ jest:

1. dobrze określona,

[11] Podobnie jak normaliator podgrupy można zdefiniować normalizator dowolnego podzbioru $X \subset G$, a więc $N_G(X) = \{g \in G : gXg^{-1} = X\}$. Także w tym przypadku $N_G(X)$ jest podgrupą grupy G.

2. injekcją,

3. surjekcją.

W pierwszym punkcie należy wykazać, że wartość ϕ na zbiorze $a^{-1}Ha$ nie zależy od tego którego reprezentanta $a^{-1}Ha$ wybierzemy. Inaczej mówiąc, że jeśli $a^{-1}Ha = b^{-1}Hb$ wówczas $N_G(H)a = N_G(H)b$. Rzeczywiście:

$$\begin{aligned} a^{-1}Ha = b^{-1}Hb &\iff ba^{-1}Hab^{-1} = H \\ &\iff (ba^{-1})H(ba^{-1})^{-1} = H \\ &\iff ba^{-1} \in N_G(H) \\ &\iff b \in N_G(H)a \\ &\iff N_G(H)a = N_G(H)b \end{aligned} \tag{2.14}$$

Aby udowodnić injektywność funkcji ϕ należy wykazać, że

$$\phi(a^{-1}Ha) = \phi(b^{-1}Hb) \Longrightarrow a^{-1}Ha = b^{-1}Hb$$

czyli

$$N_G(H)a = N_G(H)b \Longrightarrow a^{-1}Ha = b^{-1}Hb$$

W tym celu wystarczy zauważyć, że w (2.14) mamy nie tylko wynikania, ale równoważności.

Dowód surjektywności odwzorowania ϕ jest bardzo prosty: dla dowolnego elementu $N_G(H)a \in G : N_G(H)$ mamy $N_G(H)a = \phi(aHa^{-1})$. ■

W grupie G zbiór $Z(G) = \{a \in G | ab = ba \text{ dla wszystkich } b \in G\}$ nazywamy **centrum** grupy G. Oznacza to dokładnie tyle, że w centrum są wszystkie te elementy grupy, dla których mnożenie przez dowolny element grupy jest przemienne. Łatwo wykazać, że $Z(G) \leq G$. Co więcej, prawdziwe jest następujące twierdzenie (por. zadanie 2.18).

Twierdzenie 2.39 *Dla dowolnej grupy G,*

$$Z(G) \trianglelefteq G$$

. ■

Dla dowolnego elementu a grupy G przez $C(a)$ oznaczamy te wszystkie elementy grupy G, dla których mnożenie przez a jest przemienne:

$$C(a) = \{b \in G | ab = ba\}$$

$C(a)$ nazywamy **centralizatorem elementu** a. Prawdziwe jest następujące twierdzenie (por. zadanie 2.19).

Twierdzenie 2.40 *Centralizator dowolnego elemntu grupy G jest podgrupą grupy G.* ■

2.10 Grupy alternujące

Z łatwością można sprawdzić, że dowolne dwie grupy permutacji zbioru n elementowego są izomorficzne[12]. Przez S_n oznaczamy grupę wszystkich permutacji zbioru n elementowego $\{1, 2, ..., n\}$.
Z kursu algebry liniowej, czytelnik powinien pamiętać, że każdą pemutację $\sigma \in S_n$ można przedstawić jako złożenie pewnej liczby cykli długości 2, czyli *transpozycji*. Liczba tych transpozycji nie jest niezmiennikiem permutacji (to znaczy, że jeśli tylko $n \geq 2$, dla danej permutacji istnieją rozkłady na różne liczby transpozycji), natomiast niezmiennikiem permutacji jest parzystość liczby transpozycji. Jeśli więc permutacja $\sigma \in S_n$ ma rozkład na parzystą liczbę transpozycji, wówczas każdy rozkład σ ma parzystą liczbę transpozycji. Stąd można zdefiniować funkcję zwaną *znakiem permutacji* wzorem

$$\epsilon(\sigma) = \begin{cases} 1 & \text{jeśli } \sigma \text{ jest parzysta} \\ -1 & \text{jeśli } \sigma \text{ jest nieparzysta} \end{cases}$$

Przez A_n będziemy oznaczać zbiór wszystkich permutacji parzystych S_n, czyli $A_n = \{\sigma \in S_n : \epsilon(\sigma) = 1\}$. Z łatwoćią można sprawdzić, że A_n jest podgrupą grupy S_n. Podgrupę tę nazywamy *grupą alternującą*.
Zauważmy, że zbiór B_n permutacji nieparzystych podgrupą S_n nigdy nie jest. Rzeczywiście, złożenie dwóch permutacji nieparzystych jest oczywiście permutacją parzystą. Stąd działanie składania permutacji w zbiorze B_n nie jest zamknięte. Zbiory A_n i B_n są równoliczne i rozłączne. Rozłączność A_n i B_n jest oczywista. Funkcja

$$f : A_n \ni \sigma \longrightarrow (1, 2) \circ \sigma \in B_n$$

jest bijekcją zbiorów A_n i B_n. Jeśli bowiem $f(\sigma) = f(\sigma')$, wówczas $(1, 2) \circ \sigma = (1, 2) \circ \sigma'$. Mnożąc tę równość lewostronnie przez transpozycję $(1, 2)$ otrzymujemy $\sigma = \sigma'$, a więc f jest funkcją injektywną. Co więcej, jeżeli $\tau \in B_n$, wówczas $(1, 2) \circ \in A_n$ i $f((1, 2) \circ \tau) = \tau$ co oznacza, że f jest także surjekcją. Wykazaliśmy w ten sposób następujące twierdzenie.

Twierdzenie 2.41 *Jeżeli $n \geq 2$ wówczas $|A_n| = n!/2$.* ■

[12] Czytelnik zechce wskazać izomorfizm grupy permutacji n-elementowych zbiorów $\{a_1, ..., a_n\}$ i $\{b_1, ..., b_n\}$.

2.11 Zadania

Zadanie 2.1 Które z poniższych zbiorów wraz z podanymi działaniami są grupami? grupami abelowymi?

1. $\mathbb{Q}^+ = \{a \in \mathbb{Q} : a > 0\}$ z działaniem mnożenia.
2. $\mathbb{Q}^- = \{a \in \mathbb{Q} : a < 0\}$ z działaniem mnożenia.
3. $GL(n, F)$ - zbiór macierzy nieosobliwych rozmiaru $n \times n$, o współczynnikach w ciele F z działaniem mnożenia macierzy.
4. $\{1, 3, 4, 8, 12, 24\}$ z działaniem NWD (największy wspólny dzielnik).
5. $\{2, 4, 8\}$ z działaniem NWD.
6. $\{3, 4, 12\}$ z działaniem NWW (najmniejsza wspólna wielokrotna).
7. Zbiór wielomianów o współczynnikach wymiernych i wyrazem wolnym całkowitym. Z dodawaniem. Z mnożeniem.

Zadanie 2.2 Udowodnij, że jeśli element $a \in \mathbb{Z}_n$ jest *dzielnikiem zera* (to znaczy: $a \neq 0$ oraz istnieje taki element $b \in \mathbb{Z}_n - \{0\}$, że $ab = 0$), wówczas

1. n jest liczbą złożoną,
2. a nie ma elementu odwrotnego ze względu na mnożenie.

Zadanie 2.3 Niech G będzie grupą multiplikatywną, $g \in G$, $|g| < \infty$. Udowodnij, że jeżeli $g^m = 1$ wówczas $|g|$ dzieli m.

Zadanie 2.4 Niech a, b będą elementami skończonego rzędu grupy abelowej. Wykaż, że $|ab|$ dzieli $NWW(|a|, |b|)$. Wskaż przykład gdy $|ab| \neq NWW(|a|, |b|)$.

Zadanie 2.5 Dla podanych permutacji $\sigma, \tau, \omega \in S_9$ znajdź ich postaci cykliczne a następnie oblicz: $\sigma^2, \sigma \circ \tau, \sigma \circ \omega^{-1}, \sigma^{-2}, \tau^{-3}$.
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 6 & 5 & 2 & 7 & 9 & 8 & 1 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 8 & 3 & 9 & 4 & 5 & 1 & 6 \end{pmatrix}$, $\omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 6 & 7 & 1 & 2 & 9 & 8 \end{pmatrix}$.

Zadanie 2.6 Udowodnij, że jeśli dwie podgrupy rzędu będącego liczbą pierwszą p nie są identyczne to ich przecięciem jest $\{e\}$.

Zadanie 2.7 Sprawdź, że zbiór D_n z działaniem multyplikatywnym spełniającym warunki podane w definicji grupy dihedralnej na stronie 33 rzeczywiście tworzy grupę.

Zadanie 2.8 Udowodnij, że w grupie dihedralnej D_n zachodzą następujące związki:

- $a^k b a^k = b$ dla $k \in \mathbb{Z}$

- $|ba^k| = 2$ dla $k \in \mathbb{Z}$
- $ab = ba^{n-1}$
  (oznaczenia jak na stronie 33).

Zadanie 2.9 Udowodnij, że zbiory D'_n i W_n wraz z określinymi w nich działaniami tworzą grupy izomorficzne z grupą dihedralną.

1. D'_n – zbiór izometrii n-kąta foremnego ze składaniem odwzorowań jako działaniem zdefiniowany w 2.5.
2. W_n – zbiór permutacji generowanych przez $a = (1, 2, ..., n)$, $b = (1, n-1)(2, n-2)... \in S_n$ (z działaniem składania premutacji).

Zadanie 2.10 Niech G będzie grupą skończoną taką, w której dla dowolnego elementu a zachodzi $|a| \leq 2$.

1. Wykaż, że G jest przemienna.
2. Niech $H \leq G$ i $g \in G$. Wykaż. że $H \cup gH \leq G$.
3. Udowodnij, że $|H \cup gH| = 2|H|$.
4. Wykaż, że rząd grupy G jest pewną potęgą dwójki.

Zadanie 2.11 Udowodnij, że dla dowolnej podgrupy H grupy G relacja przystawania modulo H jest relacją równoważności (lemat 2.17).

Zadanie 2.12 Niech g będzie grupą, $g \in G$.
Wykaż, że

- jeśli $|G| = 28,\ g^4 \neq 1, g^7 \neq 1$ to $G =< g >$,
- jeśli $|G| = 24,\ g^8 \neq 1, g^6 \neq 1$ to $G =< g >$.

Zadanie 2.13 Niech p będzie liczbą pierwszą. Wykaż, że wszystkie właściwe podgrupy grupy G rzędu p^2 są cykliczne.
Sformułuj tekst tego zadania dla grup addytywnych.

Zadanie 2.14 Napisz tabele Cayleya dla D_2, D_3 i D_4. Sprawdź, że D_2 to grupa izomorficzna do grupy Kleina a D_3 do grupy S_3.

Zadanie 2.15 Udowodnij, że dla każdego homomorfizmu grup $h : G \to H$ jądro Ker h jest podgrupą normalną grupy G.

Zadanie 2.16 Niech G będzie grupą, $H \trianglelefteq G$. Udowodnij, że jeśli K' jest podgrupą grupy ilorazowej G/H, wówczas $K = \{x \in G |\ Hx \in G'\}$ jest podgrupą grupy G (ten fakt wykorzystamy w dowodzie twierdzenia 5.4).

Zadanie 2.17 Udowodnij, że w dowolnej grupie G relacja ρ zdefiniowana przez $a\rho b \Leftrightarrow b = xax^{-1}$ dla pewnego $x \in G$ jest relacją równoważności.
Wypisz tablicę Cayleya grupy D_4 izometrii kwadratu i znajdź wszystkie klasy równoważności relacji ρ w tej grupie.

Zadanie 2.18 Udowodnij, że centrum dowolnej grupy G jest jej podgrupą normalną.

Zadanie 2.19 Wykaż, że centralizator $C(a)$ elementu a grupy G (por. str. 40) jest podgrupą grupy G.

Zadanie 2.20 Wskaż centralizatory wszystkich elementów grupy D_4.

Rozdział 3

Arytmetyka modularna

Arytmetyka modularna to arytmetyka w zbiorach $\mathbb{Z}_n$. W bardzo skromnym zakresie w którym jest mowa o niej tutaj jest silnie związana z teorią grup.

3.1 Twierdzenie Eulera i Małe Twierdzenie Fermata

Twierdzenie 3.1 (Eulera) *Jeśli liczby naturalne a, n są względnie pierwsze, wówczas*

$$a^{\varphi(n)} \equiv 1 \ (\mod n)$$

Dowód. Jak wiemy (twierdzenie 2.3), rząd grupy $\mathbb{Z}_n^*$ jest równy $\varphi(n)$. Oznaczmy przez r rząd elementu a. Na mocy wniosku 2.22, istnieje k naturalne takie, że $\varphi(n) = kr$. Mamy więc

$$a^{\varphi(n)} = (a^r)^k \equiv 1^k = 1(\mod n)$$

■

Ogromnej popularności i użyteczności jest następujące twierdzenie udowodnione przez Fermata[1]. Twierdzenie to ma bardzo wiele dowodów (zob. [19]), z których

[1]Pierre Fermat, 1601-1665. Był matematycznym samoukiem, natomiast z zawodu był prawnikiem. Nie tylko dlatego, że ukończył studia prawnicze na uniwersytecie w Orleanie. Był aktywnym prawnikiem w sensie tworzenia prawa, także jako parlamentarzysta (członek Parlamentu Tuluzy). Jego niewątpliwie najbardziej spektakularnym odkryciem jest Wielkie Twierdzenie Fermata zwane także Ostatnim Twierdzeniem Fermata. Twierdzenie to, które zapisał na marginesie czytanego właśnie dzieła *Arithmetica* Diofantesa mówi, że dla naturalnych $n \geq 3$ nie istnieją całkowite rozwiązania równania $x^n + y^n = z^n$. Obok twierdzenia Fermat zapisał także, że odkrył ciekawy dowód, który jednak na marginesie już się nie mieści. Wiekie Twierdzenie Fermata zostało ostatecznie udowodnione w 1994 roku przez brytyjskiego matematyka Andrew Wilesa. Dowód Wilesa wykorzystuje osiągnięcia nowoczesnej matematyki, które Fermatowi nie były znane. Być może nigdy się nie dowiemy, czy dowód o którym wspomniał Fermat zawierał błąd, czy też opierał się na jakimś, ciągle nieznanym pomyśle. Nie wiadomo też, czy uwaga Fermata o znalezieniu dowodu nie była dowcipem uczynionym pokoleniom matematyków. Fermat raczej nie mógł przypuszczać, jakie zamieszanie powstanie 250 lat po jego śmierci, gdy Akademia Berlińska wyznaczyła nagrodę w wysokości 100 000 marek za wskazanie dowodu.

jeden cytujemy poniżej.

Twierdzenie 3.2 (Małe Twierdzenie Fermata) *Jeśli p jest liczbą pierwszą, $a \in \mathbf{Z}$, to*

$$a^p \equiv a(\ mod\ p)$$

Dowód.

Załóżmy wpierw, że $0 \leq a$. Dla $a = 1$ twierdzenie jest oczywiście prawdziwe. Pozdobnie dla $a = 0$.
Jeśli $1 < a < p$ to a i p są względnie pierwsze korzystając z twierdzenia Eulera i faktu, że $\varphi(p) = p - 1$ mamy

$$1 \equiv a^{\varphi(p)} = a^{p-1}\ (\mod p)$$

a stąd $a^p \equiv a(\mod p)$.
Jeśli $a \geq p$ wówczas napiszmy $a = qp + r$, gdzie $0 \leq r < p$. Mamy wtedy

$$a^p = (r + pq)^p = \sum_{i=0}^{p} \binom{p}{i} r^i (pq)^{p-i}$$

Zauważmy, że dla dowolnego $i \neq p$ składnik $\binom{p}{i} r^i (pq)^{p-i}$ jest podzielny przez p a więc, przystaje do zera modulo p. Stąd mamy

$$a^p \equiv r^p\ (\mod p)$$

Ponieważ jednak $0 \leq r < p$, mamy $a^p \equiv r^p \equiv r \equiv a(\mod p)$.

Jeśli $a < 0$, to możemy rozpatrzyć dwa przypadki.

Przypadek 1: $p = 2$**.** Jeśli a jest parzyste, wówczas także a^2 jest parzyste i oczywiście $a^2 \equiv 0(\mod 2)$ oraz $a \equiv 0(\mod 2)$. Podobnie dla a nieparzystego: $a \equiv 1(\mod 2)$ oraz $a^2 \equiv 0(\mod 2)$.

Przypadek 2: $p > 2$**.** Każda liczba pierwsza różna od 2 jest nieparzysta. Korzystając więc z udowodnionego już przypadku gdy $a \geq 0$ mamy

$$a^p = (-1)^p(-a)^p \equiv (-1)(-a) = a(\mod p)$$

■

3.2 Chińskie twierdzenie o resztach – równania modularne

Twierdzenie 3.3 *Równanie modularne*

$$ax \equiv 1\ (mod\ n) \tag{3.1}$$

ma rozwiązanie wtedy i tylko wtedy gdy a i n są względnie pierwsze (oczywiście takie rozwiązanie jest jedyne w $\mathbf{Z_n}$ i jest postaci $x \equiv a^{-1}b \ (mod\ n)$, lub inaczej: $x = x_0 + kn$, gdzie $k \in \mathbf{Z_n}$, zaś x_0 jest równy $a^{-1}b$ przy czym a^{-1} jest el. odwrotnym do a w $\mathbf{Z}_n$ ze względu na mnożenie).

Sposobem znajdowania elementu odwrotnego do elementu a w $\mathbf{Z}_n$ jest skorzystanie z algorytmu Euklidesa. Jest to możliwe zawsze wtedy gdy taki element istnieje, a mianowicie gdy a i n są względnie pierwsze. Rzeczywiście, $a \perp n$ wtedy i tylko wtedy, jeśli istnieją s i t całkowite spełniające

$$sa + tn = 1$$

Wówczas $sa = 1 + (-t)n$, co oznacza, że s jest w $\mathbf{Z}_n^*$ elementem odwrotnym do a.

Twierdzenie 3.4 (Chińskie o resztach[2]) *Niech $a, b \in \mathbf{Z}$, $m, n \in \mathbf{N}$, $m \perp n$. Wówczas układ równań*

$$\begin{cases} x & \equiv & a & (mod\ m) \\ x & \equiv & b & (mod\ n) \end{cases} \tag{3.2}$$

ma rozwiązanie. Co więcej, każde dwa rozwiązania tego układu różnią się o wielokrotność mn (można też powiedzieć, że rozwiązanie jest jedyne modulo mn lub, że zbiór rozwiązań (3.2) jest postaci $\{x_0 + k(mn) | k \in \mathbf{Z}\}$).

Dowód Chińskiego Twierdzenia o Resztach, w zupełnie naturalny sposób składa się z dwóch części: dowodu istnienia rozwiązania układu równań modularnych (3.2) modulo nm i dowodu jedyności takiego rozwiązania.

Istnienie. Z pierwszego z równań układu (3.2) wynika, że

$$x = a + \alpha m \tag{3.3}$$

gdzie $\alpha \in \mathbb{Z}$. Po wstawieniu tego wyrażenia do drugiego równania układu otrzymamy

$$a + \alpha m \equiv b(\mod n)$$

a więc

$$\alpha m = (b - a)(\mod n) \tag{3.4}$$

Ponieważ m i n są względnie pierwsze, w grupie $\mathbb{Z}_n^*$ istnieje element k odwrotny do m. Mnożąc równanie (3.4) przez k, otrzymamy

$$\alpha \equiv k(b - a)(\mod n)$$

czyli

$$\alpha = k(b - a) + \gamma n$$

gdzie $\gamma \in \mathbb{Z}$. Stąd, po wstawieniu obliczonego α do równania (3.3) otrzymujemy

$$x = a + (k(b - a) + \gamma n)m$$

[2]Twierdzenie to ukazało się po raz pierwszyl ok. 350 roku n.e. w książce Sun Tsu.

a więc

$$x \equiv a + k(b-a)m(\mod mn)$$

rozwiązanie naszego układu modulo mn.

Jedyność rozwiązania modulo mn**.** Przypuśćmy, że x_0 i x_1 są rozwiązaniami układu równań modularnych (3.2). Wówczas

$$\left\{\begin{array}{rcll} x_0 & \equiv & a & (\mod m) \\ x_0 & \equiv & b & (\mod n) \end{array}\right. \text{ oraz } \left\{\begin{array}{rcll} x_1 & \equiv & a & (\mod m) \\ x_1 & \equiv & b & (\mod n) \end{array}\right.$$

i wobec tego

$$\left\{\begin{array}{rcll} x_0 - x_1 & \equiv & 0 & (\mod m) \\ x_0 - x_1 & \equiv & 0 & (\mod n) \end{array}\right.$$

Ostatnie przystawania (modulo m i modulo n) oznaczają, że $m|x_0 - x_1$ oraz $n|x_0 - x_1$. Ponieważ jednak $m \perp n$, wynika stąd, że $mn|x_0 - x_1$ czyli, że $x_0 - x_1 \equiv 0 \pmod{mn}$ (naprawdę przekonywującego uzasadnienia ostatniej aplikacji dostarcza *zasadnicze twierdzenie arytmetyki*, o którym będzie mowa później) .

■

Zauważmy, że dowód Chińskiego Twierdzenia o Resztach zawiera algorytm rozwiązywania równań mdularnych. Warto także zwrrócić uwagę na fakt, że w metodzie tej ważną rolę odgrywa umiejętność znajdowania elementów odwrotnych modulo, a więcd i tym razem mamy tu zastosowanie algorytmu Euklidesa.

Twierdzenie 3.4 pozwala łatwo (indukcyjnie) udowodnić następujące uogólnienie chińskiego twierdzenia o resztach.

Twierdzenie 3.5 *Niech* $m_1, \ldots, m_k \in \mathbf{N}$ *będą parami pierwsze (t.zn.* $m_i \perp m_j$ *dla* $i \neq j$*). Wówczas układ równań*

$$\left\{\begin{array}{rcll} x & \equiv & a_1 & (\ mod\ m_1) \\ x & \equiv & a_2 & (\ mod\ m_2) \\ & & \cdots & \\ x & \equiv & a_k & (\ mod\ m_k) \end{array}\right. \tag{3.5}$$

ma jednoznaczne rozwiązanie modulo $m_1 \cdot \cdots \cdot m_k$.

3.3 Residua kwadratowe

Niech $n \in \mathbf{N}, a \in \mathbf{Z}_n$. Mówimy, że a jest **kwadratowym residuum modulo** n, jeżeli istnieje $b \in \mathbf{Z}_n$ takie, że $a = b^2 \pmod n$.

Można więc powiedzieć, że residua kwadratowe modulo n to elementy $\mathbb{Z}_n$, które są kwadratami pewnych elementów $\mathbb{Z}_n$.

Wypiszmy w tabelce wszystkie elementy $\mathbb{Z}_8$ i ich kwadraty.

a	0	1	2	3	4	5	6	7
a^2	0	1	4	1	0	1	4	1

Przede wszystkim, nie każdy element $\mathbb{Z}_8$ jest residuum kwadratowym. Co więcej, z łatwością zauważamy, że nasza tabelka jest niemal symetryczna (*niemal*, gdyż symetryczna staje się po pominięciu pierwszej kolumny). Rzeczywiście, jeśli $b^2 \equiv a \pmod{n}$ wówczas: w. 4 23.10.2012

$$(n-b)^2 = n^2 - 2nb + b^2 \equiv b^2 \equiv a \pmod{n}$$

Wniosek stąd taki, że jeśli b jest pierwiastkiem kwadratowym modulo n z a, wówczas także $n-b$ (czyli $-b \pmod{n}$) jest pierwiastkiem modulo n z a. Sytuacja jest więc taka, że zawsze (poza przypadkiem najmniejszego nietrywialnego zbioru modulo, to znaczy $\mathbb{Z}_2$) istnieją takie elementy, które są kwadratami dwóch różnych lelementów Z_n. Ponieaż zaś zbiór $\mathbb{Z}_n$ jest skończony, jeśli tylko $n > 2$, nie wszystkie elementy Z_n są residuami kwadratowymi. Jeśli n jest liczbą pierwszą, wówczas sytuacja jest szczególnie prosta.

Twierdzenie 3.6 *Niech p będzie liczbą pierwszą i niech $a \in \mathbf{Z}_p$ będzie residuum kwadratowym. Wówczas a ma dokładnie dwa pierwiastki kwadratowe w $\mathbf{Z}_p$.*

Dowód. Przypuśćmy, że x i y są dwoma różnym pierwiastkami kwadratowymi z a w $\mathbb{Z}_p$, przy czym $y \not\equiv -x \pmod{p}$. Mamy więc

$$y \not\equiv x \text{ oraz } y \not\equiv -x \pmod{p}$$

a wobec tego

$$x - y \not\equiv 0 \text{ oraz } x + y \not\equiv 0 \pmod{p}$$

Otrzymujemy więc $(x-y)(x+y) = x^2 - y^2 \equiv a - a = 0 \pmod{p}$. To zaś jest sprzeczne z faktem, że w $\mathbb{Z}_p$ (dla p pierwszego) iloczyn dwóch elementów różnych od zera jest także różny od zera. Tak więc nie istnieje element $y \in Z_p$, różny od x i od $-x \pmod{p}$, który jest kwadratowym pierwiastkiem z a. ■

W zastosowaniach arytmetyki modularnej w kryptografii z kluczem publicznym będzie nam niezbędna praktyczna umiejętność obliczania pierwiastków kwadratowych modulo n. Nie zawsze jest to możliwe, dla nas wystarczy, że bedziemy umieli to robić dla residuów kwadratowych modulo p, gdzie p jest liczbą pierwszą przystającą do 3 modulo 4.

Twierdzenie 3.7 *Niech $p \in \mathbf{N}$ będzie liczbą pierwszą, $p \equiv 3$ (mod 4) i niech a będzie residuum kwadratowym w $\mathbf{Z}_p$. Wówczas pierwiastkami kwadratowymi a w $\mathbf{Z}_p$ są $a^{\frac{p+1}{4}}$ (mod p) oraz $-a^{\frac{p+1}{4}}$ (mod p).*

Dowód. Niech a będzie residuum kwadratowym modulo p,gdzie $p \equiv 3 \pmod{4}$. Wówczas istnieje $b \in \mathbb{Z}$ takie, że $b^2 \equiv a \pmod{p}$. Stąd wynika, że

$$\left(a^{\frac{p+1}{4}}\right)^2 = \left((b^2)^{\frac{p+1}{4}}\right)^2 = b^p \cdot b$$

Na mocy Małego Twierdzenia Fermata $b^p \equiv b \pmod{p}$, a więc

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv b^2 \equiv a \pmod{p}$$

Oczywiście mamy także

$$\left(a^{\frac{p+1}{4}}\right)^2 = (-1)^2 \left(a^{\frac{p+1}{4}}\right)^2 \equiv a \pmod{p}$$

co kończy dowód twierdzenia. ■

Zauważmy, że obliczanie pierwiastków kwadratowych z wykorzystaniem twierdzenia 3.7 jest algorytmicznie łatwe: należy wykonać $\frac{p+1}{4}$ mnożeń.

3.4 Zasady kryptografii z kluczem publicznym

Wyobraźmy sobie, że mamy trzy osoby: Alicję, Boba i Ewę. Alicja chce przeslać Bobowi pewne informacje tak, by Ewa (ani nikt inny poza Bobem) nie mógł odgadnąć ich treści mimo, że informacje te przekazywane są w sposób jawny[3]. Warto w tym miejscu zdać sobie sprawę, że każdą informację można traktować jako liczbę. Standardowym zapisem jest powszechnie znany kod ASCII który można z łatwością zdobyć, na przykład za pomocą internetu (w kodzie tym każdemu znakowi odpowiada 3-cyfrowa liczba, *a* to 097, spacja to 032, *o* to 111 itd). Kod ASCII ma jednak oczywistą wadę: wszyscy go znają, a w każdym razie wiedzą jak sie w niego zaopatrzyć. Tak więc Alicja i Bob będą musieli przesyłane dane zaszyfrować (funkcję szyfrującą oznaczać będziemy przez E[4], na dodatek wychodząc z założenia, że wszystkie przesyłane wiadomości są podsłuchiwane (przez Ewę).

Powiedzmy, że Alicja chce zaszyfrować i następnie przesłać Bobowi liczbę naturalną l. By osiągnąć swój cel, Alicja i Bob będą postępowali według następującego schematu:

1	Bob znajduje funkcję szyfrującą (szyfrującą) E oraz rozszyfrującą D, a więc takie by $D(E(l)) = l$
2	Bob przesyła tekstem otwartym (Ewa widzi przekaz) funkcję E Alicji
3	Alicja szyfruje informację którą chce przesłać Bobowi według otrzymanej przez niego instrukcji (tę instrukcje zna także Ewa). Inaczej mówiąc Alicja oblicza wartość $m = E(l)$
4	Alicja wysyła Bobowi m (Ewa oczywiście także widzi przesyłaną informację)
5	Bob liczy $D(m)$ i poznaje treść przesyłki Alicji

Wydaje się, że znalezienie w tej sytuacji skutecznej metody szyfrowania chroniącej przesyłane informacje przed niezdrową[5] ciekawością Ewy będzie bardzo trudne.

[3] *Rozszyfrujmy* kilka spraw. Dlaczego Alicja, Bob i Ewa? To proste. Alicja, bo na literę A, Bob bo na literę B, E bo po angielsku *podsłuchiwacz* to *eavesdropper* (a więc na literę E, jak Ewa (*Eve*)). Rozsądnie jest także założyć, że wszystkie przesyłane informacje mogą być śledzone. Czyż nie tak jest gdy wyjmujemy pieniądze z bankomatu lub, w jeszcze większym stopniu, gdy płacimy za zakupy dokonywane za pośrednictwem internetu?

[4] E od angielskiego *encoding*

[5] A przede wszystkiem niebezpieczną dla Alicji i Boba!

Okazuje się, że taka metoda istnieje, choć opiera się na bardzo, na pozór, kruchej podstawie. Tą podstawą jest przekonanie (hipoteza), że nie istnieje skuteczna metoda faktoryzacji liczb naturalnych. Rzeczywiście, choć pomnożenie *ręcznie*, a więc bez użycia komputera dwóch dużych, powiedzmy o 500 pozycjach dziesiętnych liczb, wydaje się czynnością kłopotliwą, wymagającą dużej ilości czasu i papieru, dla komputera jest proste i odbywa się w mgnieniu oka, dając w rezultacie liczbę o 1000 miejscach dziesiętnych. Nawet naszemu domowemu komputerowi taka czynność zajmie mniej niż sekundę. Jeśli jednak odwrócimy zagadnienie, czyli jeśli otrzymamy 1000-pozycyjną liczbę $n = pq$, gdzie p i q są nieznanymi nam liczbami pierwszymi, i zadanie nasze będzie polegało na znalezieniu p i q, to będziemy musieli wykonać liczbę dzieleń (prób) rzędu 10^{500}, co nawet najszybszemu komputerowi zajmie niewyobrażalną ilość czasu[6]. Na dodatek, gdyby wynaleziono komputery o wiele szybsze niż znane do tej pory, wystarczy zwiększyć liczbę cyfr znaczących n z 1000 do 2000 by liczba operacji potrzebnych do znalezienia faktoryzacji wzrosła 10^{1000} krotnie.

Poniżej pokażemy w jaki sposób rozważania na temat złożoności obliczeniowej mnożenia i znajdowania rozkładu liczb na czynniki pierwsze mogą być przydatne w kryptografii.

3.4.1 Metoda Rabina

Metodę szyfrowania Rabina[7] można opisać następująco. Niech n będzie ustaloną, wystarczająco dużą, powiedzmy 300-cyfrową liczbą (okaże się, że celem uniknięcia zniekształcenia informacji l w procesie szyfrowania n musi być dobrane tak, by $l < n$). Funkcją kodującą jest

$$E(l) = l^2 (\mod n)$$

Oznacza to tyle, że Bob prześle Alicji liczbę n i funkcję szyfrującą. Alicja obliczy $l^2 \pmod n$, prześle tę informacje Bobowi. Ewa, podsłuchiwaczka, będzie znała zarówno l^2 jak i n, a jednak, z powodów opisanych wyżej, nie będzie w stanie obliczyć l. Zauważmy. że tak świetnie liczące pierwiastki kalkulatory (czy komputery) są w tej sytuacji zupełnie bezużyteczne. Na przykład gdybyśmy obliczyli przy pomocy kalkulatora $\sqrt{10}$ to otrzymalibyśmy 3.1621..., co nijak ma się do pierwiastka z 10 (mod 13) (dwie liczby dają w kwadracie 10 (mod 13), mianowicie 6 i 7). Jak to jednak możliwe, że Bob będzie w stanie zrobić to, czego nie jest w stanie uczynić Ewa, to znaczy obliczyć l?

1. Bob wybiera dwie duże liczby pierwsze p i q takie, by $p \equiv q \equiv 3 \pmod 4$. Następnie oblicza $n = pq$ i przesyła Alicji (zakładamy, że Ewa widzi przepływ tych informacji).

2. Alicja konwertuje swoją wiadomość w kodzie ASCII otrzymując liczbę l i oblicza $m = l^2 \pmod n$. Następnie przesyła Bobowi m. Ewa widzi m, zna już n, nie umie jednak obliczyć p i q, bo to jest właśnie trudny problem faktoryzacji.

[6] Sam sprawdź. Przyjmij, że jedno dzielenie wymaga 1 mikrosekundy, a dla ułatwienia obliczeń, że minuta ma 100 sekund, doba 100 godzin, rok 1000 dni.

[7] Nazwa od twórcy metody: Michaela Rabina

3. Bob znajduje pierwiastki z m obliczając wpierw $a = m^{\frac{p+1}{4}} \pmod p$, $b = -m^{\frac{p+1}{4}} \pmod p$, $c = m^{\frac{q+1}{4}} \pmod q$ oraz $d = -m^{\frac{q+1}{4}} \pmod q$, a następnie rozwiązując cztery układy równań modularnych:

$$\begin{cases} x \equiv a \pmod p \\ x \equiv c \pmod q \end{cases} \quad \begin{cases} x \equiv a \pmod p \\ x \equiv d \pmod q \end{cases}$$

$$\begin{cases} x \equiv b \pmod p \\ x \equiv c \pmod q \end{cases} \quad \begin{cases} x \equiv b \pmod p \\ x \equiv d \pmod q \end{cases}$$

Układy równań modularnych mają jednoznaczne rozwiązania modulo $n = pq$ dzięki chińskiemu twierdzeniu o resztach. Otrzymamy więc aż cztery rozwiazania, choć wiemy, że dobre jest tylko jedno z nich. To jednak, by wśród rozwiązań odróżnić właściwe będzie dla Boba bardzo proste. Po przejściu z kodu ASCII na litery otrzyma jedną wiadomość sensowną i trzy ciągi znaków nie mających sensu.

Na pierwszy rzut oka może się wydawać, że metoda liczenia pierwiastków wykorzystująca twierdzenie 3.7 nie jest zbyt efektywna. Należy przecież liczyć bardzo wysokie potęgi. Na szczęście okazuje się, ż celem obliczenia k-tej potęgi liczby b wystarczy wykonać liczbę mnożeń, która jest proporcjonalna nie do k a do $\log k$. Przyjrzyjmy się tej sytuacji na przykładzie.

Przykład 3.1 *Policzmy* 7^{12} *(mod* 9*).*
$7^2 = 49 \equiv 4$ *(mod 9)* $\Rightarrow 7^4 \equiv 16 \equiv 7$ *(mod 9)* $\Rightarrow 7^8 \equiv 49 \equiv 4$ *(mod 9)* $\Rightarrow 7^{12} = 7^8 \cdot 7^4 \equiv 4 \cdot 7 = 28 \equiv 1$ *(mod 9)*
Tak więc udało się obliczyć wysoką potęgę liczby 7 *modulo* 9 *wykonując* 5 *mnożeń i bez konieczności operacji arytmetycznych na dużych liczbach.*

3.4.2 Metoda RSA

O ile metoda Rabina wykorzystuje Małe Twierdzenie Fermata, to metoda RSA[8] opiera się na twierdzeniu Eulera. Podobnie jak to było w przypadku opisu metody Rabina załóżmy, że Alicja chce przesłać Bobowi zaszyfrowaną informację $l \in \mathbb{N}$.

Opis metody RSA.

1. Bob:
   (a) Znajduje 2 duże liczby pierwsze p, q, liczy $n = pq$ oraz $\varphi(n) = (p-1)(q-1)$ (także w tym przypadku zakładamy, że $n \geq l$).
   (b) Wybiera (dowolne) $e \in \mathbf{Z}^*_{\varphi(n)}$ (a więc e jest względnie pierwsze z $\varphi(n)$).
   (c) Przesyła Alicji n i e oraz funkcję szyfrującą $E(l) = l^e(\mod n)$.
   (d) Oblicza $d = e^{-1}$ w $\mathbf{Z}^*_{\varphi(n)}$.
2. Ewa: Widzi! Widzi zarówno n jak i e. Wie także jaka jest funkcja szyfrująca.

[8] Nazwa metody od pierwszych liter nazwisk jej twórców: Rivest, Shamir i Adleman.

3. Alicja:
   (a) Liczy $m = l^e \pmod n$
   (b) Wysyła m Bobowi.

Bob: Liczy

$$m^d = (l^e)^d \equiv l \pmod n \tag{3.6}$$

Prawdziwość wzoru 3.7 wymaga uzasadnienia. Oto one.

(a) Przypadek: $l \perp n$. Skoro $ed \equiv 1 \pmod{\varphi(n)}$ mamy: $ed = 1 + k\varphi(n)$ (gdzie n jest pewną liczbą całkowitą. Wówczas możemy wykorzystać twierdzenie Eulera:

$$l^{ed} = l^{1+k\varphi(n)} = l(l^{\varphi(n)})^k \equiv l(\bmod n)$$

(b) Przypadek: l i n nie są względnie pierwsze. Wtedy albo $p|l$ albo $q|l$ (gdyby $p|l$ i $q|l$ to mielibyśmy sprzeczność z założeniem, że $l < n$. Załóżmy, że $p|l$ oraz $q \not| l$.

Mamy teraz: $l^{ed} = l^{1+k(p-1)(q-1)} = l(l^{q-1})^{k(p-1)}$. Ale $q \perp l$ (bo q jest liczbą pierwszą i q nie dzieli l). Wiemy że, $\varphi(q) = q - 1$. A więc $l^{ed} \equiv l \cdot 1^{k(p-1)} = l \pmod q$.

Ostatecznie otrzymaliśmy

$$l^{ed} \equiv l \ (mod\ q)$$

Mamy także

$$l^{ed} \equiv l \ (mod\ p)$$

(bo $l \equiv 0 \pmod p$). Z chińskiego twierdzenia o resztach l jest jedynym modulo $n = pq$ rozwiązaniem układu równań

$$l \equiv m^d \ (mod\ q)$$

$$l \equiv m^d \ (mod\ p)$$

3.5 Zasady kryptografii z kluczem publicznym

Wyobraźmy sobie, że mamy trzy osoby: Alicję, Boba i Ewę. Alicja chce przeslać Bobowi pewne informacje tak, by Ewa (ani nikt inny poza Bobem) nie mógł odgadnąć ich treści mimo, że informacje te przekazywane są w sposób jawny[9]. Warto w tym miejscu zdać sobie sprawę, że każdą informację można traktować jako liczbę. Standardowym zapisem jest powszechnie znany kod ASCII który można z łatwością zdobyć, na przykład za pomocą internetu (w kodzie tym każdemu znakowi odpowiada 3-cyfrowa liczba, *a* to 097, spacja to 032, *o* to 111 itd). Kod ASCII ma jednak oczywistą wadę: wszyscy go znają, a w każdym razie wiedzą jak sie w niego zaopatrzyć. Tak więc Alicja i Bob będą musieli przesyłane dane zaszyfrować (funkcję szyfrującą oznaczać będziemy przez E[10], na dodatek wychodząc z założenia, że wszystkie przesyłane wiadomości są podsłuchiwane (przez Ewę).

Powiedzmy, że Alicja chce zaszyfrować i następnie przesłać Bobowi liczbę naturalną l. By osiągnąć swój cel, Alicja i Bob będą postępowali według następującego schematu:

1	Bob znajduje funkcję szyfrującą (szyfrującą) E oraz rozszyfrującą D, a więc takie by $D(E(l)) = l$
2	Bob przesyła tekstem otwartym (Ewa widzi przekaz) funkcję E Alicji
3	Alicja szyfruje informację którą chce przesłać Bobowi według otrzymanej przez niego instrukcji (tę instrukcje zna także Ewa). Inaczej mówiąc Alicja oblicza wartość $m = E(l)$
4	Alicja wysyła Bobowi m (Ewa oczywiście także widzi przesyłaną informację)
5	Bob liczy $D(m)$ i poznaje treść przesyłki Alicji

Wydaje się, że znalezienie w tej sytuacji skutecznej metody szyfrowania chroniącej przesyłane informacje przed niezdrową[11] ciekawością Ewy będzie bardzo trudne. Okazuje się, że taka metoda istnieje, choć opiera się na bardzo, na pozór, kruchej podstawie. Tą podstawą jest przekonanie (hipoteza), że nie istnieje skuteczna metoda faktoryzacji liczb naturalnych. Rzeczywiście, choć pomnożenie *ręcznie*, a więc bez użycia komputera dwóch dużych, powiedzmy o 500 pozycjach dziesiętnych liczb, wydaje się czynnością kłopotliwą, wymagającą dużej ilości czasu i papieru, dla komputera jest proste i odbywa się w mgnieniu oka, dając w rezultacie liczbę o 1000 miejscach dziesiętnych. Nawet naszemu domowemu komputerowi taka czynność zajmie mniej niż sekundę. Jeśli jednak odwrócimy zagadnienie, czyli jeśli otrzymamy 1000-pozycyjną liczbę $n = pq$, gdzie p i q są nieznanymi nam liczbami pierwszymi,

[9] *Rozszyfrujmy* kilka spraw. Dlaczego Alicja, Bob i Ewa? To proste. Alicja, bo na literę A, Bob bo na literę B, E bo po angielsku *podsłuchiwacz* to *eavesdropper* (a więc na literę E, jak Ewa (*Eve*)). Rozsądnie jest także założyć, że wszystkie przesyłane informacje mogą być śledzone. Czyż nie tak jest gdy wyjmujemy pieniądze z bankomatu lub, w jeszcze większym stopniu, gdy płacimy za zakupy dokonywane za pośrednictwem internetu?

[10] E od angielskiego *encoding*

[11] A przede wszystkiem niebezpieczną dla Alicji i Boba!

i zadanie nasze będzie polegało na znalezieniu p i q, to będziemy musieli wykonać liczbę dzieleń (prób) rzędu 10^{500}, co nawet najszybszemu komputerowi zajmie niewyobrażalną ilość czasu[12]. Na dodatek, gdyby wynaleziono komputery o wiele szybsze niż znane do tej pory, wystarczy zwiększyć liczbę cyfr znaczących n z 1000 do 2000 by liczba operacji potrzebnych do znalezienia faktoryzacji wzrosła 10^{1000} krotnie.

Poniżej pokażemy w jaki sposób rozważania na temat złożoności obliczeniowej mnożenia i znajdowania rozkładu liczb na czynniki pierwsze mogą być przydatne w kryptografii.

3.5.1 Metoda Rabina

Metodę szyfrowania Rabina[13] można opisać następująco. Niech n będzie ustaloną, wystarczająco dużą, powiedzmy 300-cyfrową liczbą (okaże się, że celem uniknięcia zniekształcenia informacji l w procesie szyfrowania n musi być dobrane tak, by $l < n$). Funkcją kodującą jest

$$E(l) = l^2 (\bmod n)$$

Oznacza to tyle, że Bob prześle Alicji liczbę n i funkcję szyfrującą. Alicja obliczy $l^2 \pmod n$, prześle tę informacje Bobowi. Ewa, podsłuchiwaczka, będzie znała zarówno l^2 jak i n, a jednak, z powodów opisanych wyżej, nie będzie w stanie obliczyć l. Zauważmy. że tak świetnie liczące pierwiastki kalkulatory (czy komputery) są w tej sytuacji zupełnie bezużyteczne. Na przykład gdybyśmy obliczyli przy pomocy kalkulatora $\sqrt{10}$ to otrzymalibyśmy 3.1621..., co nijak ma się do pierwiastka z 10 (mod 13) (dwie liczby dają w kwadracie 10 (mod 13), mianowicie 6 i 7). Jak to jednak możliwe, że Bob będzie w stanie zrobić to, czego nie jest w stanie uczynić Ewa, to znaczy obliczyć l?

1. Bob wybiera dwie duże liczby pierwsze p i q takie, by $p \equiv q \equiv 3 \pmod 4$. Następnie oblicza $n = pq$ i przesyła Alicji (zakładamy, że Ewa widzi przepływ tych informacji).

2. Alicja konwertuje swoją wiadomość w kodzie ASCII otrzymując liczbę l i oblicza $m = l^2 \pmod n$. Następnie przesyła Bobowi m. Ewa widzi m, zna już n, nie umie jednak obliczyć p i q, bo to jest właśnie trudny problem faktoryzacji.

3. Bob znajduje pierwiastki z m obliczając wpierw $a = m^{\frac{p+1}{4}} \pmod p$, $b = -m^{\frac{p+1}{4}} \pmod p$, $c = m^{\frac{q+1}{4}} \pmod q$ oraz $d = -m^{\frac{q+1}{4}} \pmod q$, a następnie rozwiązując cztery układy równań modularnych:

$$\begin{cases} x \equiv a \pmod p \\ x \equiv c \pmod q \end{cases} \quad \begin{cases} x \equiv a \pmod p \\ x \equiv d \pmod q \end{cases}$$

$$\begin{cases} x \equiv b \pmod p \\ x \equiv c \pmod q \end{cases} \quad \begin{cases} x \equiv b \pmod p \\ x \equiv d \pmod q \end{cases}$$

[12] Sam sprawdź. Przyjmij, że jedno dzielenie wymaga 1 mikrosekundy, a dla ułatwienia obliczeń, że minuta ma 100 sekund, doba 100 godzin, rok 1000 dni.

[13] Nazwa od twórcy metody: Michaela Rabina

Układy równań modularnych mają jednoznaczne rozwiązania modulo $n = pq$ dzięki chińskiemu twierdzeniu o resztach. Otrzymamy więc aż cztery rozwiazania, choć wiemy, że dobre jest tylko jedno z nich. To jednak, by wśród rozwiązań odróżnić właściwe będzie dla Boba bardzo proste. Po przejściu z kodu ASCII na litery otrzyma jedną wiadomość sensowną i trzy ciągi znaków nie mających sensu.

Na pierwszy rzut oka może się wydawać, że metoda liczenia pierwiastków wykorzystująca twierdzenie 3.7 nie jest zbyt efektywna. Należy przecież liczyć bardzo wysokie potęgi. Na szczęście okazuje się, ż celem obliczenia k-tej potęgi liczby b wystarczy wykonać liczbę mnożeń, która jest proporcjonalna nie do k a do $\log k$. Przyjrzyjmy się tej sytuacji na przykładzie.

Przykład 3.2 *Policzmy* 7^{12} *(mod* 9*).*
$7^2 = 49 \equiv 4$ *(mod 9)* $\Rightarrow 7^4 \equiv 16 \equiv 7$ *(mod 9)* $\Rightarrow 7^8 \equiv 49 \equiv 4$ *(mod 9)* $\Rightarrow 7^{12} = 7^8 \cdot 7^4 \equiv 4 \cdot 7 = 28 \equiv 1$ *(mod 9)*
Tak więc udało się obliczyć wysoką potęgę liczby 7 *modulo* 9 *wykonując* 5 *mnożeń i bez konieczności operacji arytmetycznych na dużych liczbach.*

3.5.2 Metoda RSA

O ile metoda Rabina wykorzystuje Małe Twierdzenie Fermata, to metoda RSA[14] opiera się na twierdzeniu Eulera. Podobnie jak to było w przypadku opisu metody Rabina załóżmy, że Alicja chce przesłać Bobowi zaszyfrowaną informację $l \in \mathbb{N}$.

Opis metody RSA.

1. Bob:
   (a) Znajduje 2 duże liczby pierwsze p, q, liczy $n = pq$ oraz $\varphi(n) = (p-1)(q-1)$ (także w tym przypadku zakładamy, że $n \geq l$).
   (b) Wybiera (dowolne) $e \in \mathbf{Z}^*_{\varphi(n)}$ (a więc e jest względnie pierwsze z $\varphi(n)$).
   (c) Przesyła Alicji n i e oraz funkcję szyfrującą $E(l) = l^e(\mod n)$.
   (d) Oblicza $d = e^{-1}$ w $\mathbf{Z}^*_{\varphi(n)}$.
2. Ewa: Widzi! Widzi zarówno n jak i e. Wie także jaka jest funkcja szyfrująca.
3. Alicja:
   (a) Liczy $m = l^e \pmod n$
   (b) Wysyła m Bobowi.

Bob: Liczy

$$m^d = (l^e)^d \equiv l \pmod n \tag{3.7}$$

Prawdziwość wzoru 3.7 wymaga uzasadnienia. Oto one.

[14] Nazwa metody od pierwszych liter nazwisk jej twórców: Rivest, Shamir i Adleman.

(a) Przypadek: $l \perp n$. Skoro $ed \equiv 1 \pmod{\varphi(n)}$ mamy: $ed = 1 + k\varphi(n)$ (gdzie n jest pewną liczbą całkowitą. Wówczas możemy wykorzystać twierdzenie Eulera:

$$l^{ed} = l^{1+k\varphi(n)} = l(l^{\varphi(n)})^k \equiv l(\bmod\ n)$$

(b) Przypadek: l i n nie są względnie pierwsze. Wtedy albo $p|l$ albo $q|l$ (gdyby $p|l$ i $q|l$ to mielibyśmy sprzeczność z założeniem, że $l < n$. Załóżmy, że $p|l$ oraz $q \not| l$.

Mamy teraz: $l^{ed} = l^{1+k(p-1)(q-1)} = l(l^{q-1})^{k(p-1)}$. Ale $q \perp l$ (bo q jest liczbą pierwszą i q nie dzieli l). Wiemy że, $\varphi(q) = q - 1$. A więc $l^{ed} \equiv l \cdot 1^{k(p-1)} = l \pmod{q}$.

Ostatecznie otrzymaliśmy

$$l^{ed} \equiv l\ (mod\ q)$$

Mamy także

$$l^{ed} \equiv l\ (mod\ p)$$

(bo $l \equiv 0 \pmod{p}$. Z chińskiego twierdzenia o resztach l jest jedynym modulo $n = pq$ rozwiązaniem układu równań

$$l \equiv m^d\ (mod\ q)$$

$$l \equiv m^d\ (mod\ p)$$

Rozdział 4

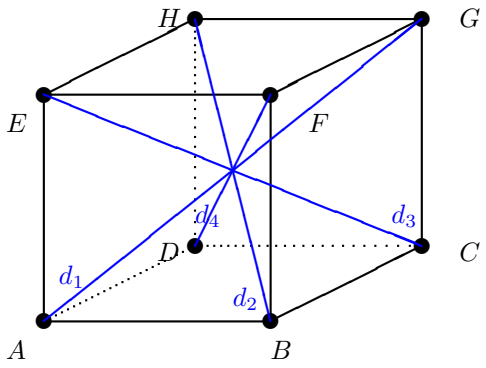
Działanie grupy na zbiorze

Niech G będzie grupą multiplikatywną. Mówimy, że G **działa na zbiorze** X jeśli jest określone odwzorowanie $\rho : G \times X \to X$ spełniające następujące dwa warunki (piszemy $g(x)$ zamiast $\rho(g, x)$):

1. dla dowolnych $g_1, g_2 \in G$ oraz dla każdego $x \in X$ $(g_1 \cdot g_2)(x) = g_1(g_2(x))$
2. dla dowolnego $x \in X$ $e(x) = x$ (gdzie e jest elementem neutralnym grupy G).

Przykład 4.1 Grupa Kleina jest, w oczywisty sposób, grupą działającą na zbiorze $X = \{A, B, C, D\}$ wierzchołków prostokąta.

Przykład 4.2 Grupa obrotów sześcianu.



Przy oznaczeniach jak na rysunku (zaznaczone na niebiesko przekątne wykorzystamy później), elementami grupy będą:

- Obroty wokół osi łączących naprzeciwległe wierzchołki, czyli permutacje (łącznie 8 permutacji):
  $(A)(G)(B, E, D)(C, F, H)$, $(A)(G)(B, D, E)(C, H, F)$,

$(B)(H)(C,F,A)(G,E,D)$, $(B)(H)(A,F,C)(D,E,G)$,
$(C)(E)(B,G,D)(A,F,H)$, $(C)(E)(B,D,G)(A,H,F)$,
$(D)(F)(A,C,H)(E,B,G)$, $(D)(F)(A,H,C)(E,G,B)$.

- Obroty wokół osi łączących środki przeciwległych ścian, czyli permutacje:
  $(A,B,F,E)(D,C,G,H)$, $(A,F)(E,B)(D,G)(C,H)$, $(A,E,F,B)(D,H,G,C)$,
  $(A,E,H,D)(B,F,G,C)$, $(A,H)(E,D)(B,G)(F,C)$, $(A,D,H,E)(B,C,G,F)$,
  $(A,B,C,D)(E,F,G,H)$, $(A,C)(B,D)(E,G)(F,H)$, $(A,D,C,B)(H,G,F,E)$. - tych permutacji jest łącznie 9.

- Sześć obrotów wokół osi łączących środki przeciwległych krawędzi, czyli permutacje:
  $(E,A)(G,C)(F,D)(H,B)$,
  $(F,B)(H,D)(E,C)(A,G)$,
  $(A,B)(H,G)(F,D)(E,C)$,
  $(E,F)(D,C)(A,G)(B,H)$,
  $(E,H)(B,C)(A,G)(D,F)$,
  $(A,D)(F,G)(C,E)(B,H)$

Ponieważ musimy także uwzględnić identyczność $(A)(B)(C)(D)(E)(F)(G)(H)$, grupa obrotów sześcanu jest rzędu 24.

Twierdzenie 4.1 *Jeśli grupa G działa na zbiorze X, $g \in G$, to g jest bijekcją zbioru X.*

Dowód.

- Niech $g \in G$ i niech x i y będą takimi elementami zbioru X, że $g(x) = g(y)$. Wówczas $g^{-1}(g(x)) = g^{-1}(g(y))$ i stąd oraz z pierwszego postulatu definicji działania grupy na zbiorze $(g^{-1} \cdot g)(x) = (g^{-1} \cdot g)(y)$. Mamy więc $e(x) = e(y)$ i na mocy drugiego warunku $x = y$. Dowolny element grupy G jest więc jako funkcja zbioru X w X, injekcją.

- Niech teraz $y \in X$. Zdefiniujmy $x := g^{-1}(y)$. Korzystając z dwóch warunków definicji działania grupy na zbiorze łatwo można sprawdzić, że $y = g(x)$. Dowolny element $g \in G$ jako funkcja działająca na zbiorze X jest więc surjekcją. ■

Dla grupy G działającej na zbiorze X oraz el. $x \in X$ **stabilizatorem** x nazywamy

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

Przykład 4.3 Przyjmując oznaczenia takie, jak w przykładzie 4.2 stabilizatorem elementu A w grupie obrotów sześcianu jest zbiór złożony z trzech permutacji: $\{id_X, (A)(G)(B,E,D)(C,F,H), (A)(G)(B,D,E)(C,H,F)\}$.

Przykład 4.4 Bryłą platońską (inaczej: bryłą foremną), nazywamy bryłę, której wszystkie ściany są wielokątami foremnymi, częścią wspólną dwóch ścian jest albo

zbiór pusty, albo zbiór jednoelementowy - wierzchołek bryły, albo wspólny bok (krawędź wieloboku).
Okazuje się, że istnieje jedynie pięć brył platońskich: czworościan, sześcian, ośmiościan, dwunastościan i dwudziestościan[1]. Siatki brył platońskich są przedstawione na rysunkach. Ich izometrie można traktować jako działania grupy na zbiorach wierzchołków, ścian lub krawędzi (por. zad 4.2).

Twierdzenie 4.2 *Jeśli G jest grupą działającą na zbiorze X, wówczas stabilizator dowolnego elementu $x \in X$ jest podgrupą grupy G.*

Orbitą elementu $x \in X$ nazywamy zbiór

$$\text{Orb } x = \{g(x) : g \in G\}$$

Relacja R określona przez

$$xRy \iff \exists g \in G : \ g(x) = y$$

jest w X równoważnościowa.

Następne twierdzenie (oraz wynikający z niego wniosek 4.4) będziemy wielokrotnie wykorzystywać. Nazwiemy go **twierdzeniem o orbicie i stabilizatorze**.

Twierdzenie 4.3 *Jeśli skończona grupa G działa na zbiorze X, wówczas dla każdego $x \in X$*

$$|\text{Orb } x| = |G : G_x| \tag{4.1}$$

Dowód. Zdefiniujmy funkcję

$$\phi : G : G_x \ni G_x g \to g^{-1}(x) \in \text{Orb } x$$

Udowodnimy, że ϕ jest bijekcją zbiorów $G : G_x$ prawostronnych klas podgrupy G_x na orbitę elementu x i stąd oczywiście będzie wynikała równoliczność zbiorów $G : G_x$ oraz $Orb\ x$.
Nim jednak udowodnimy, że ϕ jest bijekcją wykażemy, że funkcją ϕ jest dobrze określona. Musimy więc udowodnić, że jeśli $g, h \in G$ są takimi elementami, że $G_x g = G_x h$, wówczas $\phi(G_x g) = \phi(G_x h)$. Inaczej mówiąc, że wartość funkcji ϕ nie zależy od tego jakiego reprezentanta warstwy wybierzemy. Dowód można przedstawić jako ciąg implikacji:

$$\begin{array}{rcll} G_x g = G_x h & \Rightarrow & g = f \circ h \text{ dla pewnego } f \in G_x & \text{(pamiętamy, że } e \in G_x) \\ & \Rightarrow & g^{-1} = h^{-1} \cdot f^{-1} & \\ & \Rightarrow & g^{-1}(x) = (f \cdot h)^{-1}(x) & \\ & \Rightarrow & g^{-1}(x) = (h^{-1} \cdot f^{-1})(x) & \\ & \Rightarrow & g^{-1}(x) = h^{-1}(f^{-1}(x)) & \text{(z drugiego warunku} \\ & & & \text{działania grupy na zbiorze)} \end{array}$$

Skoro $f \in G_x$, to także $f^{-1} \in G_x$ a zatem $f^{-1}(x) = x$ i ostatecznie $g^{-1}(x) = h^{-1}(x)$,

[1] Odkrycie tego faktu zawdzięczamy starożytnym Grekom (por. [13]). Hermann Weil w [24] odkrycie dwunastościanu i dwudziestościanu foremnego nazywa *jednym z najpiękniejszych i najbardziej osobliwych odkryć w całej historii matematyki.* Ciekawostką może być, że grupy obrotów brył platońskich znajdują ważne zastosowania w nanofizyce (jako grupy symetrii niektórych fulleroidów). Potwierdza to kilka znanych i lubianych przez matematyków powiedzeń o tym, że jak coś jest ważne, to jest i piękne, a jak piękne to i użyteczne (prędzej czy później).

czyli $\phi(G_x g) = \phi(G_x h$.
Injektywność funkcji ϕ. Przypuśćmy, że $\phi(G_x g) = \phi(G_x h)$. Wówczas $g^{-1}(x) = h^{-1}(x)$, a więc $h \circ g^{-1}(x) = x$, czyli $h \circ g^{-1} \in G_x$, a więc $g \equiv h$ modulo G_x i wobec tego $G_x g = G_x h$.
Surjektywność ϕ. Niech $y \in Orb\ x$. Wówczas istnieje $g \in G$ takie, że $y = g(x)$, czyli $y = (g^{-1})^{-1}(x) = \phi(G_x g^{-1})$. ■

Z wniosku 2.21 i z twierdzenia 4.3 wynika kolejny wniosek.

Wniosek 4.4 *Jeśli skończona grupa G działa na zbiorze X, wówczas dla każdego $x \in X$*

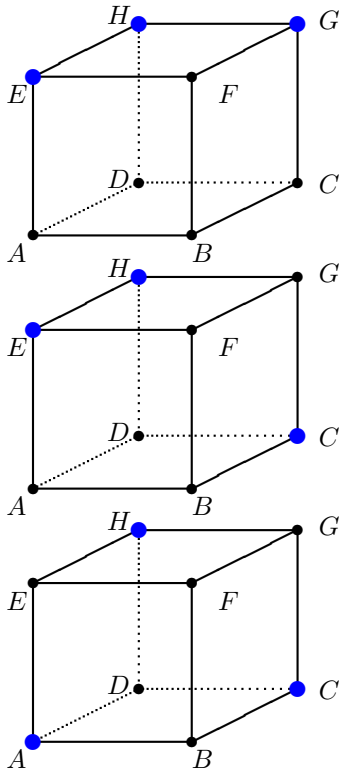
$$|G| = |G_x| \cdot |Orb\ x| \tag{4.2}$$

■

Wniosek 4.4 (lub, co na jedno wychodzi, twierdzenie 4.3) jest ważnym i wielokrotnie wykorzystywanym twierdzeniem teorii grup. Jednym z takich ważnych zastosowań jest lemat Burnside'a, o którym będzie mowa poniżej. Warto zauważyć, że formalnie lewa strona wzoru (4.2) nie zależy od elementu x, zaś prawa tak. To bardzo silna własność polegająca na fakcie, że dla dowolnego elementu $x \in X$ iloczyn $|G_x||Orb\ x|$ przyjmuje taką samą wartość (równą $|G|$).

4.1 Lemat Burnside'a

Bardzo często bywa tak, że chcemy wiedzieć jaka jest liczba istotnie różnych struktur. Dla przykładu, przynajmniej dla pewnych celów, można przyjąć, że jest tylko jeden sześcian, pomijając bowiem wielkość, wszystkie są do siebie podobne. Inaczej jednak będzie, jeżeli będziemy moglo pomalować ściany naszego sześcianu, na przykład dwoma kolorami: czerwonym i niebieskim. Powiedzmy, że interesuje nas, ile jest różnych pokolorowań ścian sześcianu na czerwono i niebiesko tak, by dwie ściany były czerwone, pozostałe zaś cztery niebieskie. Krótka chwila refleksji wystarczy by się przekonać, że są dokładnie dwa takie pokolorowania: w jednym ściany pokolorowane na czerwono są przeciwległe, w drugim zaś sąsiednie.
Nie zawsze jednak musi być aż tak łatwo. Przyjrzyjmy się innemu przykładowi, mianowicie powiedzmy, że dwoma kolorami, czarnym i niebieskim malujemy wierzchołki naszego sześcianu tak, by trzy wierzchołki były niebieskie a pozostałe czarne. Także ten przykład nie jest bardzo trudny, na rysunku widać, że pokolorowań takich są co najmniej trzy, ale czy to już wszystkie?



Trzy różne pokolorowania wierzchołków sześcianu dwoma kolorami

Problemy zliczania nieizomorficznych obiektów pomaga zliczać teoria, której jednym z pierwszych i najważniejszych wyników jest twierdzenie zwane lematem Burnside'a[2].

Dla danej grupy G działającej na zbiorze X oraz $g \in G$ zbiór punktów stałych g oznaczamy przez $Fix\ g$:

$$Fix\ g = \{x \in X : g(x) = x\}$$

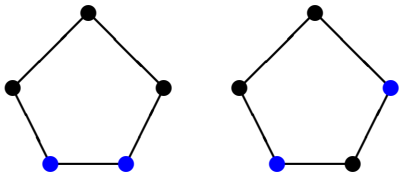
Twierdzenie 4.5 (Lemat Burnside'a) *Niech G będzie grupą skończoną działającą na zbiorze skończonym X. Wówczas liczba N orbit zbioru X ze względu na G wynosi*

$$N = \frac{1}{|G|} \sum_{g \in G} |Fix\ g|$$

[2]William Burnside (1852-1927) był wybitnym matematykiem angielskim. Tak zwany lemat Burnside'a opublikował w swojej książce *Theory of Groups of Finite Order* w 1897 roku zaznaczając, że twierdzenie to zostało udowodnione przez Frobeniusa (1849-1917) 10 lat wcześniej. Niemniej twierdzenie (zwane czasami *Twierdzeniem o przeliczaniu*) związane pozostało z nazwiskiem Burnside'a. Ciekawe, jaką rolę w tym odegrał fakt, że Burnside zapomniał wspomnieć o autorstwie Frobeniusa w drugim wydaniu swojej książki (1911), które stało się na wiele lat podstawową pracą w tej dziedzinie.

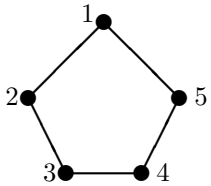
Nim udowodnimy Lemat Burnside'a, przyjrzymy się jeszcze jednemu przykładowi.

Przykład 4.5 *Powiedzmy, że mamy naszyjnik z pięcioma koralikami, z których dwa są niebieskie zaś pozostałe trzy czarne. Problem jest następujący: ile jest istotnie różnych takich naszyjników?*
Dla tylko pięciu koralików problem jest bardzo prosty i jego wszystkie rozwiązania można podać natychmiast, bez wykorzystywania teorii grup. Widać, że są dwa rozwiązania i można je przedstawić na rysunku.



Sprawdźmy jednak, jak zastosować można w naszym przykładzie Lemat Burnside'a.

Nasz naszyjnik to pięciokąt foremny, którego grupę izometri D_5 doskonale znamy. Oznaczmy przez g izometrię odpowiadającą permutacji $g = (1,2,3,4,5)$. Wówczas $D_5 = \{id, g, g^2, g^3, g^4, h, hg, hg^2, hg^3, hg^4\}$, gdzie $h = (1)(2,5)(3,4)$ jest symetrią (oś symetrii przechodzi przez wierzchołek 1 (oczywiście oznaczenia są tu takie, jak na kolejnym rysunku).



Liczba różnych naszyjników, to liczba N orbit.
Rząd grupy równy $D_5 = 10$. Natomiast liczby $|Fix\ g|$ będą różne, w zależności od typu izometrii.

- $|Fix\ id|$: Każdy naszyjnik przechodzi przez identyczność w samego siebie, a wszystkich naszyjników jest tyle, na ile sposobów można ze zbioru $\{1,2,3,4,5\}$ wybrać dwa elementy odpowiadające koralikom niebieskim. Tak więc $|Fix\ id| = \binom{10}{2} = 10$.

- Obroty: Żaden naszyjnik nie przejdzie w siebie przez żaden obrót. Rzeczywiście, na przykład dla obrotu $(1,2,3,4,5)$ zawsze znajdzie się koralik niebieski, po którego lewej stronie będzie koralik czarny. Stąd dla dowolnego obrotu f mamy $|Fix\ f| = 0$.

- Symetrie: Dla każdej symetrii są dokładnie dwa naszyjniki, które przejdą przez tę symetrię w siebie. Na przykład dla symetrii $(1)((2,5)(3,4)$ takimi naszyjnikami są te, które mają nieiebuieskie koraliki na pozycjach 2 i 3 lub na pozycjach 3 i 4. Pamiętamy, że takich symetrii jest 5.

Ze wzoru na liczbę orbit w Lemacie Burnside'a otrzymujemy więc

$$N = \frac{1}{10}(10 + 2 + 2 + 2 + 2 + 2) = \frac{20}{10} = 2$$

a więc wynik, którego się spodziewaliśmy.

Dowód Lematu Burnside'a przeprowadzimy metodą, która w kombinatoryce jest znana pod nazwą *metody podwójnego zliczania*. Ta metoda polega na oczywistej zasadzie, że jeśli liczymy liczność jakiegoś zbioru na dwa sposoby to wynik za każdym razem musi być ten sam (oczywiście zakładamy, że obie metody są poprawne). w. 6 6.11.2012
Policzymy liczbę elementów zbioru

$$S = \{(x, g) \in X \times G : g(x) = x\}$$

Utwórzmy zero-jedynkową macierz $M = (m_{g,x})_{g\in G, x\in X}$ zdefiniowaną wzorem

$$m_{g,x} = \begin{cases} 1 & \text{jeśli } g(x) = x \\ 0 & \text{jeśli } g(x) \neq x \end{cases}$$

O takiej macierzy mówimy, że ma wiersze *indeksowane* elementami zbioru G, zaś kolumny indeksowane elementami zbioru X.
Liczba elementów zbioru S jest oczywiście równa liczbie jedynek w macierzy M. Liczbę tę można obliczyć na dwa sposoby.

Sposób 1. Sumujemy wyrazy w każdym wierszu macierzy S otrzymując dla wiersza o indeksie g

$$\sum_{x\in X} m_{g,x} = |Fix\ g|$$

a następnie liczymy sumę wszystkich wierszy i mamy w wyniku

$$|S| = \sum_{g\in G} |Fix\ g|$$

Sposób 2. Sumujemy wyrazy w każdej z kolumn otrzymując dla kolumny o ideksie x

$$\sum_{g\in G} m_{g,x} = |G_x|$$

i następnie sumujemy po wszystkich $x \in X$ co daje w wyniku

$$|S| = \sum_{x\in X} |G_x|$$

Powiedzmy, że mamy N orbit (rozłącznych i dających w sumie cały zbiór X) $O_1, O_2, ..., O_N$. Możemy teraz napisać

$$\begin{aligned} \sum_{g\in G} |Fix\ g| &= \sum_{x\in X} |G_x| \\ &= \sum_{i=1}^{N} (\sum_{x\in O_i} |G_x|) \end{aligned}$$

Dla każdej z orbit O_i wybierzmy (dokładnie jeden) element $x_i \in O_i$. Skoro, na mocy wniosku 4.4, dla każdego $x \in X$ prawdziwy jest wzór $|G_x| \cdot |Orb\ x| = |G|$, mamy także $|G_x| = |G_{x_i}|$ dla każdego $x \in O_i$. Stąd (i korzystając ponownie z wniosku 4.4) otrzymujemy

$$\begin{aligned} \sum_{g\in G} |Fix\ g| &= \sum_{i=1}^{N} (|O_i| \cdot |G_{x_i}|) \\ &= N \cdot |G| \end{aligned}$$

Co kończy dowód naszego twierdzenia. ■

Przykład 4.6 *(Kontynuacja przykładu w którym kolorowaliśmy wierzchołki sześcianu kolorami czarnym i niebieskim).*
Utwórzmy tabelkę, w której wypiszemy:

- wszystkie typy permutacji grupy działającej na sześcianie (pierwsza kolumna),
- $|Fix\ g|$ - a więc dla każdego typu permutacji liczba sześcianów z trzema wierzchołkami niebieskimi i pozostałymi czarnymi, które przez g przechodzą w siebie, to znaczy: kolory wierzchołków pozostają zachowane (druga kolumna)
- liczbę permutacji danego typu (trzecia kolumna).

Typ permutacji	$\|Fix\ g\|$	liczba permutacji typu
Identyczność	$\binom{8}{3} = 56$	1
Obroty wokół osi łączących wierzchołki przeciwległe	2	8
Obroty wokół osi łączących środki przeciwległych ścian	0	9
Obroty wokół osi łączących środki przeciwległych krawędzi	0	6

Zgodnie z Lematem Burnside'a, liczba N różnych pokolorowań wierzchołków sześcianu, w których trzy wierzchołki są niebieskie a pięć czarnych jest równa

$$N = \frac{1}{21}(1 \cdot 56 + 2 \cdot 8 + 0 \cdot 9 + 6 \cdot 0) = \frac{72}{24} = 3$$

Tak więc na rysunku ze strony 63 przedstawione są wszystkie możliwe, istotnie różne takie pokolorowania.

4.2 Grupa obrotów sześcianu

Twierdzenie 4.6 *Grupa obrotów sześcianu jest izomorficzna z grupą symetryczną* S_4.

Dowód. Oznaczmy przez d_1, d_2, d_3 i d_4 przekątne łączące odpowiednio wierzchołki: A z G, B z H, C z E i D z F (oznaczenia wierzchołków jak w przykładzie 4.1 na str. 63, na rysunku wymienione cztery przekątne narysowane są w kolorze niebieskim).
Niech $\alpha = (ABCD)(EFGH)$ i $\beta = (ADHE)(BCGF)$.
Obroty sześcianu, które do tej pory traktowaliśmy jako elementy grupy G działające na wierzchołkach $A, B, \ldots, H$ możemy także traktować jako elementy G działające na przekątnych d_1, d_2, d_3 i d_4. Wówczas permutacji α odpowiada $\sigma = (d_1 d_2 d_3 d_4)$ zaś β to $\rho = (d_1 d_4 d_2 d_3)$.
Oznaczmy $a = (d_1 d_2 d_3 d_4)$ i $b = (d_1 d_2)(d_3 d_4)$. Czytelnik zechce sprawdzić, że prawdziwe są następujące fakty:

- $|a| = 4$, $|b| = 2$.
- $aba = b$
- $|\{(1), a, a^2, a^3, b, ba, ba^2, ba^3\}| = 8$
  (czyli elementy zbioru $D_4 = \{(1), a, a^2, a^3, b, ba, ba^2, ba^3\}$ są między sobą różne).

D_4 jest więc grupą dihedralną rzędu 8 (por. str. 33). Oczywiście D_4 jest podgrupą grupy obrotów sześcianu.

Mamy $\sigma \circ \rho = (d_1 d_2 d_3 d_4)(d_1 d_4 d_2 d_3) = (d_2 d_4 d_3)$, wobec tego $|\sigma \circ \rho| = 3$. Grupa obrotów sześcianu zawiera więc podgrupę $< \sigma \circ \rho >$ rzędu 3, generowaną przez $\sigma \circ \rho$.
Udowodniliśmy więc, że grupa obrotów sześcianu jest zawarta w grupie izomorficznej z S_4 (każdy jej element jest permutacją zbioru $\{d_1, d_2, d_3, d_4\}$) i zawiera podgrupę rzędu 8 i podgrupę rzędu 3. Liczba elementów grupy obrotów sześcianu jest więc podzielna przez 24. Ponieważ $|S_4| = 24$, to kończy dowód twierdzenia. ■

4.3 Zadania

Zadanie 4.1 Pola szachownicy o wymiarach 4×4 kolorujemy dwoma kolorami: niebieskim i czarnym. Ile jest różnych pokolorowań w których 4 pola są niebieskie a pozostałe czrne, przy założeniu, że

- szachownica jest jednostronna,
- szachownica jest dwustronna.

Zadanie 4.2 Ile jest istotnie różnych pokolorowań ścian ośmiościanu regularnego, w których trzy ściany są niebieskie a pozostałe czarne?
Porównaj otrzymany wynik z przykładem 4.6. Wyjaśnij fakt, że wyniki są identyczne.

Zadanie 4.3 Porównaj kolorowanie ścian dwudziestościanu foremnego z kolorowaniem wierzchołków dwunastościanu foremnego. Ile jest różnych pokolorowań ścian dwunastościanu foremnego, w których 5 ścian jest niebieskich a pozostałe są czarne? Odpowiedz na podobne pytanie dotyczące liczby pokolorowań wierzchołków dwudziestościanu.

Rozdział 5

Skończone grupy abelowe

Niech $H_1, H_2, ..., H_k$ będą grupami. Przez $H_1 \oplus H_2 \oplus ... \oplus H_k$ będziemy oznaczali zbiór $H_1 \times H_2 \times ... \times H_k$ (iloczyn kartezjański zbiorów $H_1, H_2, ..., H_k$) z działaniem określonym wzorem $(x_1, x_2, ..., x_k)(y_1, y_2, ..., y_k) = (x_1y_1, x_2y_2, ..., x_ky_k)$. Oczywiście każde działanie x_iy_i, zapisane tu multiplikatywnie czyli jako mnożenie, jest działniem w odpowiedniej grupie H_i.
Z łatwością można wykazać, że $H_1 \oplus H_2 \oplus ... \oplus H_k$ jest wtedy grupą. Jeśli grupy $H_1, H_2, \ldots, H_k$ są abelowe, wówczas także grupa $H_1 \oplus H_2 \oplus ... \oplus H_k$ jest abelowa (por. zad. **??**). $H_1 \oplus H_2 \oplus ... \oplus H_k$ nazywamy **iloczynem prostym** grup $H_1, H_2, ..., H_k$.
Iloczynem prostym wewnętrznym podgrup $H_1, H_2, ..., H_k$ grupy G nazywamy zbiór $H_1 \cdot H_2 \cdot ... \cdot H_k = \{h_1h_2 \cdot ... \cdot h_k | h_i \in H_i$ gdzie $i = 1, 2, ..., k\}$, o ile $(H_1 \cdot H_2 \cdot ... \cdot H_i) \cap H_{i+1} = \{e\}$ dla wszystkich $i = 1, 2, \ldots k-1$. Zamiast $H_1 \cdot H_2 \cdot ... \cdot H_k$ piszemy wtedy $H_1 \otimes H_2 \otimes ... \otimes H_k$

Definicja iloczynu wewnętrznego k podgrup jest nieco zawiła. Tym bardziej, że dla dwóch podgrup definicja jest bardziej intuicyjna: $H_1 \otimes H_2 = H_1 \cdot H_2$ jeśli $H_1, H_2 \leq G$ i $H_1 \cap H_2 = \{e\}$. Chodzi jednak o to, by prawdziwe było następujące twierdzenie, które wykorzystywać będziemy w dwodzie zasadniczego twierdzenia o skończonych grupach abelowych (twierdzenie 5.4).

Twierdzenie 5.1 *Jeżeli grupa G jest abelowa, $H_i \leq G$ dla $i = 1, 2, ..., k$ oraz $(H_1 \cdot H_2 \cdot ... \cdot H_i) \cap H_{i+1} = \{e\}$ dla $i = 1, 2, ..., k-1$, wówczas grupy $H_1 \oplus H_2 \oplus ... \oplus H_k$ i $H_1 \otimes H_2 \otimes ... \otimes H_k$ są izomorficzne.*

Dowód. Wykażemy wpierw, że jeśli $H_1, H_2, \ldots, H_k \leq G$ oraz $(H_1 \cdot H_2 \cdot ... \cdot H_i) \cap H_{i+1}$ dla wszystkich $i = 1, 2, ..., k-1$, wówczas przedstawienie elementu $H_1 \cdot H_2 \cdot ... \cdot H_k$ w postaci $g_1g_2 \ldots g_k$, gdzie $g_i \in H_i$ dla $i = 1, 2, \ldots, k$ jest jednoznaczne.
Przypuśćmy, że

$$g_1 \cdot g_2 \cdot ... \cdot g_k = h_1 \cdot h_2 \cdot ... \cdot h_k \tag{5.1}$$

przy czym $g_i, h_i \in H_i$ $i = 1, 2, ..., k$. Korzystając z faktu, że grupa G jest abelowa,

otrzymujemy

$$\underbrace{(h_1 g_1^{-1})(h_2 g_2^{-1})...(h_{k-1} g_{k-1}^{-1})}_{\in H_1 \cdot H_2 \cdot ... \cdot H_{k-1}} = \underbrace{h_k^{-1} g_k}_{\in H_k}$$

a stąd, że $h_k^{-1} gk = e$, czyli $h_k = g_k$. Wymnażając obie strony nierówności (5.1) przez g_k^{-1} (jej lewą stronę) i h_k^{-1} (prawą stronę) otrzymujemy

$$g_1 \cdot g_2 \cdot ... \cdot g_{k-1} = h_1 \cdot h_2 \cdot ... \cdot h_{k-1}$$

Powtarzamy poprzednie rozumowanie do ostatniej równości i otrzymujemy $g_{k-1} = h_{k-1}$ a następnie jeszcze $k-2$ krotnie by otrzymać, kolejno: $g_{k-2} = h_{k-2}$, $g_{k-3} = h_{k-3}$, ... , $g_1 = h_1$.
Odwzorowanie

$$f : H_1 \times H_2 \times ... \times H_k \ni (g_1, g_2, ...g_k) \longrightarrow g_1 \cdot g_2 \cdot ... \cdot g_k \in H_1 \cdot H_2 \cdot ... \cdot H_k$$

jest izomorfizmem grupy $H_1 \oplus H_2 \oplus ... \oplus H_k$ na grupę $H_1 \otimes H_2 \otimes ... \otimes H_k$.
Rzeczywiście, fakt, że f jest epimorfizmem grup jest trywialny, natomiast iniektywność f wynika z udowodnionej powyżej jednoznaczności przedstawienia elementu podgrupy $H_1 \cdot ... \cdot H_k$ jako iloczynu $g_1 \cdot ... \cdot g_k$, gdzie $g_i \in G_i$ dla $i = 1, ..., k$. ■

Wniosek 5.2 *Jeśli G jest grupą abelową sończoną, $K \leq G <\ L \leq G$, $K \cap L = \{e\}$ oraz $G = KL$, wówczas $|G| = |K| \cdot |L|$.* ■

Najważniejszym twierdzeniem niniejszego rozdziału jest zasadnicze twierdzenie o skończonych grupach abelowych udowodnione w 1858 roku przez Leopolda Kroneckera. W dowodzie tego twierdzenia wielokrotnie będziemy korzystać z twierdzenia Cauchy'ego dla grup skończonych. Twierdzenie to jest zaprezentowane w rozdziale 6 poświęconym twierdzeniom Sylowa (wniosek 6.4), niemniej wersję tego twierdzenia dla grup abelowych udowodnimy niezależnie, już teraz, by nie stracić okazji do przedstawienia jej nietrudnego i kształcącego dowodu.

5.1 Twierdzenie Cauchy'ego dla grup abelowych

Twierdzenie 5.3 *Niech p będzie liczbą pierwszą. Jeśli G jest skończoną grupą abelową i p dzieli $|G|$, wówczas w G istnieje element rzędu p.*

Dowód. Twierdzenie udowodnimy indukcyjnie, ze względu na rząd grupy G.

- Bardzo łatwo sprawdzić, że twierdzenie jest prawdziwe jeśli $|G| = 2$.
- Przypuśćmy więc, że $|G| > 2$ i twiedzenie jest prawdziwe dla wszystkich grup rzędu mniejszego niż $|G|$.
  Udowodnimy teraz, że w G istnieje element rzędu pierwszego. Rzeczywiście niech $x \neq e$ i niech $|x| = nq$, gdzie q jest pewną liczbą pierwszą. Wówczas

$|x^n| = q$.
Przypuśćmy teraz, że x jest rzędu pierwszego q.
Jeśli $q = p$, to twierdzenie już jest udowodnione. Przypuśćmy więc, że $q \neq p$.
Niech $G' = G/ < x >$. Ponieważ G jest grupą abelową, podgrupa $< x >$ jest normalna i G' jest grupą abelową, $|G'| = |G|/q \ < \ |G|$ i p dzieli rząd grupy G'. Na mocy założenia indukcyjnego istnieje element $y < x > \in G'$ rzędu p. Wtedy $(y < x >)^p = y^p < x > = < x >$ i $y^p \in < x >$. Wobec tego $y^p = e$ lub $|y^p| = q$ (w podgrupie $< x >$ rzędu pierwszego q każdy element poza elementem neutralnym jest rzędu q).
Gdyby rząd y^p był równy q, wówczas mielibyśmy $(y < x >)^q = < x >$. Wtedy p dzieliłoby q - sprzeczność, która kończy dowód. ■

5.2 Zasadnicze twierdzenie o skończonych grupach abelowych

Twierdzenie 5.4 (Zasadnicze twierdzenie o skończonych grupach abelowych) *Każda skończona grupa abelowa G jest izomorficzna z iloczynem prostym grup cyklicznych rzędów będących potęgami liczb pierwszych.*
Co więcej, zarówno liczba czynników w tym iloczynie jak ich rzędy są jednoznacznie wyznaczone przez grupę G.

Przykład 5.1 Funkcjonowanie zasadniczego twierdzenia o skończonych grupach abelowych zilustrujemy na przykładach grup $\mathbb{Z}_{24}^*$ i $\mathbb{Z}_{36}^*$.
Sprawdzimy z którymi iloczynami prostymi grup cyklicznych te grupy są izomorficzne. W badaniach przydają się umiejętności detektywistyczne.

- $|\mathbb{Z}_{24}^*| = 8$ a więc, na mocy twierdzenia 5.4, grupa $\mathbb{Z}_{24}^*$ jest izomorficzna z jedną z grup:
$$\mathbb{Z}_8 \qquad \mathbb{Z}_2 \oplus \mathbb{Z}_4 \qquad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$
Elementami grupy $\mathbb{Z}_{24}^*$ są $1, 5, 7, 11, 13, 17, 19, 23$. Ponieważ rzędem grupy jest 8, jedynymi możliwymi rzędami elementów są $2, 4$ i 8. Po nietrudnych obliczeniach otrzymujemy wynik, który da się łatwo zapisać w tabeli:

element	1	5	7	11	13	17	19	23
rząd	1	2	2	2	2	2	2	2

Jedynie grupa $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ ma wszystkie elementy (poza neutralnym) rzędu 2, stąd $\mathbb{Z}_{24} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

- $|\mathbb{Z}_{36}^*| = 12 = 2^2 \cdot 3$ a więc
$$\mathbb{Z}_{36}^* \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \qquad \text{lub} \qquad \mathbb{Z}_{36}^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$
Można sprawdzić, że elementy $5, 7, 11$ a także $-5 \equiv 31, -7 \equiv 29, -11 \equiv 25$ (wszystkie przystawania modulo 36) są rzędu 6. W $\mathbb{Z}_4 \oplus \mathbb{Z}_3$ tylko dwa elementy są rzędu 6. Stąd
$$\mathbb{Z}_{36}^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

Dowód twierdzenia 5.4 jest trudny i długi. Przedstawimy go w postaci kilku lematów.

Lemat 5.5 *Niech G będzie grupą abelową rzędu kl, gdzie k i l są liczbami naturalnymi, $k \perp l$. Zdefiniujmy zbiory $K = \{x \in G | x^k = e\}$ oraz $L = \{x \in G | x^l = e\}$ Wówczas*

1. *K i L są podgrupami grupy G,*
2. *$G = K \cdot L$,*
3. *$K \cap L = \{e\}$,*
4. *$|K| = k, |L| = l$.*

Dowód.

Ad 1. Łatwo jest sprawdzić, że $K \leq G$ oraz $L \leq G$ (por. zadanie 5.9).

Ad 2. Skoro $k \perp l$, istnieją $s, t \in \mathbb{Z}$ takie, że

$$sk + tl = 1$$

Dla dowolnego $x \in G$ mamy wtedy $x = x^1 = x^{sk+tl} = x^{sk}x^{tl}$.
Z wniosku 2.22 z twierdzenia Lagrange'a: $x^{|G|} = e$ i stąd:

$$(x^{sk})^l = (x^{kl})^s = e^s = e \text{ a więc } x^{sk} \in L$$

Podobnie

$$(x^{tl})^k = (x^{kl})^t = e^t = e \text{ a więc } x^{tl} \in K$$

Otrzymaliśmy więc, że dla dowolnego $x \in G$ istnieją $y \in K, z \in L$ takie, że $x = yz$, a więc $G \subset K \cdot L$. Zawieranie $K \cdot L \subset G$ jest oczywiste, wobec tego $G = K \cdot L$.

Ad 3. Wykażemy, że $K \cap L = \{e\}$.
Niech $x \in K \cap L$. Wówczas $x^k = e = x^l$. Stąd $|x|$ dzieli k i $|x|$ dzieli l (por. zadanie 2.3). Skoro zaś $k \perp l$ mamy $|x| = 1$. Jedynym elementem rzędu 1 jest element neutralny e i wobec tego $x = e$.

Ad 4. Na mocy wniosku 5.2 wiemy, że $kl = |G| = |K \cdot L| = |K| \cdot |L|$.
Biech p będzie dzielnikiem pierwszym liczby k. Wykażemy, że p nie dzieli $|L|$. Gdyby p dzieliło $|L|$ wówczas, na mocy twierdzenia 5.3, do L należałby pewien element rzędu p a więc, na mocy wniosku 2.22 i definicji L, p dzieliłoby l. To zaś sprzeczne z założeniem, że $k \perp l$. Stąd $k = |K|$ a w konsekwencji także $l = |L|$. ■

Z lematu 5.5 i zasady indukcji wynika istnienie rozkładu skończonej grupy abelowej, na iloczyn prosty grup o rzędach będących potęgami różnych liczb pierwszych. Sformułujmy ten wynik w postaci wniosku.

Wniosek 5.6 *Jeśli G jest grupą abelową, $|G| = p_1^{n_1} p_2^{n_2} \cdot ... \cdot p_k^{n_k}$, gdzie $p_1, p_2, ..., p_k$ są różnymi liczbami pierwszymi, $G(p_i) = \{x \in G |\ x^{p_i^{n_i}} = e\}$, wówczas*

$$G = G(p_1) \cdot G(p_2) \cdot ... \cdot G(p_k) \simeq G(p_1) \oplus G(p_2) \oplus ... \oplus G(p_k)$$

przy czym $|G(p_i)| = p_i^{n_i}$ oraz $(G(p_1) \cap G(p_2) \cap ... \cap G(p_i)) \cap G(p_{i+1}) = \{e\}$ dla $i = 1, ..., k-1$.

Lemat 5.7 *Jeśli $a \in G$, gdzie G jest pewną grupą, $|a| = n$, $k \in \mathbb{N}$, wówczas $< a^k > = < a^{\mathrm{NWD(n,k)}} >$.*

Dowód. Oznaczmy przez $d = \mathrm{NWD(k,n)}$ i niech $k = rd$ $(r \in \mathbb{N})$. Ponieważ $a^k = (a^d)^r$, $a^k \in < a^d >$, a więc $< a^k > \subset < a^d >$.
Niech s, t będą tak dobranymi liczbami całkowitymi, że $d = sn + tk$. Wówczas $a^d = a^{sn+tk} = (a^n)^s (a^k)^t = e(a^k)^t \in < a^k >$. Stąd wynika, że $< a^d > = < a^k >$. ■

Lemat 5.8 *Niech G będzie grupą abelową rzędu p^n, gdzie p jest liczbą pierwszą, $n \geq 1$, i niech $a \in G$ będzie elementem największego rzędu w G.*
Wtedy $G \simeq < a > \oplus K$, gdzie K jest pewną podgrupą grupy G.

Dowód (indukcyjny ze względu na rząd grupy G).

Jeżeli $|G| = p$, wówczas, na mocy twierdzenia Cauchy'ego, $G = \{a, a^2, ..., a^p = e\}$ i $G = < a > \oplus < e >$.

Przypuśćmy, że lemat jest prawdziwy dla grafów rzędu p^k gdy $k < n$. Niech a będzie elementem maksymalnego rzędu w G, powiedzmy $|a| = p^m$. Możemy założyć, że $G \neq < a >$ (w przeciwnym przypadku $G = < a > \oplus < e >$ i dowód jest zakończony). Niech $b \in G$ będzie elementem najmniejszego rzędu wśród tych, które nie należą do $< a >$.

Zachodzi wtedy równość: $|b^p| = |b|/p$.

Rzeczywiście, oznaczmy przez p^r rząd elementu b^p. Mamy $e = (b^p)^{p^r} = b^{p^{r+1}}$, skąd wynika, że $|b| \leq p^{r+1} = |b^p| \cdot p$. Gdyby $|b| < p^{r+1}$ to, skoro rząd b jest potęgą p, istniałoby $r' \leq r$ takie, że $b^{p^{r'}} = e$, stąd $(b^p)^{r'-1} = e$ a to sprzeczność z faktem, że rzędem b^p jest p^r.
Ponieważ b jest elementem o najmniejszym rzędzie w zbiorze $G - < a >$ i $|b^p| < |b|$ element $b^p \in < a >$, powiedzmy $b^p = a^i$.
Skoro $|a| = p^m$ i $a^i = b^p$ mamy $b^{p^m} = (a^i)^{p^m} = (a^{p^m})^i = e^i = e$. Stąd $e = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}}$ a więc $|a^i| \leq p^{m-1}$. a^i nie jest więc generatorem $< a >$. Na mocy lematu 5.7 $\mathrm{NWD(p^m, i)} \neq 1$ a więc $p|i$. Możemy więc napisać $i = pj$, gdzie $j \in \mathbb{N}$ i wobec tego $b^p = a^i = a^{pj}$.

Oznaczmy przez $c = a^{-j}b$.
$c \notin < a >$ w przeciwnym przypadku mielibyśmy $b = ca^j \in < a >$, tymczasem wiemy, że $b \notin < a >$).
$c^p = a^{-jp}b^p = a^{-i}b^p = b^{-p}b^p = e$, a więc c jest elementem rzędu p.
Skoro b jest elementem nie należącym do $< a >$ i o najmniejszym rzędzie o tej własności, mamy

$$|b| = p$$

Skoro b jest elementem rzędu pierwszego, dowolny element podgrupy $< b >$, o ile tylko jest różny od e, generuje $< b >$. Wobec faktu, że $b \notin < a >$, jedynym wspólnym elementem podgrup $< a >$ i $< b >$ jest e, czyli

$$< a > \cap < b >= \{e\}$$

Rozważmy teraz grupę ilorazową $G' = G/ < b >$.
Przez $[x]$ będziemy oznaczali klasę elementu x, a więc $[x] = x < b >$.

Udowodnimy, że $|[a]| = |a|$ $(= p^m)$.
Prawdziwa jest nierówność $|[a]| \leq |a|$, bowiem $[a]^{p^m} = (a < b >)^{p^m} = a^{p^m} < b >= =< b >$ (element neutralny w $G/ < b >$).
Gdyby $|[a]| < |a|$, mielibyśmy $[a]^{p^{m-1}} = [e]$, czyli

$$(a < b >)^{p^{m-1}} = a^{p^{m-1}} < b >=< b >$$

a więc $a^{p^{m-1}} \in < a > \cap < b >= \{e\}$ a to sprzeczność z $|a| = p^m$.

Dla dowolnego elementu $c \in G$ zachodzi $|c < b > | \leq |c|$, a więc $[a]$ jest maksymalnego rzędu w G'.
Mamy:

$$|G'| = |G/ < b > | = |G|/p^p$$

a więc

$$|G'| < |G|$$

Na mocy założenia indukcyjnego

$$G' \simeq < [a] > \oplus K'$$

gdzie $K' \leq G'$.

K' jako podgrupa grupy G' jest zbiorem elementów postaci $x < b >$. Oznaczmy przez K zbiór tych wszystkich elementów x, dla których $x < b > \in K'$, czyli

$$K = \{x \in G : x < b > \in K'\}$$

Z łatwością można udowodnić, że $K \leq G$ (zad. 5.15)
Pozostaje nam wykazanie, że $< a > K = G$ i $< a > \cap K = \{e\}$ (co na mocy definicji oznacza, że $< a > K =< a > \otimes K \simeq < a > \oplus K$).

Udowodnimy wpierw, że $< a > \cap K = \{e\}$.
Niech $x \in < a > \cap K$. Wówczas $x = a^\alpha, \alpha \in \mathbb{N}$ a więc $[x] = x < b >= a^\alpha < b > \in <$ $[a] >$.
Z kolei z faktu, że $x \in K$ wynika, że $x < b > \in K'$ a więc $[x] \in K'$
Ostatecznie $[x] \in < [a] > \cap K'$. Z założenia indukcyjnego wiemy jednak, że $< [a] >$ K' jest iloczynem wewnętrznym, czyli $< [a] > \cap K' = [b]$ (pamiętamy, że $[b]$ jest elementem neutralnym w G').
Mamy więc

$$| < a > K| = | < a > ||K| = |[a]| \cdot |K'| \cdot p = |G'|p = |G|$$

(w drugiej z powyższych równości wykorzystaliśmy fakt, że $|[a]| = |a|$ oraz, że z definicji K i K': $K' = K/ < b >$ i $| < b > | = |b| = p$; w trzeciej, że $G' =< [a] > K'$ i $< [a] > \cap K' = \{e\}$). Stąd $< a > K = G$, co kończy dowód lematu. ■

Z lematu 5.8 wynika lemat następujący.

Lemat 5.9 *Każda grupa abelowa rzędu potęgi liczby pierwszej jest iloczynem prostym grup cyklicznych.* ■

Z lematów 5.5 i 5.9 wynika istnienie rozkładu dowolnej skończonej grupy abelowej na sumę prostą grup cyklicznych. Jedyność tego rozkładu udowodnimy jako lemat kolejny.

Lemat 5.10 *Niech G będzie skończoną grupą abelową rzędu będącego potęgą liczby pierwszej. Jeżeli*

$$G = H_1 \oplus H_2 \oplus ... \oplus H_m \text{ oraz}$$

$$G = K_1 \oplus K_2 \oplus ... \oplus K_k$$

gdzie H_i oraz K_j $(i = 1, ..., m,\ j = 1, ..., n)$ są nietrywialnymi grupami cyklicznymi, $|H_1| \geq |H_2| \geq ... \geq |H_m|$ oraz $|K_1| \geq |K_2| \geq ... \geq |K_n|$, wówczas $m = n$ i $|H_i| = |K_i|$ dla wszystkich i.

5.3 Zadania

Zadanie 5.1 Udowodnij, że jeśli G i H są podgrupami pewnej grupy abelowej, $G \cap H = \{e\}$, wówczas $G \oplus H$ także jest grupą.

Zadanie 5.2 Wykaż, że grupa Kleina jest izomorficzna z $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Zadanie 5.3 Wykaż, że dla podgrup G, H i F pewnej grupy przemiennej, spełniających warunek $G \cap H = G \cap F = \{e\}$ takich, że podgrupy H i F są izomorficzne, podgrupy GH i GF także są izomorficzne.

Zadanie 5.4 Podaj rząd elementu a w grupie G.

- $a = (2, 5)$, $G = \mathbb{Z}_4 \oplus \mathbb{Z}_7$,
- $a = ((1, 2)(3, 4, 5), (1, 2, 3, 4))$, $G = S_5 \oplus S_6$.

Zadanie 5.5 Wskaż przykład grupy G i podgrup H_1, H_2 takich, że $H_1 \cdot H_2$ nie jest podgrupą.

Zadanie 5.6 Niech p będzie liczbą pierwszą. p-grupą nazywamy grupę rzędu p^α ($\alpha \in \mathbb{N}$). Udowodnij, że jeśli G jest p-grupą, wówczas

- Każda podgrupa grupy G jest p-podgrupą.
- Dla dowolnej podgrupy normalnej H grupy G grupa ilorazowa G/H jest p-grupą.

Zadanie 5.7 Wykaż, że jeśli G jest skończoną grupą przemienną, $H, F \leq G$, $H \cap F = \{e\}$, wówczas $|H \otimes F| = |H| \cdot |F|$.

Zadanie 5.8 Niech G będzie grupą abelową. Wykaż, że $G^n := \{x^n | x \in G\} \leq G$.

Zadanie 5.9 Wykaż, że dla dowolnego $n \in \mathbb{Z}$ i dla dowolnej grupy abelowej G

$$\{x \in G |\ x^n = e\} \leq G$$

.

Zadanie 5.10 Niech G będzie p-grupą abelową, gdzie p jest pewną liczbą pierwszą. Udowodnij, że $G^p < G$.

Zadanie 5.11 Udowodnij, że jeśli p jest liczbą pierwszą, G grupą, $x \in G$, $x \neq e$ i $x^p = e$ wówczas $|x| = p$.

Zadanie 5.12 (Kwaterniony.) Niech $G = \{\pm 1, \pm i, \pm j, \pm k\}$ będzie zbiorem z działaniem multiplikatywnym określonym wzorami $i^2 = j^2 = k^2 = -1, (-1)i = -i, (-1)j = -j, (-1)k = -k, (-1)^2 = 1, ij = -ji = k, jk = -kj = i, ki = -ik = j$, 1 jest elementem neutralnym.

- Utwórz tablicę Cayleya dla G.
- Wykaż, że G jest grupą (zwaną **grupą kwaternionów** (W. Hamilton 1943)).
- Wykaż, że $H = \{1, -1\}$ jest podgrupą normalną G.
- Skonstruuj tabelę Cayleya grupy G/H. Czy G/H jest izomorficzna z $\mathbb{Z}_4$ lub $\mathbb{Z}_2\mathbb{Z}_2$?

Zadanie 5.13 Udowodnij, ż jeśli H jest normalną podgrupą grupy G i $F \leq G$, to $HF \leq G$.

Zadanie 5.14 Wykaż, że jeśli G jest grupą przemienną, $H, F \leq G, H \cap F = \{e\}$, wówczas $|H \otimes F| = |H| \cdot |F|$.

Zadanie 5.15 Niech G będzie grupą (niekoniecznie abelową) i niech $H \trianglelefteq G$. Udowodnij, że dla dowolnej podgrupy K' grupy G/H zbiór $K = \{g \in G : gH \in K'\}$ jest podgrupą grupy G.

Zadanie 5.16 Znajdź rząd grupy $\mathbb{Z}_{12} \oplus \mathbb{Z}_9 / < (3,5) >$.

Zadanie 5.17 Udowodnij, że iloczyn prosty $G \oplus H$ skończonych grup cyklicznych G i H jest grupą cykliczną wtedy i tylko wtedy gdy rzędy grup G i H są względnie pierwsze.

Wykaż twierdzenie 5.1. Podaj przykład dowodzący, że założenie przemienności jest istotne a więc, że przez opuszczenie tego założenia otrzymujemy zdanie nieprawdziwe.

Zadanie 5.18 Dla grup:

$$\mathbb{Z}_4 \oplus \mathbb{Z}_8 \qquad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \qquad \mathbb{Z}_{32}$$

wskaż podgrupy rzędów 2, 4, 8, 16 i 32.

Zadanie 5.19 Niech p będzie liczbą pierwszą, $k, l \in \mathbb{N}, l \leq k$. Udowodnij, że w $\mathbb{Z}_{p^k}$ element p^{k-l} generuje grupę rzędu p^l.

Zadanie 5.20 Wskaż wszystkie, z dokładnością do izomorfizmu, grupy abelowe rzędu 225.

Zadanie 5.21 Udowodnij, że istnieją dokładnie 2, z dokładnością do izomorfizmu, grupy rzędu 6.

Zadanie 5.22 Wskaż iloczyny proste grup cyklicznych izomorficznych z $\mathbb{Z}_{18}^*$, $\mathbb{Z}_{20}^*$, $\mathbb{Z}_{24}^*$, $\mathbb{Z}_{36}^*$, $\mathbb{Z}_{72}^*$.

Zadanie 5.23 Niech $k, l \in N, (k,l) = 1$. Wykaż, że $Z_k \oplus Z_l$ jest izomorficzna z Z_{kl}.

Zadanie 5.24 Z jakim iloczynem prostym grup cyklicznych jest izomorficzna poniższa skończona grupa abelowa

1. Z_9^*,Z_{15}^*,Z_{20}^*
2. $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ z działaniem mnożenie modulo 65
3. $G = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\}$ z działaniem mnożenia modulo 135
4. $G = \{1, 7, 43, 49, 51, 57, 93, 99, 101, 107, 143, 149, 151, 157, 193, 199\}$ z działaniem mnożenia modulo 200

5. $G = \{1, 4, 11, 14, 16, 19, 26, 29, 31, 34, 41, 44\}$ z działaniem mnożenia modulo 45

Zadanie 5.25 Oblicz liczbę wszystkich (z dokładnością do izomorfizmu) grup abelowych rzędu:

a) 200, b) 125, c) 35, d) 64

Zadanie 5.26 Niech G będzie skończoną grupą abelową taką, że $g \in G \Rightarrow 3g = 0$. Z jakim iloczynem prostym grup cyklicznych grupa G może być izmorficzna?

Zadanie 5.27 Niech $|G| = 120$ będzie grupą abelową taką, że w grupie G nie ma elementów rzędu 4 ani 8. Z jakim iloczynem prostym grup cyklicznych grupa G może być izmorficzna?

Zadanie 5.28 Niech $|G| = 36$ będzie grupą abelową taką, że w grupie G nie ma elementów rzędu 9. Z jakim iloczynem prostym cyklicznych grupa G może być izmorficzna?

Zadanie 5.29 Wykaż, istnieją 4 nieizomorficzne grupy abelowe rzędu 36.

Zadanie 5.30 Wykaż, że każda grupa abelowa rzędu 45 ma element rzędu 15. Czy każda grupa abelowa rzędu 45 ma element rzędu 9?

Zadanie 5.31 Wykaż, że istnieją 2 grupy abelowe rzędu 108 które mają dokładnie 4 podgrupy rzędu 3.

Wykaż, że każda skończona grupa abelowa może być przedstawiona jako iloczyn prosty grup rzędu $n_1, n_2, n_3, ..., n_t$ takich, że n_{i+1} dzieli n_i dla $i = 1, 2, ..., t-1$.

Zadanie 5.32 Element rzędu 2 nazywamy inwolucją. Oblicz liczbę inwolucji w $Z_{16}, Z_8 \oplus Z_4, Z_4 \oplus Z_4, Z_4 \oplus Z_2 \oplus Z_4$

Udowodnij, że liczba inwolucji w dowolnej skończonej grupie abelowej jest postaci $2^t - 1$ dla pewnego $t \in N$

Zadanie 5.33 Niech G będzie skończoną grupą abelową taką, że G ma k inwolucji $\{i_1, i_2, ...i_k\}$. Udowodnij, że

$$\sum_{g \in G} g = \begin{cases} 0, & k \neq 1; \\ i_1, & k = 1. \end{cases}$$

Rozdział 6

Twierdzenia Sylowa

Głównym celem rozdziału jest zaprezentowanie trzech twierdzeń zwanych twierdzeniami Sylowa. Twierdzenia te są uważane za jedne z najważniejszych twierdzeń teorii grup, obok twierdzenia Lagrange'a. Podczas referowania twierdzeń Sylowa wykorzystamy wiadomości o podgrupach normalnych i sprzężeniach, które poznaliśmy w podrozdziałach 2.8 i 2.35. Warto sobie przypomnieć te wiadomości przed czytaniem następnych odrozdziałów, poświęconych twierdzeniom Sylowa.

Zgodnie z twierdzeniem Lagrange'a, Jeśli H jest podgrupą skończonej grupy G, $|H| = k, |G| = n$, wówczas k dzieli n. Można w związku z tym zapytać, czy jeśli rząd n grupy G jest podzielny przez $k \in \mathbb{N}$ to istnieje podgrupa H rzędu k? Okazuje się, że nie musi tak być. Jeśli jednak p jest liczbą pierwszą, wówczas dla dowolnego l naturalnego takiego, że p^l dzieli $|G|$ podgrupa rzędu p^l istnieje. Ten wynik, a także dwa inne, które zostaną podane w tym podrozdziale, zawdzięczamy norweskiemu matematykowi Sylowowi[1], który udowodnił swoje twierdzenie w 1872 roku. Dowód, który tu zostanie przytoczony jest znacznie bardziej współczesny. Został podany w 1959 roku przez Wielanda i korzysta z techniki działania grup na zbiorach.
Uważa się (Cox [8]), że pierwsze twierdzenie Sylowa znane było Ewarystowi Galois[2]. Nie wiadomo, czy Galois twierdzenie to udowodnił, czy też podjrzewał jego prawdziwość.

6.1 Pierwsze twierdzenie Sylowa

Twierdzenie 6.1 *Niech G będzie grupą skończoną a p liczbą pierwszą, $l \in \mathbb{N}$. Jeśli p^l dzieli rząd grupy G wówczas istnieje w G podgrupa rzędu p^l.*

Dowód. Zdefiniujmu zbiór X wzorem

$$X = \{U \subset G : |U| = p^l\}$$

[1] Ludwig Sylow 1832-1918.

[2] Ewaryst Galois 1810-1832 odegrał w historii nauki ogromną rolę. Poświęcona mu notka biograficzna stanowi istatni rozdział niniejszej książki.

Na tak utworzonym zbiorze określmy działanie grupy

$$X \ni U \to gU \in X$$

Przez G_U uznaczmy stabilizator zbioru $U \in X$, a więc

$$G_U = \{g \in G : gU = U\}$$

Przyjmijmy także, że $|G| = p^l m,\ m = p^r w$, przy czym p nie dzieli w (czyli $p \perp w$).

W dowodzie kluczową rolę będzie odgrywał następujący fakt.

Fakt 6.2 *W zbiorze X istnieje taki element V (a więc p^l-elementowy podzbiór zbioru G), że*

$$p^{r+1} \not| \ |G : G_V|$$

Dowód faktu 6.2. Orbitą zbioru $U \in X$ jest

$$Orb\ U = G \cdot U = \{gU : g \in G\} = \{\{g \cdot h : h \in U\} : g \in G\}$$

Zgodnie z twierdzeniem 4.3 o orbicie i stabilizatorze (str. 61)

$$|Orb\ U| = |G : G_U|$$

dla każdego $U \in X$.
Przypuśćmy, że dla każdego $U \in X$ liczba p^{r+1} dzieli $|G : G_U|$. Wówczas p^{r+1} dzieliłoby liczność każdej orbity $|Orb\ U|$, a ponieważ X jest sumą wszystkich orbit, p^{r+1} dzieliłoby liczność zbioru X.

$$|X| = \binom{p^l m}{p^l} = \frac{p^l m(p^l m - 1) \cdot \ldots \cdot (p^l m - i) \cdot \ldots \cdot \ldots \cdot (p^l m - (p^l - 1))}{p^l (p^l - 1) \cdot \ldots \cdot (p^l - i) \cdot \ldots \cdot (p^l - (p^l - 1))}$$

a więc

$$|X| = \binom{p^l m}{p^l} = \frac{m(p^l m - 1) \cdot \ldots \cdot (p^l m - i) \cdot \ldots \cdot \ldots \cdot (p^l m - (p^l - 1))}{(p^l - 1) \cdot \ldots \cdot (p^l - i) \cdot \ldots \cdot (p^l - (p^l - 1))}$$

Zauważmy teraz, że jeśli p^α dzieli czynnik $p^l m - i$ licznika, to $\alpha < l$. Gdyby bowiem $\alpha \geq l$ to także mielibyśmy $p^l \mid p^l - i$ i wobec tego $p^l \mid i$, podczas gdy wiemy, że $i < p^l$. Dla $\alpha < l$ prawdziwa jest równoważność

$$p^\alpha \mid p^l m - i \ \Leftrightarrow\ p^\alpha \mid p^l - i$$

Ostatecznie: gdyby p^{r+1} dzieliło wszystkie indeksy $|G : G_U|$ wówczas p^{r+1} dzieliłoby m, podczas gdy $m = p^r w$, gdzie $p \perp w$. Ta sprzeczność kończy dowód faktu 6.2. □

Konkluzja dowodu twierdzenia 6.1. Niech $V \in X$ będzie zbiorem, którego istnienie gwarantuje fakt 6.2 (czyli takim, że p^{r+1} nie dzieli $|G : G_V|$).

Grupa G jest skończona, mamy więc

$$|G : G_V| = \frac{|G|}{|G_V|} = \frac{p^{l+r}w}{|G_V|}$$

Ponieważ p^{r+1} nie dzieli $|G : G_V|$ i p nie dzieli w, p^l dzieli $|G_V|$. Stąd wynika, że

$$p^l \leq |G_V|$$

Niech $v \in V$. Wtedy $G_V \cdot v \subset V$ a stąd ciąg prostych zależności:

$$|G_V| = |G_V v| \leq |V| = p^l$$

i ostatecznie $|G_V| = p^l$ - szukaną podgrupą rzędu p^l jest stabilizator G_V. ■

6.1.1 Wnioski z pierwszego twierdzenia Sylowa

Niech p będzie liczbą pierwszą. Grupę (lub podgrupę) nazywamy **p-grupą** (*p-podgrupą* jeżeli jej rząd jest potęgą liczby p. Jeżeli p^k dzieli rząd grupy G, powiedzmy, że $|G| = p^k w$, przy czym w nie jest podzielne przez p (inaczej mówiąc k jest maksymalną potęgą p, która dzieli $|G|$), wówczas każdą podgrupę H rzędu p^k nazywamy **p-podgrupą Sylowa** grupy G.
Pierwszym wnioskiem jest twierdzenie, zwane Pierwszym Twierdzeniem Sylowa (twierdzenie 6.1 jest jego mocniejszą wersją[3]).

Wniosek 6.3 *Jeśli p jest liczbą pierwszą dzielącą rząd skończonej grupy G, wówczas istnieje p-podgrupa Sylowa grupy G.*

Jeśli G jest grupą skończoną, której rząd jest podzielny przez liczbę pierwszą p wówczas, na mocy twierdzenia 6.1, istnieje podgrupa H rzędu p. Skoro rząd podgrupy H jest liczbą pierwszą, podgrupa ta nie ma nietrywialnych podgrup (jedynymi podgrupami H jest zbiór składający sie wyłącznie z elementu neutralnego oraz cała grupa H). Ponieważ zaś każdy element $h \in H$ (poza elementem neutralnym) generuje pewną podgrupę H, wobec tego generuje cała podgrupę H, a więc jest rzędu p. W ten oto sposób twierdzenie 6.1 implikuje twierdzenie zwane twierdzeniem Cauchy'ego[4][5]. Twierdzenie to poznaliśmy już wcześniej (strona 70), jednak udowodniliśmy je wtedy tylko dla grup przemiennych.

Wniosek 6.4 (Twierdzenie Cauchy'ego) *Jeśli grupa skończona G jest rzędu podzielnego przez liczbę pierwszą p, wówczas w G istnieje element rzędu p.* ■

[3] Zarówno twierdzenie 6.1 jak wniosek 6.3 bywają nazywane *Pierwszym Twierdzeniem Sylowa*. Nie jest to ani za bardzo logiczne, ani wygodne ale tak jest i pozostaje się z tym faktem pogodzić.

[4] A.L. Cauchy (1789-1857)

[5] Twierdzenie Cauchy'ego jest oczywiście znacznie starsze niż twierdzenie Sylowa. Co więcej, twierdzenie Cauchy'ego jest wykorzystywane w znanym dowodzie Pierwszego Twierdzenia Sylowa pochodzącym od Frobeniusa (1849-1917). Tu podany został dowód twierdzenia 6.1 zaproponowany przez Wielanda.

Ćwiczenie 6.1 *Udowodnij, że istnieją jedynie dwie grupy rzędu* 6*, mianowicie* $\mathbb{Z}_6$ *oraz grupa symetryczna* S_3 *(czyli grupa permutacji zbioru* $\{1,2,3\}$*)* [6]

Przykład 6.1 *Korzystając z ćwiczenia 6.1 wykażemy, że 12-to elementowa grupa permutacji parzystych* $\mathbf{A}_4$ *nie zawiera podgrupy rzędu* 6*, choć* 6 *dzieli jej rząd* 12*. Rzeczywiście, gdyby podgrupa o* 6 *elementach istniała, to zgodnie z ćwiczeniem 6.1 byłaby izomorficzna z* $\mathbb{Z}_6$ *albo z* $\mathbf{S}_3$*. Tymczasem w* $\mathbb{Z}_6$ *istnieje element rzędu* 6*, podczas gdy żadna permutacja* 4 *elementów nie jest rzędu* 6*. Nie może to być także grupa* $\mathbf{S}_3$*, bo w* $\mathbf{S}_3$ *istnieją nieprzemienne elemnty rzędu* 2*, natomiast w* $\mathbf{A}_4$ *są* 3 *elementy rzędu* 2*:* $(1,2)(3,4), (1,3)(2,4)$ *i* $(1,4)(2,3)$*, które są parami przemienne.*

Przykład 6.2 *Jak stwierdziliśmy w przykładzie 4.2, grupa obrotów sześcianu ma* $24 = 3 \cdot 2^3$ *elementów. Wobec tego każda jej* 2*-podgrupa Sylowa ma* $2^3 = 8$ *elementy. Przy oznaczeniach jak w przykładzie 4.2 taką podgrupą jest na przykład podgrupa* $P = \{id, \sigma, \sigma^2, \sigma^3, \tau, \tau\circ\sigma, \tau\circ\sigma^2, \tau\circ\sigma^3\}$*, gdzie* $\sigma = (A,B,C,D)(E,F,G,H)$ *i* $\tau = (A,H)(E,D)(B,G)(F,C)$ *(grupa dihedralna* D_4*).*

6.1.2 Twierdzenie o rozkładzie na orbity

Dla dowolnej grupy G działającej na skończonym zbiorze X przez X_{fix} oznaczmy zbiór tych elementów $x \in X$, dla których $g(x) = x$ dla dowolnego $g \in G$. Inaczej mówiąc X_{fix} jest zbiorem tych elementów zbioru X, które mają orbity jednoelementowe.

Załóżmy, że grupa G i zbiór X są skończone. Oznaczmy przez $x_1, ..., x_n$ takie elementy zbioru X, że

$$X = X_{fix} \cup Orb\ x_1 \cup ... \cup Orb\ x_n \tag{6.1}$$

przy czym

$$X_{fix} \cap Orb\ x_i = \emptyset,\ Orb\ x_i \cap Orb\ x_j = \emptyset \text{ dla } i \neq j$$

($x_1, ..., x_n$ istnieją dzięki temu, że X jest zbiorem skończonym). Rzeczywiście, X jest sumą wszystkich orbit jednoelementowych, czyli składających się na zbiór X_{fix} i pozostałych (a więc orbit więcej niż jednoelementowych, o ile takie istnieją). Z (6.1) wynika natychmiast, że

$$|X| = |X_{fix}| + \sum_{i=1}^{n} |Orb\ x_i|$$

a stąd i z twierdzenia 4.3 otrzymujemy twierdzenie znane jako **twierdzenie o rozkładzie na orbity**. Z twierdzenia tego, następującego po nim lematu i niektórych wniosków będziemy wielokrotnie korzystać.

Twierdzenie 6.5 *Jeśli* G *jest grupą działającą na zbiorze* $X \neq \emptyset$*,* $x_1, ..., x_n \in X$ *są elementami orbit między sobą różnych i więcej niż jednoelementowych, wówczas*

$$|X| = |X_{fix}| + \sum_{i=1}^{n} |G : G_{x_i}| \tag{6.2}$$

[6] Jedyność oznacza tu oczywiście jedyność z dokładnością do izomorfizmu. Dokładniej należałoby powiedzieć, że każde grupa rzędu 6 jest izomorficzna z $\mathbb{Z}_6$ albo z grupą symetryczną $\mathbf{S}_3$.

Wzór (6.2) zwany *wzorem o rozkładzie na orbity* i ma szczególnie ważne konsekwencje gdy G jest p-grupą.

Lemat 6.6 *Jeżeli p jest liczbą pierwszą a G jest p-grupą działającą na zbiorze X, wówczas $|X| - |X_{fix}|$ jest podzielne przez p.*

Dowód lematu 6.6 wynika ze wzoru (6.2). Rzeczywiście, przyjmijmy, że $x_1, ..., x_n$ są wybranymi reprezentantami różnych orbit o licznościach większych od 1. Wiemy, że G jest p-grupą. Wobec tego dla każdego i indeks podgrupy G_{x_i} w G, czyli $|G : G_{x_i}| = \frac{|G|}{|G_{x_i}|} = |Orb\ x_i|$ jest podzielny przez p. Stąd i z (6.2) także $\sum_{i=1}^{n} |G : G_{x_i}| = |X| - |X_{fix}|$ jest podzielne przez p. ■

Twierdzenie 6.7 *Niech $Z(G)$ będzie centrum grupy G. Jeśli grupa $G : Z(G)$ jest cykliczna, wówczas G jest grupą abelową.*

Dowód. Niech $gZ(G)$ będzie generatorem grupy ilorazowej $G : Z(G)$ i niech $a, b \in G$. Istnieją $k, l \in \mathbb{Z}$ takie, że $aZ(G) = g^k Z(G), bZ(G) = g^l Z(G)$. Ponieważ element neutralny należy do $Z(G)$ ($Z(G)$ jest podgrupą G) istnieją $z, z' \in Z(G)$ takie, że $a = g^k z, b = g^l z'$.
Ponieważ g^k komutuje z g^l (to znaczy: $g^k \cdot g^l = g^l \cdot g^k$) a elementy z i z', jako elementy centrum, komutują z każdym elementem grupy G, otrzymujemy

$$ab = (g^k z)(g^l z') = (g^l z')(g^k z) = ba$$

■

Twierdzenie 6.8 *W dowolnej nietrywialnej p-grupie G, gdzie p jest dowolną liczbą pierwszą, w centrum $Z(G)$ są co najmniej dwa elementy.*

Dowód. Nietrudno jest sprawdzić, że $g : G \ni x \to gxg^{-1} \in G$ jest działaniem grupy G na G (por. zad. 6.1). Dla tego działania $G_{fix} = Z(G)$. Z lematu 6.6 wynika więc, że $|G| - |Z(G)|$ jest podzielne przez p. Ponieważ p dzieli $|G|$, $|Z(G)|$ nie może być równe 1. ■

Wniosek 6.9 *Każda grupa G rzędu p^2, gdzie p jest pewną liczbą pierwszą, jest przemienna.*

Dowód. Z twierdzenia Lagrange'a wynika, że $|Z(G)| \in \{1, p, p^2\}$.

- Na mocy twierdzenia 6.8, $|Z(G)| \neq 1$.
- Gdyby $|Z(G)| = p$ wówczas $|G : Z(G)| = p$. Stąd grupa ilorazowa $G : Z(G)$ byłaby cykliczna a więc, na mocy twierdzenia 6.7, G abelowa (stąd jednak $G = Z(G)$ i w konskwencji $|Z(G)| = p^2$).

- Jeśli $|Z(G)| = p^2$ to G jest abelowa na mocy definicji centrum. ■

Następne twierdzenie, interesujące samo dla siebie, wykorzystamy w dowodzie twierdzenia 6.21.

Twierdzenie 6.10 *Jeżeli p jest liczbą pierwszą i $P \leq G$ jest p-podgrupą Sylowa swojego normalizatora, wówczas jest także p-podgrupą Sylowa grupy G.*

W dowodzie[7] twierdzenia 6.10 wykorzystamy następujący lemat.

Lemat 6.11 *Niech p będzie liczbą pierwszą. Jeśli H jest p-podgrupą grupy skończonej G to $|N_G(H) : H| \equiv |G : H| \pmod p$.*

Dowód. Można sprawdzić, że przyporządkowanie zdefiniowane dla każdego dla $a \in H$ wzorem

$$a : G/H \ni Hb \to Hba^{-1} \in G/H$$

jest działaniem podgrupy H na G/H (por. zadanie 6.8). Dla tak określonego działania grupy H na zbiorze G/H fakt, że $Hb \in (G/H)_{fix}$ oznacza, że dla dowolnego $a \in H$ zachodzi $Hba^{-1} = Hb$ a więc $Hbab^{-1} = H$, czyli $bab^{-1} \in H$. Element b jest więc wtedy elementem normalizatora $N_G(H)$, a więc $Hb \in N_G(H) : H$. Na mocy lematu 6.6 $|G/H| - |N_G(H)/H|$ jest podzielne przez p, a więc $|G/H| \equiv |N_G(H)/H| \pmod p$. ■

Konkluzja dowodu twierdzenia 6.10. Jeśli P jest p-podgrupą Sylowa swojego normalizatora $N_G(P)$ to $|N_G(P) : P| \not\equiv 0 \pmod p$ i wobec lematu 6.11 $|G : P| \not\equiv 0 \pmod p$, co oznacza, że P jest p-podgrupą Sylowa grupy G. ■

6.2 Drugie twierdzenie Sylowa

Twierdzenie 6.12 (Drugie Twierdzenie Sylowa) *Jeśli P jest p-podgrupą Sylowa grupy skończonej G zaś H jest p-podgrupą grupy G, wówczas*

$$H \subset gPg^{-1}$$

dla pewnego $g \in G$.

Dowód. Niech $X = \{gP : g \in G\}$. Podgrupa H działa na X w następujący sposób.

$$H \ni h : X \ni gP \longrightarrow h \cdot gP \in X$$

Elementy zbioru X to klasy lewostronne modulo podgrupa P. Ponieważ P jest p-podgrupą Sylowa grupy G, możemy napisać $|P| = p^l$ oraz $|G| = p^l w$, gdzie $p \perp w$.

[7] Dowód ten zawdzięczam profesorowi Kazimierzowi Szymiczkowi.

Zauważmy, że zbiór X jako zbiór lewostronnych klas przystawania modulo podgrupa P jest równoliczny ze zbiorem prawostronnych klas a więc mamy

$$|X| = |G : P| = w$$

i wobec tego $|X|$ nie jest podzielne przez p.
Elementy zbioru X są postaci $g_1 \cdot P, g_2 \cdot P, ..., g_w \cdot P$, gdzie $g_1, g_2, ..., g_w$ są stosownie dobranymi elementami G (*stosownie dobrane* oznacza tu, że $g_i \cdot P \cap g_j \cdot P = \emptyset$ dla $i \neq j$).

Zastosujmy lemat 6.6 do naszej sytuacji (czyli sytuacji takiej, że mamy p-grupę H działającą na zbiór klas X i $|Orb\ g_i \cdot P| = \frac{|H|}{|H_{g_i \cdot P}|}$). Skoro $|X|$ jest niepodzielne przez p i $|X| - |X_{fix}|$ jest podzielne przez p liczba $|X_{fix}|$ jest niepodzielna przez p. W szczególności $X_{fix} \neq \emptyset$.
Niech $g \cdot P \in X_{fix}$ $(g \in G)$. Oznacza to dokładnie tyle, że

$$hg \cdot P = g \cdot P \text{ dla wszystkich } h \in H$$

a wobec tego $g^{-1}hg \in P$ dla wszystkich $h \in H$, czyli $g^{-1}Hg \subset P$, co można inaczej zapisać $H \subset gPg^{-1}$. ■

Przykład 6.3 *Kontynuujmy przykłady 4.2 i 6.2. Jedną z 2-podgrup obrotów sześcianu jest*

$$Q = \{id, (A,B,F,E)(D,C,G,H), (A,F)(E,B)(D,G)(C,H),$$

$$(A,E,F,B)(D,H,G,C)\}$$

zbiór obrotów wokół osi przechodzącej przez środki ścian $ABFE$ i $DCGH$. W przykładzie 6.2 widzieliśmy, że jedną z 2-podgrup Sylowa wszystkich obrotów sześcianu jest $P = \{id, \sigma, \sigma^2, \sigma^3, \tau, \sigma \circ \tau, \tau \circ \sigma, \tau \circ \sigma^2\}$, gdzie $\sigma = (A,B,C,D)(E,F,G,H)$ i $\tau = (A,H)(E,D)(B,G)(F,C)$. Dla permutacji $\rho = (A,D,H,E)(B,C,G,F)$ mamy $Q \subset \rho P \rho^{-1}$.

6.3 Wnioski z Drugiego Twierdzenia Sylowa

Twierdzenie Sylowa z 1872 jest dość oczywistym wnioskiem z twierdzenia 6.12.

Wniosek 6.13 (Sylow) *Dowolne dwie p-podgrupy Sylowa grupy skończonej są sprzężone.* ■

Stąd łatwo wynika następny wniosek.

Wniosek 6.14 *p-podgrupa Sylowa grupy skończonej jest normalna wtedy i tylko wtedy gdy jest jedyna.* ■

Jeśli P jest p-podgrupą Sylowa pewnej grupy skończonej (gdzie p jest liczbą pierwszą), wówczas dla dowolnego elementu g grupy także gPg^{-1} jest p-podgrupą Sylowa. Stąd i z twierdzenia 6.12 wynika natychmiast następujący wniosek.

Wniosek 6.15 *Jeśli p jest liczbą pierwszą, wówczas każda p-podgrupa grupy skończonej G jest zawarta w pewnej p-podgrupie Sylowa grupy G.* ■

6.4 Trzecie twierdzenie Sylowa

Istotą drugiego twierdzenia Sylowa jest fakt, że dowolne p-podgrupy H_1 i H_2 grupy skończonej G takie, że $|H_1| = |H_2|$ są sprzężone, w trzecim twierdzeniu Sylowa mowa jest o liczbie różnych p-podgrup Sylowa.

Twierdzenie 6.16 (Trzecie Twierdzenie Sylowa) *Niech p będzie liczbą pierwszą, G grupą skończoną, $|G| = p^l w, l \geq 1, w \perp p$.*
Oznaczmy przez n_p liczbę p-podgrup Sylowa grupy G. Wówczas

1. $n_p = |G : N_G(P)|$, *gdzie P jest dowolną p-podgrupą Sylowa grupy G.*
2. $n_p \equiv 1 \pmod p$
3. $n_p \mid w$

Dowód. Punkt pierwszy twierdzenia wynika natychmiast z drugiego twierdzenia Sylowa i twierdzenia 2.38.
Wykażemy, że $n_p \equiv 1 \pmod p$.
Niech X oznacza zbiór wszystkich p-podgrup Sylowa grupy G i niech P będzie ustaloną podgrupą Sylowa grupy G. Bardzo łatwo sprawdzić, że

$$P \ni g : X \ni Q \longrightarrow gQg^{-1}$$

jest działaniem grupy P na zbiorze X. Dla tego działania

$$X_{fix} = \{Q : Q \text{ jest } p\text{-podgrupą Sylowa grupy } G \text{ i } gQg^{-1} = Q \text{ dla każdego } g \in P\}$$

Skoro P jest p-podgrupą Sylowa (a więc także p-grupą), na mocy lematu 6.6 mamy

$$n_p = |X| \equiv |X_{fix}| \pmod p$$

Oczywiście prawdą jest, że $P \in X_{fix}$. Wykażemy, że P jest jedynym elementem zbioru X_{fix}, czyli $X_{fix} = \{P\}$, co zakończy dowód części drugiej twierdzenia.
Przypuśćmy, że Q jest p-podgrupą i $Q \in X_{fix}$. Wtedy $P \subset N_G(Q)$ i wobec tego $P \leq N_G(Q)$ (P jest podgrupą grupy $N_G(Q)$). Wiemy także, że Q jest podgrupą normalną swojego normalizatora (twierdzenie 2.37). Co więcej, grupy P i Q są p-podgrupami Sylowa grupy $N_G(Q)$ mają bowiem rząd maksymalny podzielny przez p. Korzystając z wniosku 6.14 otrzymujemy $P = Q$.

W dowodzie trzeciej części twierdzenia, wykorzystamy udowodnione już dwa punkty twierdzenia. Skoro $n_p = |G : N_G(P)| = |G|/|N_G(P)|$, gdzie P jest pewną p-podgrupą Sylowa grupy G, n_p dzieli $|G|$. Wiemy jednak, że $|G| = p^l w$, gdzie $p \perp w$. Na dodatek $n_p \perp p$ (bo $n_p \equiv 1 \pmod p$). Stąd $n_p \mid w$. ■

6.5 Wnioski z twierdzeń Sylowa

Poniżej użyteczne wnioski, które wynikają z co najmniej dwóch twierdzeń Sylowa.

Wniosek 6.17 *Jeśli G jest grupą rzędu pq, gdzie p i q są liczbami pierwszymi, $p < q$ oraz p nie dzieli $q - 1$, wówczas G jest cykliczna (a zatem izomorficzna z $\mathbb{Z}_{pq}$).*

Dowód. Na mocy pierwszego twierdzenia Sylowa, w G istnieją p-podgrupa Sylowa H i q-podgrupa Sylowa K. Niech, podobnie jak to zdefiniowano w trzecim twierdzeniu Sylowa, n_p oznacza liczbę p-podgrup Sylowa, zaś n_q liczbę q-podgrup Sylowa w G.

Na mocy trzeciego twierdzenia Sylowa, $n_p = 1 + kp$, gdzie $k \in \mathbb{N}$ oraz (punkt (3) tego twierdzenia) $n_p|q$. Skoro jednak q jest liczbą pierwszą wynika stąd , że $n_p = 1$ lub $n_p = q$.

Gdyby $n_p = q$ wówczas $q = 1 + kp$ a stąd $p|(q-1)$, sprzeczność z założeniem. Tak więc $n_p = 1$.

Dalej, z trzeciego twierdzenia Sylowa, $n_q = 1 + lq$, gdzie $l \in \mathbb{N}$, oraz $n_q|p$. Stąd $n_q = 1$ lub $n_q = p$. Gdyby $n_q = p$ to mielibyśmy $1 + lq = p$, a skoro $p < q$ to $l = 0$. Wykazaliśmy więc, że także $n_q = 1$.

Na mocy wniosku 6.14 podgrupy H i K są normalne. Skoro ich rzędy są liczbami pierwszymi, podgrupy te są cykliczne. Powiedzmy, że $H =< x >$, $K =< y >$. Wykażemy, że $xy = yx$. Rzeczywiście:

$$xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in Ky^{-1} = K$$

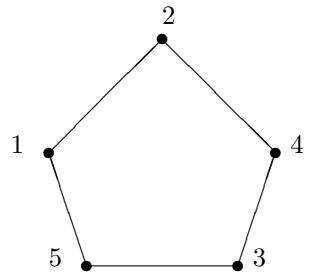
$$xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in xH = H$$

Stąd $xyx^{-1}y^{-1} \in K \cap H = \{e\}$ i wobec tego $xyx^{-1}y^{-1} = e$, skąd już łatwo wynika, że $xy = yx$. Wobec tego $|xy| = |x||y| = pq$, co oznacza, że element xy jest generatorem G. ■

Przykład 6.4 Rząd 6 jest co prawda iloczynem dwóch liczb pierwszych $p = 2$ i $q = q$, niemniej nie jest spełnione założenie, że $p \not| (q-1)$ i rzeczywiście, jedną z dwóch grup rzędu 6 jest S_3, która nie tylko nie jest cykliczna, ale także jest nieprzemienna.

Z wniosku 6.17 wynika natychmiast wniosek następujący.

Wniosek 6.18 *Każda grupa rzędu* 15 *jest cykliczna.* ■



Rysunek 6.1: $\Gamma = (\{1,2,3,4,5\}; \{\{1,2\},\{2,4\},\{3,4\},\{3,5\},\{1,5\}\})$

6.6 Zastosowanie w matematyce dyskretnej

Poniżej pewne zastosowanie twierdzeń Sylowa w teorii grafów.

6.6.1 Grafy samodopełniające

Grafem nazywamy parę $\Gamma = (V; E)$, gdzie V jest dowolnym zbiorem, zaś E pewnym podzbiorem dwuelementowych podzbiorów zbioru V. Elementy zbioru V nazywamy **wierzchołkami** grafu, natomiast elementy zbioru E **krawędziami**[8] grafu Γ. Grafy, które tu będą rozważane będą grafami skończonymi to jest takimi, że ich zbiory wierzchołków będą skończone.
Grafy mają bardzo prostą i wygodną interpretację geometryczną. Wierzchołki grafu interpretujemy jako punkty na płaszczyźnie, natomiast krawędzie $\{x, y\}$ jako krzywe łączące wierzchołki x z y.

Twierdzenie 6.19 *Jeśli σ jest antymorfizmem grafu samodopełniającego wierzchołkowo przechodniego, wówczas każdy cykl tej permutacji (w rozkładzie σ na cykle rozłączne) ma długość podzielną przez 4, poza jednym cyklem długości 1 (punkt stały σ).*

Wniosek 6.20 *Jeśli Γ jest grafem samodopełniającym i regularnym, wówczas $|\Gamma| \equiv 1(\mod 4)$.*

6.6.2 Twierdzenie Muzychuka

Twierdzenie 6.21 *Jeśli Γ iest wierzchołkowo przechodnim grafem samodopełniającym, $|\Gamma| = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, gdzie $p_1, \ldots, p_s$ są różnymi liczbami pierwszymi, wówczas*

$$p_i^{\alpha_i} \equiv 1(\mod 4)$$

[8] Inaczej mówiąc $E \subset \{\{x, y\} : x, y \in V, x \neq y\}$. Skoro piszemy, że E jest zbiorem dwuelemntowych podzbiorów V to jasne jest, że zbiory jednoelementowe krawędziami (w sensie tu podanej definicji grafu) nie są.

Twierdzenie 6.21 wynika z wniosku 6.20 oraz następującego lematu.

Lemat 6.22 *Niech $\Gamma = (V; E)$ będzie grafem samodopełniającym i wierzchołkowo przechodnim. Jeżeli p jest liczbą pierwszą, $|\Gamma| = p^m w$, gdzie $p \perp w$, wówczas istnieje zbiór $W \subset V, |W| = p^m$ taki, że graf $(W; E \cap \binom{W}{2})$ jest samodopełniającym grafem wierzchołkowo przechodnim.*

Dowód. Oznaczmy przez $G = \mathrm{Aut}(\Gamma)$ grupę automorfizmów grafu Γ, to znaczy zbiór permutacji g zbioru $V(\Gamma)$ takich, że dla dowolnych dwóch wierzchołków $u, v \in V(\Gamma)$ zachodzi: $uv \in E(\Gamma) \Leftrightarrow g(u)g(v) \in E(\Gamma)$. Przez $\mathrm{Anty}(\Gamma)$ oznaczmy zbiór **antymorfizmów grafu** Γ, to znaczy taki zbiór permutacji σ zbioru wierzchołków $V(\Gamma)$, że $uv \in E(\Gamma) \Leftrightarrow \sigma(u)\sigma(v) \notin E(\Gamma)$.

FAKT 1 $Anty(\Gamma) \cup Aut(\Gamma) \leq S(V)$

Niech $n, b \in \mathbb{N}$ będą takie, że $|G| = p^n b$ i $b \perp p$.

FAKT 2 $m \leq n \ i \ \forall v \in V \ |G_v| = p^{n-m} c, c \perp p$

Dla p-podgrupy grupy G oznaczmy przez

$$c(P) = \{\sigma \in \mathrm{Anty}(\Gamma) : \sigma P \sigma^{-1} = P \wedge |P_{\varphi(\sigma)}| = p^{n-m}\}$$

gdzie $\varphi(\sigma$jest punktem stałym permutacji σ.
Przez $\mathcal{P}$ oznaczamy zbiór (rodzinę) tych p-podgrup $P \leq G$, dla których $c(P) \neq \emptyset$.

FAKT 3 $\mathcal{P} \neq \emptyset$

Od tej chwili do końca dowodu P oznacza p-podgrupę G taką, że

1. $c(P) \neq \emptyset$ oraz
2. P jest maksymalną (ze względu na zawieranie) p-podgrupą grupy G z tą własnością.

Także σ jest od teraz nie dowolną, ale taką permutacją w $\mathrm{Anty}(\Gamma)$, że $\sigma P \sigma^{-1} = P$ i $|P_{\varphi(\sigma|}| = p^{n-m}$ (a więc są spełnione warunki definiujące $c(P)$). Oznaczmy przez K normalizator podgrupy P w G, to znaczy $K = N_G(P) = \{x \in G : xPx^{-1} = P\}$.

FAKT 4 $\sigma K \sigma^{-1} = K$

Przez $\tilde{P}$ oznaczmy p-podgrupę Sylowa K.

FAKT 5 $P \lhd \tilde{P}$

FAKT 6 $\sigma \tilde{P} \sigma^{-1}$ *jest p-podgrupą Sylowa K.*

Z drugiego twierdzenia Sylowa wynika, że istnieje $k \in K$ spełniające $\sigma \tilde{P} \sigma^{-1} = k \tilde{P} k^{-1}$ a więc $(k^{-1}\sigma)\tilde{P}(k^{-1}\sigma)^{-1} = \tilde{P}$. Oznaczmy przez $\tilde{\sigma} = k^{-1}\sigma$.

FAKT 7 $\tilde{\sigma} \in c(\tilde{P})$

Wobec definicji $\tilde{\sigma}$, dla **dowodu faktu 7** wystarczy wykazać, że $|\tilde{P}_{\varphi(\tilde{\sigma})}| = p^{n-m}$. Oznaczmy przez $\Delta = |[k(\varphi(\sigma)) : k \in K\} = K(\varphi(\sigma))$.

7.1. $\sigma(\Delta) = \Delta$

Udowodnimy wpierw zawieranie $\sigma(\Delta) \subset \Delta$.
$a \in \sigma(\Delta) \Rightarrow a = \sigma(f(\varphi(\sigma))), f \in K$
$\overset{Fakt\ 4}{\Longrightarrow} a = \sigma(\sigma^{-1}g\sigma(\varphi)\sigma)), g \in K$
$\Rightarrow a = g(\varphi(\sigma)) \in \Delta$
$\Rightarrow \sigma(\Delta) \subset \Delta$.
Zawieranie $\Delta \subset \sigma(\Delta)$ wynika z faktu, że powyższe wynikania są, jak łatwo stwierdzić, równoważnościami[9]

7.2. $|\Delta| \equiv 1(\mod 4)$

Rzeczywiście, jeśli pewien element u należy do Δ, to na mocy 7.1 także wszystkie elementy cyklu permutacji σ, do którego należy u także należą do tegoż cyklu[10]. Wszystkie cykle permutacji σ są długości przystającej do zera modulo 4 poza dokładnie jednym cyklem długości 1 składającym się z wierzchołka $\varphi(\sigma)$ - stąd już wynika równość 7.2.

7.3. $\tilde{\sigma}(\Delta) = \Delta$

Rzeczywiście: $\tilde{\sigma}(\Delta) = k^{-1}(\sigma(\Delta)) \overset{7.1}{=} k^{-1}(\Delta) = \{k^{-1}(g(\varphi(\sigma)) : g \in K\} \overset{k^{-1}g \in K}{=} \{f(\varphi(\sigma)) : f \in K\} = \Delta$.

7.4. $\varphi(\tilde{\sigma}) \in \Delta$.

Z 7.2 wiemy, że $\Delta| \equiv 1(\mod 4)$. Z kolei z 7.3 wiemy, że $\tilde{\sigma}(\Delta) = \Delta$, a więc Δ musi zawierać punkt stały $\varphi(\tilde{\sigma})$, element jedynego cyklu długości 1 permutacji $\tilde{\sigma}$ (która także jest antymorfizmem naszego grafu Γ, a więc ma wszystkie cykle podzielne przez 4 poza jednym, długości 1).

7.5. Istnieje $l \in K$ takie, że $lP_{\varphi(\sigma)}l^{-1} \leq G_{\varphi(\tilde{\sigma})}$

Teraz jesteśmy już gotowi do udowodnienia faktu 7 (pozostaje nam wykazać, że $|\tilde{P}_{\varphi(\tilde{\sigma})}| = p^{n-m}$).
Niech $l \in K$ będzie takie, że $lP_{\varphi(\sigma)}l^{-1} \leq G_{\varphi(\tilde{\sigma})}$ (istnienie l spełniającego ten warunek gwarantuje nam 7.5). Mamy wtedy

$$lP_{\varphi(\sigma)}l^{-1} \leq lPl^{-1} = P$$

bo l należy do K - normalizatora P. Stąd zaś wynika, że

$$lP_{\varphi(\sigma)}l^{-1} \leq P_{\varphi(\tilde{\sigma})}$$

[9] Innym sposobem przekonania się, że mamy nie tylko zawieranie $\sigma(\Delta) \subset \Delta$, ale równość zbiorów jest zauważenie, że zbiory Δ i $\sigma(\Delta)$ są równoliczne ($\sigma : \Delta \ni v \to \sigma(v) \in \sigma(\Delta)$ jest bijekcją).

[10] Można bardziej szczegółowo wyjaśnić to tak: powiedzmy $u = u_1$ jest elemetem cyklu $(u_1, u_2, ..., u_l)$ permutacji σ (w rozkładzie σ na cykle rozłączne). Skoro $\sigma(\Delta) = \Delta$, $\sigma(u_1) = u_2 \in \Delta$. Na tej samej zasadzie $\sigma(u_2) = u_3 \in \Delta$ i tak dalej, aż dojdziemy do $u_l \in \Delta$.

a wobec tego

$$p^{n-m} \stackrel{P\in\mathcal{P}}{=} |lP_{\varphi(\sigma)}l^{-1}| \leq |P_{\varphi(\tilde{\sigma})}|$$

Pamiętamy jednak, że p^{n-m} jest rzędem p-podgrupy Sylowa $G_{\varphi(\tilde{\sigma})}$ (fakt 2), czyli

$$p^{n-m} = |P_{\varphi(\tilde{\sigma})}|$$

co kończy dowód faktu 7. □

FAKT 8 $\tilde{P} = P$

Rzeczywiście, z założenia P jest maksymalnym ze względu na zawieranie elementem w $\mathcal{P}$. Wiemy także, że $P \lhd \tilde{P}$ (fakt 5) a także $\tilde{P} \in \mathcal{P}$ (z faktu 7). Stąd wynika oczywiście równość $P = \tilde{P}$. □

FAKT 9 *P jest p-podgrupą Sylowa grupy G.*

Fakt 9 wynika z faktu 8 oraz stąd, że jeśli p-podgrupa P grupy G jest p-podgrupą Sylowa swojego normalizatora, wówczas P jest p-podgrupą sylowa grupy G (twierdzenie 6.10). □

Niech $W := \varphi(\sigma) = \{g(\varphi(\sigma)) : g \in P\}$.

FAKT 10 $\sigma(W) = W$

Rzeczywiście:

$$\begin{array}{rcl} \sigma(W) & = & \{\sigma f(\varphi(\sigma)) : f \in P\} \\ & \stackrel{\sigma^{-1}P\sigma=P}{=} & \{\sigma(\sigma^{-1}g\sigma)(\varphi(\sigma)) : g \in P\} \\ & = & \{g(\varphi(\sigma)) : g \in P\} = W \end{array}$$

□

FAKT 11 *Grupa P jest przechodnia na zbiorze W. $|W| \equiv 1(\mod 4)$.*

Niech $u, v \in W$. Powiedzmy $u = g_1(\varphi(\sigma))$, $v = g_2(\varphi(\sigma))$. Wtedy $v = g_2 \cdot g^{-1}(u)$. Równość $|W| \equiv 1(\mod 4)$ wynika z faktu 10. Rzeczywiście, jeśli jakiś element v należy do pewnego cyklu c permutacji σ, wówczas, na mocy faktu 10, wszystkie wierzchołki cyklu c należą do zbioru W. Wiemy zaś (twierdzenie 6.19), że długości tych cykli, poza jednym cyklem długości 1, są podzielne przez 4. Co więcej, ponieważ $id_V \in P$, $\varphi(\sigma) \in W$. Fakt 11 został w ten sposób udowodniony. □

Finał dowodu twierdzenia Muzychuka. Z faktu 9 $|P| = p^n$. Z kolei z twierdzenia o orbicie i stabilizatorze i z faktu 11 mamy:

$$1 \equiv |W| = |\mathrm{Orb}_P\varphi(\sigma)| = \frac{|P|}{P_{\varphi(\sigma)}|} = \frac{p^n}{p^{n-m}} = p^m$$

■

6.7 Zadania

Zadanie 6.1 Wykaż, że $G \ni g : G \ni x \to gxg^{-1} \in G$ jest działaniem grupy G (na zbiorze G).

Zadanie 6.2 Udowodnij twierdzenie: Jeżeli H jest podgrupą grupy G i H jest sumą klas sprzężoności to $H \lhd G$. Korzystając z tego twierdzenia wyznacz podgrupy normalne S_3, S_4, A_4, Q.

Zadanie 6.3 Podgrupy H_1, H_2 grupy G nazywamy sprzężonymi jeśli istnieje $g \in G$ takie, że $H_1 = gH_2g^{-1}$. Które podgrupy grup S_3, S_4, A_4, Q są sprzężone?

Zadanie 6.4 Niech G będzie grupą a X dowolnym jej niepustym podzbiorem. Wykaż, że $N_G(X) = \{g \in G; gXg^{-1} = X\}$ jest podgrupą G.
Wyznacz $N_{D_3}(H)$, gdzie $|H|$ jest podgrupą rzędu 2.

Zadanie 6.5 Centralizatorem elementu $a \in G$ (gdzie G jest pewną grupą) nazywamy zbiór

$$Z(a) = \{b \in G : ab = ba\}$$

Udowodnij, że odwzorowanie

$$f : G/Z(a) \ni xZ(a) \to xax^{-1} \in \mathrm{cl}(a)$$

jest bijekcją (pamiętaj, że wpierw należy wykazać, że f jest dobrze określona czyli, że jeśli $xZ(a) = yZ(a)$ wówczas $f(xZ(a)) = f(yZ(a))$).
Zwróć uwagę na fakt, że jeśli grupa G jest skończona, wówczas w konsekwencji prawdziwy jest wzór $|\mathrm{cl}(a)| = |G|/|Z(a)|$.
Sprawdź ten wzór na przykładzie grupy D_3.

Zadanie 6.6 Niech G będzie grupą. Wykaż, że $a \in Z(G)$ wtedy i tylko wtedy gdy $N(a) = G$ (gdzie $N(a) = N_G(\{a\})$). Jak można opisać $Z(G)$ za pomocą klas sprzężoności? Korzystając z tego opisu wyznacz $Z(S_3)$, $Z(A_4)$, $Z(S_4)$ i $Z(Q)$.

Zadanie 6.7 Sprawdź, że centrum grupy S_3 jest trywialne. Jak się to ma do twierdzenia 6.8?
Znajdź centrum D_4.

Zadanie 6.8 Niech G będzie grupą i $H \leq G$. Wykaż, że zdefiniowane na podgrupie H przyporządkowanie $H \ni h : G/H \ni Ha \to (Ha)h^{-1} \in G/H$ określa działanie grupy H na zbiorze G/H.

Zadanie 6.9 Ile jest 5-podgrup Sylowa w S_5? A ile 3-podgrup?

Zadanie 6.10 Na dwa sposoby wykaż, że istnieje tylko jedna grupa rzędu 35 i jest to grupa izomorficzna z $\mathbb{Z}_{35}$.

Zadanie 6.11 Czy grupa rzędu 45 może być nieprzemienna?
Wykaż, że każda grupa rzędu 45 ma element rzędu 15.

Zadanie 6.12 Znajdź wszystkie grupy rzędu 45.

Zadanie 6.13 Powiedzmy, że G jest grupą rzędu 396. Ile G ma 11-podgrup Sylowa jesli wiadomo, że $n_{11} \neq 1$?

Zadanie 6.14 Wskaż 2-podgrupy Sylowa grupy diedralnej D_n gdy $n = 2m$ i m jest liczbą nieparzystą. Ile jest takich 2-podgrup?

Zadanie 6.15 Niech G będzie grupą rzędu pm gdzie p jest liczbą pierwszą i $p > m$.Wykaż, że p-podgrupa Sylowa jest normalna.

Zadanie 6.16 Na wykładzie zostało udowodnione następujące twierdzenie: Jeżeli G jest grupą $|G| = p^2$ gdzie p jest liczbą pierwszą to grupa G jest abelowa. W niniejszym zadaniu wskazany zostanie przykład nieprzemiennej grupy rzędu p^3.
Niech $p \geq 3$ będzie liczbą pierwszą. Niech $G = Z_p \times Z_p \times Z_p$. Działanie określamy następująco:
$(x, y, z) * (x_1, y_1, z_1) = (x + x_1, y + y_1, z + z_1 - yx_1)$
Wykaż, że $(G, *)$ jest nieabelową grupą rzędu p^3 oraz rząd każdego elementu różnego od neutralnego wynosi p.

Zadanie 6.17 Niech p będzie liczbą pierwszą. Wykaż, że jeśli G jest p-grupą skończoną i $G \neq \{1\}$, wówczas $Z(G) \neq \{1\}$.

Zadanie 6.18 Niech G będzie dowolną grupą. Udowodnij, że jeśli $H, K \leq G$ wówczas:

$$HK \leq G \Leftrightarrow HK = KH \Leftrightarrow KH \leq G$$

Zadanie 6.19 Jeżeli H i K są podgrupami normalnymi grupy G, wówczas:

- $HK = KH$
- HK i KH są podgrupami normalnymi G.

Zadanie 6.20 Udowodnij, że jeśli G jest grupą, $H \trianglelefteq G$ oraz $K \leq G$, wówczas $HK \leq G$. Jeśli G jest grupą skończoną i $H \cap K = \{e\}$, wówczas $|HK| = |H||K|$.

Zadanie 6.21 Niech K będzie cykliczną i normalną podgrupą grupy G. Udowodnij, że każda podgrupa H grupy K jest normalną podgrupą grupy G.

Zadanie 6.22 Dla wszystkich liczb pierwszych p wyznacz wszystkie p-podgrupy Sylowa grup D_3, S_3, S_4, A_4, Q, D_4, Z_{12}.

Zadanie 6.23 Oblicz

1. n_5 w A_5
2. n_{11} w G, takiej, że $|G| = 396$ i wiemy, że $n_{11} \neq 1$

Zadanie 6.24 Udowodnij, że jeśli H i K są normalnymi podgrupami grupy G takimi, że $H \cap K = \{e\}$, wówczas $hk = kh$ dla dowolnych $h \in H$ i $k \in K$.

Zadanie 6.25 Wykaż, że

1. Każda grupa rzędu 15 jest cykliczna.
2. Każda grupa rzędu 245 jest izomorficzna z $\mathbb{Z}_5 \oplus \mathbb{Z}_{49}$ lub $\mathbb{Z}_5 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$.

Zadanie 6.26 Udowodnij, że każda grupa rzędu 30 ma podgrupę cykliczną rzędu 15.

Zadanie 6.27 Wykaż, że żadna grupa rzędu 40 nie jest prosta.

Zadanie 6.28 Czy w dowolnej grupie G rzędu 45 istnieje element rzędu 15?

Zadanie 6.29 Wykaż, że jeżeli p, q są liczbami pierwszymi to grupa rzędu pq nie jest prosta.

Zadanie 6.30 Wykaż, że grupy następujących rzędów nie są proste:

1. 36
2. 72
3. 56
4. p^2q^2 (gdzie p, q są liczbami pierwszymi).

Zadanie 6.31 Wykaż,że istnieją, z dokładnością do izomorfizmu,

1. dokładnie 2 grupy rzędu 99
2. dokładnie 1 grupa rzędu 1001

Zadanie 6.32 *Wykaż, że* $Aut(\Gamma)$ *(zdefiniowany na stronie 89* Γ *jest grupą.*

Rozdział 7

Grupy rozwiązalne

Mówimy, że **grupa** G **jest rozwiązalna** jeżeli istnieje $n \in \mathbb{N}$ oraz grupy $G_0 = G, G_1, ..., G_n$ takie, że

$$G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_i \supset G_{i+1} \supset ... \supset G_n = \{1\} \tag{7.1}$$

oraz dla każdego $i = 0, 1, ..., n-1$

1. $G_{i+1} \lhd G_i$
2. grupa ilorazowa G_i/G_{i+1} jest abelowa.

Ciąg zstępujący grup (7.1) spełniający warunki 1-2 nazywamy **ciągiem rozwiązalnym**. Czasami będziemy go zapisywać w postaci

$$G = G_0 \rhd G_1 \rhd G_2 \rhd ... \rhd G_i \rhd G_{i+1} \rhd ... \rhd G_n = \{1\}$$

Pojęcie grup rozwiązalnych jest, jak zobaczymy, ważne w badaniu rozwiązalności równań algebraicznych. Było znane Ewarystowi Galois, który napisał (str. 57 [9]): *Wpierw zauważyłem, że aby rozwiązać równanie, konieczne jest zredukowanie jego grupy aż do momentu, gdy zawiera tylko jedną permutację.*

Przykład 7.1 Wykażemy, że grupa S_4 permutacji zbioru 4-elementowego $\{1, 2, 3, 4\}$ jest grupą rozwiązalną.

Niech $K = \{(1), (12)(34), (13)(24), (14)(23)\}$. Szukanym ciągiem rozwiązalnym będzie

$$\{(1)\} \lhd K \lhd A_4 \lhd S_4$$

Wynika to z następujących faktów:

- $\{(1)\} \lhd K$ (jednoelementowa podgrupa zawierająca jedynie element neutralny jest normalna, $K/\{(1)\} \cong K$ jest abelowa, bowiem $|K| = 4$ (K jest izomorficzna z grupą Kleina).

- Elementami grupy A_4/K są K oraz

$$K(123) = (123)K = \{(123), (243), (142), (134)\}$$

$$K(132) = (132)K = \{(132), (143), (234), (124)\}$$

  Stąd wynika, że $K \lhd A_4$. Grupa A_4/K jest 3-elementowa a więc przemienna.

- Parzystość dowolnej permutacji σ jest taka sama jak parzystość permutacji σ^{-1}. Stąd wynika, że jeśli $\tau \in A_n$ wówczas $\sigma \circ \tau \circ \sigma^{-1} \in A_n$, a więc $A_n \lhd S_n$. Grupa S_n/A_n jest 2-elementowa a więc abelowa. □

Przykład 7.2 Każda grupa G rzędu $|G| = p \cdot q$, gdzie p i q są liczbami pierwszymi jest rozwiązalna.
Rzeczywiście, zgodnie z Trzecim Twierdzeniem Sylowa (str. 86), liczba p-podgrup Sylowa grupy G to $n_p \equiv 1 \pmod p$ i $n_p | q$ a więc $n_p = 1$ i wobec tego (oraz wniosku 6.14) istnieje podgrupa normalna H rzędu p grupy G. Mamy także $|G : H| = q$ a więc grupa $G : H$ jest przemienna. Ciąg rozwiązalny dla G to

$$G \rhd H \rhd \{1\}$$

□

Przykład 7.3 Wykażemy, że **grupa** A_5 nie tylko **nie jest rozwiązalna**, ale nie ma w ogóle nietrywialnej podgrupy normalnej.
Grupa alternująca A_5 ma 60 elementów, spośród których:

- 24 jest rzędu 5,
- 20 jest rzędu 3,
- 15 jest rzędu 2,
- 1 (element neutralny oznaczany w tym przypadku przez (1)) jest rzędu 1.

Gdyby istniała nietrywialna (różna od $\{1\}$ i A_5) podgrupa normalna H grupy A_5, mogłaby mieć jeden z następujących rzędów:

$$2, 3, 4, 5, 6, 10, 12, 15, 20, 30$$

- Gdyby $|H| \in \{3, 6, 12, 15\}$ wówczas mielibyśmy $|A_5 : H| \perp 3$ i w H musiałyby być zawarte wszystkie elementy rzędu 3 co jest niemożliwe, bo jest ich 20.
- Gdyby $|H| = 30$ to $|A_5 : H| = 2$ i do H musiałyby należeć wszystkie elementy rzędów 3 i 5. To także jest niemożliwe, bowiem jest ich łącznie 44.
- Gdyby $|H| \in \{5, 10, 15, 20\}$ to $|A_5 : H| \perp 5$ i w H byłoby 24 elementy rzędu 5, co jest niemożliwe.
- Gdyby $|H| = 4$ wówczas $|A_5 : H| = 15$ i z wniosku 6.18 grupa $A_5 : H$ byłaby grupą cykliczną rzędu 15, zawierałaby więc element rzędu 15. Wtedy także grupa A_5 musiałaby zawierać element rzędu 15, a to jest nieprawdą.

- Gdyby $|H| = 2$, wówczas H zawierałaby (1) i permutację σ rzędu 2. Bez straty ogólności możemy założyć, że $\sigma = (12)(34)$ (pamiętamy, że A_5 to grupa altermująca, a więc także w H wszystkie permutacje są parzyste). Mielibyśmy wtedy dla $\tau = (152) \in A_5$:

$$\tau \circ \sigma \circ \tau^{-1} = (152)(12)(34)(125) = (1509(2)(34) \notin H$$

co oznacza, że H nie jest podgrupą normalną. □

7.1 Komutatory i komutanty

Niech G będzie pewną grupą, $a, b \in G$. **Komutatorem** a i b nazywamy element postaci

$$[a, b] = aba^{-1}b^{-1}$$

Z łatwością można sprawdzić, że $ab = ba$ (elementy a i b są ze sobą przemienne) wtedy i tylko wtedy, gdy $[a, b] = 1$. Co więcej łatwo sprawdzić (zadanie 7.3), że prawdziwe jest następujące.

Twierdzenie 7.1 *Grupa G jest przemienna wtedy i tylko wtedy gdy $[g, h] = 1$ dla dowolnych $g, h \in G$.* ■

Zbiór wszystkich iloczynów wszystkich komutatorów grupy G nazywamy **komutantem** grupy G lub **grupą pochodną** grupy G i oznaczamy przez G'. Nietrudny dowód twierdzenia 7.2 pozostawiony jest jako zadanie 7.2.

Twierdzenie 7.2 *Grupa pochodna dowolnej grupy G jest podgrupą normalną G.*

Twierdzenie 7.3 *Dla dowolnej grupy G grupa ilorazowa $G : G'$ jest abelowa.*

Dowód. Na mocy faktu udowodnionego jako zadanie 7.3 wystarczy wykazać, że $[G'a, G'b] = G'$ dla dowolnych $a, b \in G$. Mamy:

$$[G'a, G'b] = (G'a)(G'b)(G'a)^{-1}(G'b)^{-1} = G'(aba^{-1}b^{-1}) = G'$$

bowiem $aba^{-1}b^{-1} \in G'$. ■

Następne dwa twierdzenia wyjaśniają sens rozważania komutantów w kontekście grup rozwiązalnych.

Twierdzenie 7.4 *Niech G będzie pewną grupą, $K \leq G$. Komutant G' zawiera się w K wtedy i tylko wtedy gdy K jest podgrupą normalną grupy G i grupa ilorazowa G/K jest abelowa.*

Dowód. Twierdzenie 7.4 można zapisać tak: jeśl $K \leq G$ wówczas

$$G' \subset K \Leftrightarrow K \lhd G \wedge G/K \text{ jest abelowa}$$

- Załóżmy, że $g \in G, k \in K$. Wówczas

$$gkg^{-1} = \underbrace{gkg^{-1}k^{-1}}_{\in G'} k \in Kk = K$$

Stąd wynika, że $K \lhd G$.
Dla dowolnych klas $Ka, Kb \in G/K$ mamy

$$Ka \cdot Kb \cdot Ka^{-1} \cdot Kb^{-1} = K \underbrace{aba^{-1}b^{-1}}_{\in G' \subset K} = K$$

skąd wynika, że grupa ilorazowa G/K jest abelowa (pamiętamy, że K jest elementem neutralnym grupy G/K).

- Jeśli grupa G/K jest abelowa wówczas dla dowolnych elementów $a, b \in G$ mamy $Kaba^{-1}b^{-1} = K$ i stąd $aba^{-1}b^{-1} \in K$ skąd wynika, że $G' \subset K$. ■

Twierdzenie 7.5 *Grupa G jest rozwiązalna wtedy i tylko wtedy gdy $G^{(n)} = \{1\}$ dla pewnego $n \in \mathbb{N}$.*

Dowód.

- Załóżmy, że

$$G = G^{(0)} \supset G^{(1)} \supset ... \supset G^{(n)} = \{1\}$$

gdzie $n \in \mathbb{N}$.
Ponieważ, że $G^{(n+1)} = (G^{(n)})' \subset G^{(i)}$, na mocy twierdzenia 7.4 (za G i K w twierdzeniu 7.4 przyjmujemy, odpowiednio, $G^{(i)}$ i $G^{(i+1)}$)

$$G^{(i+1)} \lhd G^{(i)} \text{ oraz grupa } G^{(i)}/G^{(i+1)} \text{ jest abelowa}$$

dla każdego $i = 0, 1, ..., n-1$, co oznacza, że G jest grupą rozwiązalną.

- Powiedzmy teraz, że

$$G = G_0 \supset G_1 \supset ... \supset G_n = \{1\}$$

jest ciągiem rozwiązalnym. Wystarczy wykazać, że $G^{(i)} \subset G_i$ dla $i = 0, 1, ..., n$.
Dowód przeprowadzimy przez indukcję.
Dla $i = 0$ mamy $G_0 = G^{(0)} = G$.
Przypuśćmy, że $G^{(i)} \subset G_i$ dla pewnego $i \geq 0, i \leq n-1$. Skoro $G_{i+1} \lhd$ oraz grupa G_i/G_{i+1} jest abelowa, na mocy twierdzenia 7.4 otrzymujemy

$$G^{(i+1)} = (G^{(i)})' \subset G_i' \subset G_{i+1}$$

(twierdzenie 7.4 interweniuje w ostatniej z powyższych inkluzji: jako K w twierdzeniu 7.4 przyjmujemy G_{i+1} a jako G grupę G_i). ■

Wniosek 7.6 *Każda podgrupa dowolnej grupy rozwiązalnej jest rozwiązalna.*

Dowód. Jeśli G jest rozwiązalna, wówczas (na mocy twierdzenia 7.5) istnieje $n \in \mathbb{N}$ takie, że

$$G \supset G' \supset G'' \supset ... \supset G^{(n)} = \{1\}$$

Jeśli teraz $H \leq G$ to $H^{(i)} \subset G^{(i)}$ i stąd $H^{(n)} = \{1\}$. ■

Przykład 7.4 *Dla każdego $n \geq 5$ grupa S_n nie jest rozwiązalna.*

Rzeczywiście, dla każdego n mamy: $A_5 \leq S_n$. Wiemy także (przykład 7.3), że grupa A_5 nie jest rozwiązywalna. Stąd także S_n nie jest rozwiązalna. ■

7.2 Twierdzenia o izomorfizmie grup

W dalszych rozważaniach o grupach rozwiązalnych wygodnie będzie nam wykorzystywać twierdzenia nazywane **twierdzeniami o izomorfizmie grup**. W dowodzie tych twierdzeń wykorzystywać będziemy Podstawowe Twierdzenie o Izomorfizmie Grup (twierdzenie 2.33).

Twierdzenie 7.7 (Drugie Twierdzenie o Izomorfizmie Grup) *Jeśli G jest grupą, H podgrupą normalną G i K podgrupą G wówczas*

- $HK = KH$
- $HK \leq H$
- $H \cap K \lhd K$
- *grupy* $\frac{K}{H \cap K}$ *i* $\frac{HK}{H}$ *są izomorficzne.*

Dowód. Twierdzenie 7.7 łatwiej będzie nam zapamiętać, gdy zapiszemy je w postaci symbolicznej:

$$H \lhd G, K \leq G \implies HK = KH,\ HK \leq H,\ H \cap K \lhd K \text{ oraz } \frac{K}{H \cap K} \cong \frac{HK}{H}$$

- Wykażemy wpierw, że $HK = KH$:

$$HK = \{hk | h \in H, k \in K\} = \bigcup_{k \in K} Hk \overset{H \lhd G}{=} \bigcup_{k \in K} kH = KH$$

- $HK \leq H$
  Musimy wykazać, że $HK \subset H$ oraz, że HK jest grupą.
  $HK \subset H$:

$$hk \in HK, h \in H, k \in K \Rightarrow hk = k \underbrace{k^{-1}hk}_{\in H} \in KH = HK$$

Ponieważ 1 należy zarówno do H jak do K, $1 \in HK$. Pozostaje więc wykazać, że w HK działanie jest zamknięte i element odwrotny do dowolnego elementu z HK też do HK należy.
Zamkniętość działania wynika z ciągu następujących równości:

$$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$$

Niech $hk \in HK, h \in H, k \in K$. Wówczas $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.

- $H \cap K \lhd K$ i $\frac{K}{H \cap K} \cong \frac{HK}{H}$.
$H \cap K \leq K$ wiemy bowiem, że iloczyn mnogościowy podgrup jest podgrupą.
Rozważmy teraz następujące odwzorowanie:

$$\Theta : K \ni k \longrightarrow Hk \in HK/H$$

Zauważmy, że skoro $K \subset HK$, dla dowolnego $k \in K$ mamy: $Hk \in HK/H$. Fakt, że Θ jest homomorfizmem jest do sprawdzenia bardzo łatwy. Θ jest także epimorfizmem, bowiem dla każdego elementu Hhk grupy ilorazowej HK/H ($h \in H, k \in K$) mamy:

$$Hhk = (Hh)k = Hk = \Theta(k)$$

Jądrem Θ jest $\operatorname{Ker}\Theta = \{k \in K | Hk = H\} = \{k \in K | k \in H\} = H \cap K$. Na mocy twierdzenia 2.32 mamy więc

$$H \cap K \lhd K$$

Na mocy Podstawowego Twierdzenia o Izomorfizmie Grup (twierdzenie 2.33, strona 37) otrzymujemy

$$K/(H \cap K) \cong HK/H$$

■

Twierdzenie 7.8 (Trzecie Twierdzenie o Izomorfizmie Grup) *Jeśli G jest grupą, $K \subset H \subset G$ i $K \lhd G, H \lhd G$ wówczas*

- $H/K \lhd G/K$
- $\frac{G/K}{H/K} \cong G/H$

Dowód. Zdefiniujmy funkcję $\Phi : G/K \ni Kg \to Hg \in G/H$.

- Funkcja Φ jest dobrze zdefiniowana.
Rzeczywiście, jeśli $Kg = Kh$ dla pewnych $g, h \in G$, wówczas $Kgh^{-1} = K \subset H$ a stąd $Hg = Hh$, czyli $\Phi(Kg) = \Phi(Kh)$.
- Φ jest epimorfizmame G/K na G/H.
- $\operatorname{Ker}\Phi = \{Kg : Hg = H\} = \{Kg : g \in H\} = H/K$.

Twierdzenie 7.8 wynika więc z twierdzenia 2.33. ■

7.3 Warunek konieczny i wystarczający rozwiązalności grupy

Następne twierdzenie okaże się praktycznym narzędziem w dowodach rozwiązalności grup.

Twierdzenie 7.9 *Niech G będzie grupą, $K \lhd G$. G jest rozwiązalna wtedy i tylo wtedy gdy grupy K oraz G/K są rozwiązalne.*

Dowód.

- Załóżmy wpierw, że K i G/K są grupami rozwiązalnymi. Istnieją wtedy ciągi rozwiązalne dla K i G/K, powiedzmy

$$K = K_0 \supset K_1 \supset ... \supset K_m = \{1\} \tag{7.2}$$

oraz

$$G/K = G_0/K \supset G_1/K \supset ... \supset G_n/K = \{K\} \tag{7.3}$$

Wykażemy, że ciąg

$$G = G_0 \supset ... \supset G_n = K = K_0 \supset K_1 \supset ... \supset K_m = \{1\} \tag{7.4}$$

jest ciągiem rozwiązalnym dla grupy G.
Ciąg (7.4) jest normalny ponieważ:

(1) Ciąg (7.2) jest normalny (i wobec tego $K_i \rhd K_{i+1}$ dla $0 \leq i \leq m-1$).

(2) Dla $0 \leq j \leq n-1$ i dla wszystkich $g \in G_j$ i $h \in G_{j+1}$ wiemy, że

$$(Kg)(Kh)(Kg)^{-1} \in GJi/K$$

bowiem ciąg (7.3) jest normalny. Stąd

$$K(ghg^{-1}) \in G_j/K$$

i wobec tego $ghg^{-1} \in G_i$, co oznacza $G_j \rhd G_{j+1}$ dla $0 \leq j \leq n-1$

Na mocy Trzeciego Twierdzenia o Izomorizmie Grup mamy

$$G_i/G_{i+1} \cong \frac{G_i/K}{G_{i+1}/K}$$

Ponieważ ciąg (7.3) jest rozwiązalny, grupa $(G_i/K)/(G_{i+1}/K)$ jest abelowa. Wobec tego także grupa G_i/G_{i+1} jest przemienna.
To kończy dowód faktu, że ciąg (7.4) jest rozwiązalny dla grupy G.

- Niech G będzie grupą rozwiązalną i niech $K \lhd G$. Wiemy (wniosek 7.6), że grupa K, jako podgrupa grupy rozwiązalnej, jest rozwiązalna. Pozostaje więc udowodnić, że grupa ilorazowa G/K jest rozwiązalna.
  Załóżmy, że ciąg rozwiązalny dla grupy G jest postaci (7.4).
  Wykażemy, że ciąg

$$G/K = G_0K/K \supset ... \supset G_iK/K \supset G_{i+1}/K \supset ... \supset G_nK/K = \{K\} \qquad (7.5)$$

  jest ciągiem rozwiązalnym dla G/K. Musimy więc udowodnić, że $G_{i+1}K/K \lhd G_iK/K$ a także, że grupa $(G_iK/K)/(G_{i+1}K/K)$ jest abelowa.

  - $G_{i+1}K/K \lhd G_iK/K$
    Wystarczy wykazać, że $G_{i+1}K \lhd G_iK$ (Czytelnikowi radzę się upewnić, że rozumie dlaczego rzeczywiście tylko tyle wystarczy udowodnić).
    Niech $g_i \in G_i; k, k' \in K; g_{i+1} \in G_{i+1}$ (pamiętamy, że $G_{i+1} \lhd G_i$ i $K \lhd G$).

$$\begin{aligned}(g_ik)(g_{i+1}k')(g_ik)^{-1} &= g_ikg_{i+1}k'k^{-1}g_i^{-1}\\ &= g_i\underbrace{kg_{i+1}k^{-1}}_{\in G_{i+1}}\underbrace{kk'k^{-1}}_{\in K}g_i^{-1}\\ &= g_iabg_i^{-1} \text{ (gdzie } a \in G_{i+1}, b \in K)\\ &= \underbrace{g_iag_i^{-1}}_{\in G_{i+1}}\underbrace{g_ibg_i^{-1}}_{\in K} \in G_{i+1}K\end{aligned}$$

  - Grupa $(G_iK : K)/(G_{i+1}K : K)$ jest abelowa:

$$\begin{aligned}&(G_iK : K)/(G_{i+1}K : K) = \\ =\ &(G_i(G_{i+1}K))/(G_{i+1}K) && \text{bo } G_{i+1} \subset G_i \text{ i stąd } G_iG_{i+1} = G_i\\ \cong\ &G_i/(G_i \cap (G_{i+1}K)) && \text{na mocy twierdzenia 7.7}\\ \cong\ &(G_i : G_{i+1})/((G_i \cap (G_{i+1}K)) : G_{i+1}) && \text{na mocy twierdzenia 7.8}\end{aligned}$$

  Skoro grupa ilorazowa $G_i : G_{i+1}$ jest abelowa, także grupa $(G_iK/K)/(G_{i+1}K/K)$ jest abelowa i G/K jest rozwiązalna. ■

7.4 Zadania

Zadanie 7.1 Udowodnij, że w dowolnej grupie G dla każdych $a, b, g \in G$ spełnione są równości:

- $[a, b]^{-1} = [b, a]$
- $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$

Zadanie 7.2 Udowodnij, że $G' \lhd G$ dla dowolnej grupy G (w dowodzie można wykorzystać zadanie 7.1).

Zadanie 7.3 Udowodnij, że grupa G jest przemienna wtedy i tylko wtedy gdy $G' = \{1\}$.

Zadanie 7.4 Udowodnij, że każda grupa przemienna jest rozwiązalna.

Zadanie 7.5 Które z poniższych grup są rozwiązalne?
(a) S_2 (b) S_3 (c) S_4 (d) D_n

Zadanie 7.6 Udowodnij, że jeśli G jest grupą, $F \lhd G$ i $H \lhd G$ wówczas $F \cap H \lhd G$.

Zadanie 7.7 Wykaż, że jeśli H jest cykliczną i normalną podgrupą grupy G, wówczas każda podgrupa grupy H jest normalną podgrupą G

Zadanie 7.8 Udowodnij, że jeśli $H \lhd G$ i grupa G/H jest abelowa, wówczas $G' \subset H$.

Zadanie 7.9 Wykorzystaj zadanie 7.8 do wykazania, że $S_4' = A_4$.

Zadanie 7.10 Czy komutant każdej grupy rozwiązalnej jest grupą abelową?

Zadanie 7.11 Udowodnij, że każda grupa rzędu p^2q, gdzie p i q są liczbami pierwszymi, jest rozwiązalna.

Zadanie 7.12 Dla dowolnej liczby pierwszej p udowodnij, że każda p-grupa jest rozwiązalna.

Rozdział 8

Pierścienie i ciała

W definicji pierścienia, którą podajemy poniżej, stosujemy powszechnie znaną ze zbiorów liczbowych ($\mathbf{R}, \mathbf{N}, \mathbf{Z}$ etc) konwencję nie pisania znaku działania $\cdot$ (inaczej: działania multyplikatywnego), o ile tylko nie prowadzi to do nieporozumień. W wyrażeniach postaci $(ab)+c$ opuszczamy nawias i piszemy $ab+c$, co oznacza, że jeśli nie ma nawiasu, to stosujemy regułę pierwszeństwa *mnożenia* przed *dodawaniem* (właściwie powinniśmy powiedzieć: *pierwszeństwa działania multyplikatywnego* (to znaczy: oznaczanego przez $\cdot$) *przed działaniem addytywnym* (to znaczy: oznaczanym przez $+$)).
Będziemy pisać $a - b$ zamiast $a + (-b)$.

Definicja 8.1 *Zbiór P z dwoma działaniami $+$ (dodawania) oraz $\cdot$ (mnożenia) nazywamy pierścieniem jeśli:*

- *P z działaniem dodawania jest grupą przemienną,*
- *działanie mnożenia jest łączne,*
- *dla dowolnych elementów $a, b, c \in P$: $a(b+c) = ab+ac$ oraz $(a+b)c = ac+bc$ (rozdzielność mnożenia względem dodawania)*

Element neutralny dla działania $+$ pierścienia P nazywamy **zerem** *pierścienia (i najczęściej oznaczamy przez 0).*

Jeśli działanie $\cdot$ jest przemienne to P nazywamy **pierścieniem przemiennym**.

Jeśli $ab = 0 \Rightarrow a = 0$ lub $b = 0$ to P jest **pierścieniem bez dzielników zera**.

Jeśli zaś w P istnieje taki element $1 \in P$, że dla dowolnego $x \in P$ zachodzi: $1x = x1 = x$ to P nazywamy **pierścieniem z jedynką** *(a element 1* **jedynką** *pierścienia P).*

Pierścień przemienny z jedynką i bez dzielników zera nazywamy **pierścieniem całkowitym**.

Pierścien całkowity P w którym każdy element różny od zera ma element odwrotny ze względu na mnożenie[1] *nazywamy* **ciałem**.

[1] Inaczej: dla każdego $a \in P, a \neq 0$ istnieje $a' \in P$ taki, że $aa' = 1$.

Twierdzenie 8.1 *Pierścień P jest bez dzielników zera wtedy i tylko wtedy dla dowolnych elementów spełniony jest warunek:*

$$\forall a,b,c \in P,\ c \neq 0 \left\{ \begin{array}{lcl} ac = bc & \Rightarrow & a = b \\ ca = cb & \Rightarrow & a = b \end{array} \right. \quad (\text{ prawa skracania}) \tag{8.1}$$

Dowód. Przypuśćmy wpierw, że w pierścieniu P spełniony jest warunek (8.1) oraz, że dla pewnych $a, b \in P$ zachodzi $ab = 0$. Wówczas mamy ciąg implikacji: $ab = 0 \Rightarrow ab = a0 \Rightarrow ab - a0 = 0 \Rightarrow a(b-0) = 0 \Rightarrow a(b-0) = a0$. Z ostatniej równości oraz z drugiej z implikacji warunku (8.1) wynika, że jeśli $a \neq 0$, wówczas $b - 0 = 0$, a więc $b = 0$.
Przypuśćmy teraz, że pierścień P jest bez dzielników zera. Wówczas, dla dowolnego $c \in P, c \neq 0$ prawdziwe są implikacje $ac = bc \Rightarrow ac - bc = 0 \Rightarrow ac + (-b)c = 0 \Rightarrow (a + (-b))c = 0 \Rightarrow a + (-b) = 0 \Rightarrow a = b$. Podobnie dowodzimy prawa lewostronnego skracania. ■

8.1 Przykłady pierścieni

Z pewnością najlepiej znanymi pierścienimi są zbiory liczbowe: liczb całkowitych, wymiernych, rzeczywistych i zespolonych ze zdefiniowanymi w znany sposób działaniami dodawania zczególną rolę w teorii pierścieni odgrywa pierścień liczb całkowitych.
Z łatwością można sprawdzić, że poniższe zbiory ze wskazanymi w nich działaniami są pierścieniami.

- Zbiór macierzy $\mathbf{R}^{n\times n}$ (o n wierszach i n kolumnach) z działaniami określonymi w zwykły sposób.

- Łatwo sprawdzić, że w zbiorze liczb całkowitych $\mathbf{Z}$ relacja *przystawania modulo* n zdefiniowana przez
$$a \equiv b \pmod{n} \iff n|b-a$$
jest zgodna z działaniami dodawania i mnożenia w $\mathbb{Z}$. Można więc zdefiniować działania indukowane dodawania i mnożenia w zbiorze klas $\mathbf{Z}/(\mathrm{mod}\ n)$. Nietrudno także wykazać, że z tymi działaniami $\mathbf{Z}/(\mathrm{mod}\ n)$ jest pierścieniem (z jedynką, bez dzielników zera wtedy i tylko wtedy gdy n jest liczbą pierwszą).
Jeśli n jest liczbą pierwszą, wówczas $\mathbf{Z}/(\mathrm{mod}\ n)$ jest ciałem.

- Niech P będzie pierścieniem przemiennym. Zbiór $\{\sum_{i=0}^{\infty} a_i \mathbf{x}^i | a_i \in P\}$ nazywamy zbiorem **szeregów formalnych** Łatwo można wykazać, że zbiór ten tworzy pierścień

- Pierścień **wielomianów** $P[\mathbf{x}]$ o współczynnikach w pierścieniu P to zbiór szeregów formalnych, w których skończona liczba współczynników jest różna od zera.

Inaczej: oznaczmy przez $\mathbf{x}^i = (\underbrace{0,...,0}_{i\ zer},1,\underbrace{0,...}_{zera})$. Zdefiniujmy mnożenie naszych $\mathbf{x}$-ów wzorem $\mathbf{x}^i\mathbf{x}^j = \mathbf{x}^{i+j}$. Wówczas, jak to łatwo można udowodnić, zbiór szeregów foralnych o skończonej liczbie współczynników różnych od zera z działaniami określonymi wzorami:

- $(\sum_{i=0}^{\infty} a_i\mathbf{x}^i) + (\sum_{i=0}^{\infty} b_i\mathbf{x}^i) = \sum_{i=0}^{\infty}(a_i + b_i)\mathbf{x}^i$
- $(\sum_{i=0}^{\infty} a_i\mathbf{x}^i) \cdot (\sum_{j=0}^{\infty} b_j\mathbf{x}^j) = \sum_{l=0}^{\infty} c_l\mathbf{x}^l$, gdzie $c_l = \sum_{k=0}^{l} a_k b_{l-k}$ jest pierścieniem przemiennym (z jedynką, o ile w P jest jedynka).

8.2 Podpierścienie

Podpierścieniem pierścienia P nazywamy dowolny podzbiór $A \subset P$, $A \neq \emptyset$ jeśli A wraz z działaniami + i $\cdot$ (zacieśnionymi do zbioru A) jest pierścieniem.

Bez trudu można wykazać następujący warunek konieczny i wystarczający, by podzbiór pierścienia był jego podpierścieniem (poz. zadanie 8.5).

Twierdzenie 8.2 *Niech P będzie pierścieniem. $A \subset P$, $A \neq \emptyset$. A jest podpierścieniem P wtedy i tylko wtedy, gdy*

1. $\forall a, b \in A\ a - b \in A$,
2. $\forall a, b \in A\ ab \in A$.

8.3 Ideały

Definicja 8.2 *Niech P będzie pierścieniem, $I \subset P, I \neq \emptyset$. Mówimy, że I jest* **ideałem** *pierścienia P jeśli spełnione są następujące dwa warunki:*

1. $a, b \in P \Rightarrow a - b \in I$
2. $\alpha \in P, a \in I \Rightarrow \alpha a \in I, a\alpha \in I$

Łatwo zauważyć, że każdy ideał pierścienia P jest podpierścieniem tego pierścienia.

Przykład 8.1 *W dowolnym pierścieniu P zbiory $\{0\}$ i P są ideałami.*

Rola ideałów w teorii pierścieni przypomina nieco tę, którą w teorii grup odgrywają podgrupy normalne. Wyjaśnia to następujące twierdzenie.

Twierdzenie 8.3 *Niech P będzie pierścieniem i niech A będzie podpierścieniem pieścienia P. Zbiór $P/A = \{a + A : a \in P\}$ jest działaniami określonymi wzorami:*

$$(a + A) \oplus (b + a) = (a + b) + A \tag{8.2}$$

$$(a + A) \circ (b + A) = ab + A \tag{8.3}$$

jest pierścieniem wtedy i tylko wtedy, gdy A jest ideałem.

Dla dowolnego pierścienia P i jego ideału A pierścień P/A z działaniami określonymi wzorami (8.2) i 8.3 nazywamy **pierścieniem ilorazowym**. Działania w pierścieniu ilorazowym oznaczamy tak jak w pierścieniu, a więc piszemy $(a+A)+(b+A)$ oraz $(a+A)(b+A)$, jeśli tylko nie prowadzi to do nieporozumień[2]
Oczywiście zbiór P/A (oznaczany także przez $P:A$) jest zbiorem klas równoważności relacji R zdefiniowanej w P przez

$$aRb \Leftrightarrow b-a \in A$$

- mówimy wtedy, że elementy a i b pierścienia **przystają modulo** A .

Dowód twierdzenia 8.3. Przypuśćmy wpierw, że A jest ideałem pierścienia P. Wykażemy, że wtedy P/A jest pierścieniem.
Ze względu na dodawanie P jest grupą przemienną, stąd A jest addytywną podgrupą normalną. Wobec tego P/A jest grupą przemienną ze względu na dodawanie (w której $A = 0 + A$ jest elementem neutralnym).
Wykażemy, że działanie mnożenia zdefiniowane na klasach wzorem 8.3 jest dobrze określone (inaczej: relacja R jest zgodna z tym działaniem), to znaczy, że

$$aRb \wedge a'Rb' \Rightarrow (aa')R(bb')$$

Rzeczywiście, jeśli aRb i $a'Rb'$ to $b-a \in A, b'-a' \in A$ a stąd $a = b+\alpha, a' = b'+\alpha'$, gdzie $\alpha, \alpha' \in A$. Wtedy $aa' = bb' + b\alpha' + b'\alpha$, a więc $aa' - bb' = b\alpha' + b'\alpha \in A$ (A jest ideałem, $\alpha, \alpha' \in A$).
Pozostaje teraz wykazać, że (ciągle zakładając, iż A jest ideałem) z działaniami zdefiniowanymi wzorami (8.2) i (8.3) P/A jest pierścieniem. To jednak jest nietrudnym zadaniem, które pozostawiam do wykonania czytelnikowi[3].
Przypuśćmy teraz, że podpierścień A nie jest ideałem. Wówczas istnieją $a \in A$ i $\alpha \in P$ takie, że $a\alpha \notin A$ lub $\alpha a \notin A$. Powiedzmy, że $a\alpha \notin A$ (przypadek gdy $\alpha a \notin A$ jest podobny). Mamy oczywiście $a = a - 0 \in A$ i $0 = \alpha - \alpha \in A$ a stąd $aP0$ i $\alpha R\alpha$. Z drugiej strony $a\alpha - 0\alpha = a\alpha \notin A$ a więc $a\alpha$ nie jest w relacji R z 0α co oznacza, że R nie jest zgodna z mnożeniem w A a więc wzór (8.3) nie definiuje działania w P/A. ■

W dalszym ciągu działania na klasach (a więc działania określone wzorami (8.2) i (8.3) w $P:A$) oznaczamy przez $+$ i $\cdot$, a więc dokładnie tak jak w pierścieniu i zachowujemy konwencję niepisania kropki dla mnożenia wszędzie tam, gdzie nie prowadzi to do nieporozumień. Wzory (8.2) i (8.3) przybierają wtedy postać

$$(a+A)+(b+A) = (a+b)+A$$

i

$$(a+A)(b+A) = ab+A$$

Pierścień $P:A$ z tak określonymi działaniami nazywamy **pierścieniem ilorazowym**. Z łatwością można stwierdzić (por. zadanie 8.6), że prawdziwe jest następujące twierdzenie.

[2] A nigdy nie prowadzi.

[3] Warto jednak zwrócić uwagę na fakt, że elementem neutralnym dla dodawania w P/A jest oczywiście $0+A$ (piszemy także $0+A=A$).

Twierdzenie 8.4 *Jeśli I jest ideałem pierścienia P i pierścień P jest pierścieniem z jedynką lub przemiennym, wówczas P/I jest pierścieniem, odpowiednio, z jedynką lub ilorazowym.* ■

8.4 Ideały i pierścienie główne

W dowolnym pierścieniu przemiennym P, dla dowolnego $a \in P$, zbiór $(a) = \{\alpha a | \alpha \in P\}$ jest ideałem. Ideały tej postaci nazywać będziemy **ideałami głównymi**. W takiej sytuacji mówimy też, że ideał główny (a) jest **generowany** przez element a. Jeśli w pierścieniu przemiennym P każdy ideał jest ideałem głównym wówczas P nazywamy **pierścieniem głównym**.

Najlepiej znanym przykładem pierścienia głównego jest pierścień liczb całkowitych.

Twierdzenie 8.5 *Pierścień liczb całkowitych $\mathbb{Z}$ jest pierścieniem głównym.*

Dowód. Ideał zerowy $\{0\}$ jest oczywiście ideałem głównym generowanym przez 0. Przypuśćmy, że A jest ideałem w $\mathbb{Z}$, $A \neq \{0\}$. Zauważmy, że do A należy co najmniej jedna liczba dodatnia. Rzeczywiście, skoro $A \neq \{0\}$, w A jest jakaś liczba $a \neq 0$. Wobec tego także $-a \in A$ (wiemy, że 0 jest w dowolnym ideale, a zatem i $0 - a = a \in A$), zaś jedna z liczb: a lub $-a$ jest dodatnia.
Niech teraz a_0 będzie najmniejszą liczbą dodatnią w A. Oczywiście A zawiera wszystkie wielokrotności liczby a, a więc $A \supset (a)$. Wystarczy więc wykazać, że $A \subset (a)$.
Na mocy twierdzenia o dzieleniu z resztą w zbiorze liczb całkowitych, istnieją $q, r \in \mathbf{Z}$ spełniające

$$b = qa + r, \qquad 0 \leq r < a$$

$r = b - qa$, a więc $r \in A$, a ponieważ a jest najmniejszym dodatnim elementem A, mamy $r = 0$ i w konsekwencji $a|b$. ■

8.5 Homomorfizmy pierścieni

Niech P, Q będą pierścieniami. Odwzorowanie $f : P \to Q$ nazywamy **homomorfizmem** jeśli

- dla dowolnych $a, b \in P$ zachodzi warunek $f(a + b) = f(a) + f(b)$ - mówimy wtedy, że f jest **addytywne** oraz
- dla dowolnych $a, b \in P$ zachodzi warunek $f(ab) = f(a_f(b)$ - mówimy, że f jest multyplikatywne.

Tak więc homomorfizm to odwzorowanie, które jest addytywne i multyplikatywne.

Homomorfizm, który jest surjektywny nazywamy **epimorfizmem** a taki, który jest injektywny **epimorfizmem**. Homomorfizm, który jest epimorfizmem i monomorfizmem (a więc jest bijekcją) nazywamy **izomorfizmem**.

Jądrem homomorfizmu pierścieni f nazywamy zbiór $\text{Ker } f = f^{-1}(\{0\}) = \{a \in P : f(a) = 0\}$. Łatwo wykazać, że dla dowolnego homomorfizmu f pierścieni $f(0) = 0$, stąd $0 \in \text{Ker } f$ i w konsekwencji jądro homomorfizmu pierścieni nigdy nie jest zbiorem pustym.

Dowody następujących twierdzeń są nietrudnymi ćwiczeniami, pozostawiam je do wykonania samodzielnie, jako zadania 8.12 i 8.13.

Twierdzenie 8.6 *Homomorfizm f pierścieni jest monomorfizmem wtedy i tylko wtedy gdy $Ker\ f = \{0\}$.* □

Twierdzenie 8.7 *Dla dowolnego homomorfizmu pierścieni $f : P \to Q$ jądro jest ideałem pierścienia P.* □

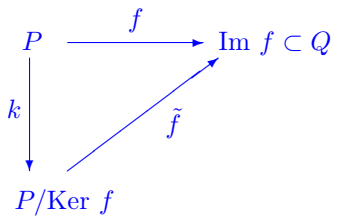
Przez Im f oznaczamy zbiór wartości homomorfizmu pierścieni $f : P \to Q$, czyli $\text{Im } f = \{f(a) | a \in P\}$. Z łatwością można wykazać, że Im f jest podpierścieniem pierścienia Q.

Twierdzenie 8.8 (Twierdzenie o izomorfizmie pierścieni) *Niech $f : P \to Q$ będzie homomorfizmem pierścieni. Wtedy*

$$f = \tilde{f} \circ k \tag{8.4}$$

gdzie $k : P \ni a \to a + Ker\ f \in P/Ker\ f$ jest homomorfizmem (zwanym homomorfizmem kanonicznym), zaś
$\tilde{f} : P/Ker\ f \ni a + Ker\ f \to \tilde{f}(a + A) = f(a) \in Im\ f$ jest izomorfizmem pierścieni - ilorazowego $P/Ker\ f$ na $Im\ f$.

Funkcjonowanie twierdzenia o izomorfizmie pierścieni wygodnie jest prześledzić na ilustującym je diagramie.



Dowód. Bardzo łatwo można udowodnić, że jądro dowolnego homomorfizmu $f : P \to Q$ jest ideałem pierścienia Q (por. zadanie 8.13). $P/\text{Ker } f$ jest więc pierścieniem. Udowodnimy teraz, że odwzorowanie $\tilde{f}$ zdefiniowane wzorem $\tilde{F}(a+\text{Ker } f) = f(a)$ jest dobrze określone to znaczy, że wartość $\tilde{f}$ na klasie elementu a, czyli na $a + \text{Ker } f$ nie zależy od tego jakiego reprezentanta klasy wybraliśmy. Inaczej mówiąc, powinniśmy

mieć $\tilde{f}(a + \text{Ker } f) = \tilde{f}(b + \text{Ker } f)$ o ile tylko $b - a \in \text{Ker } f$. Mamy jednak ciąg równoważności:

$$a + \text{Ker } f = b + \text{Ker } f \Leftrightarrow a - b \in \text{Ker } f \Leftrightarrow f(a - b) = 0 \Leftrightarrow f(a) = f(b)$$

Stąd wynika zaś, że funkcja $\tilde{f}$ jest dobrze określona.
$\tilde{f}$ jest homomorfizmem, bowiem mamy

$$\tilde{f}((a + \text{Ker } f) + (b + \text{Ker } f)) = \tilde{f}((a + b) + \text{Ker } f) = f(a + b) = f(a) + f(b)$$
$$= \tilde{f}(a + \text{Ker } f) + \tilde{f}(b + \text{Ker } f)$$

oraz

$$\tilde{f}((a + \text{Ker } f)(b + \text{Ker } f)) = \tilde{f}(ab + \text{Ker } f) = f(ab) = f(a)f(b)$$
$$= \tilde{f}(a + \text{Ker } f)\tilde{f}(b + \text{Ker } f)$$

Mamy także ciąg wynikań:

$$\tilde{f}(a + \text{Ker } f) = \tilde{f}(b + \text{Ker } f) \overset{\text{z def. } \tilde{f}}{\Longrightarrow} f(a) = f(b) \Rightarrow f(a - b) = 0 \Rightarrow a - b \in \text{Ker } f$$
$$\Rightarrow a - b + \text{Ker } f = \text{Ker } f \Rightarrow a + \text{Ker } f = b + \text{Ker } f$$

a więc $\tilde{f}$ jest monomorfizmem. Fakt, że $\tilde{f}$ jest epimorfizmem oraz zachodzi wzór (8.4) jest oczywisty z definicji $\tilde{f}$. ■

8.6 Podzielność w pierścieniach

Definicja 8.3 *Niech P będzie pierścieniem całkowitym, $a, b \in P$. Mówimy, że a* **dzieli** *b jeżeli istnieje $c \in P$ takie, że $b = ac$. Piszemy wówczas $a|b$.*
Jeśli $a|b$ i $b|a$ to elementy a i b nazywamy **stowarzyszonymi**.

Oczywiście jeśli $a \in \mathbb{Z}, a \neq 0$, wówczas a i $-a$ są elementami stowarzyszonymi w $\mathbb{Z}$, zaś $a, -a, ai, -ai$ są elementami stowarzyszonymi w pierścieniu $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.
W $\mathbb{Z}/(\text{mod}6)$ elementy 1 i 5 są stowarzyszone. Co więcej, każdy element $a \in \mathbb{Z}_n$ taki, że $a \perp n$ jest stowarzyszony z 1.
W ciele każde dwa różne od zera elementy są stowarzyszone.

Definicja 8.4 *Elementy stowarzyszone z 1 (jedynką pierścienia) nazywamy* **jednościami pierścienia**.

Twierdzenie 8.9 *Zbiór jedności pierścienia P tworzy grupę (multyplikatywną). (Grupę tę nazywamy* **grupą jedności pierścienia**).

Przykłady.

1. Zbiór $\{-1, 1\}$ jest zbiorem jedności w pierścieniu liczb całkowitych.

2. W pierścieniu $\mathbf{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbf{Z}\}$ (sprawdź, że to pierścień!) prawdziwy jest wzór
$$(2 - \sqrt{3})(2 + \sqrt{3}) = 1$$
Stąd
$$(2 - \sqrt{3})^k (2 + \sqrt{3})^k = 1$$
dla dowolnego k naturalnego. A więc w pierścieniu $\mathbf{Z}[\sqrt{3}]$ zbiór jedności jest nieskończony.

Każde przedstawienie elementu a pierścienia P w postaci
$$a = a_1 \cdot \cdots \cdot a_n \tag{8.5}$$
nazywamy **rozkładem na czynniki**. O rozkładzie 8.5 mówimy, że jest **właściwy**, jeśli

1. $n \geq 2$,
2. żaden z czynników $a_1, \ldots, a_n$ nie jest jednością.

Jeśli żaden właściwy rozkład elementu a nie istnieje, wówczas mówimy, że a jest **nierozkładalny**.

Element a pierścienia P nazywamy **pierwszym**, jeżeli zachodzi implikacja:
$$a|bc \Rightarrow a|b \text{ lub } a|c$$

Pamiętamy ze szkoły, że liczby całkowite nierozkładalne i pierwsze to to samo. Tak jest w istocie. Niemniej przekonamy się, że w pewnych pierścieniach i to, na dodatek, w pierścienich liczbowych, istnieją elementy nierozkładalne, które nie są pierwsze[4]. Poniższe twierdzenie podaje relację zawierania pomiędzy zbiorami elementów pierwszych i nierozkładalnych dowolnego pierścienia całkowitego.

Twierdzenie 8.10 *W dowolnym pierścieniu całkowitym P, każdy element pierwszy jest nierozkładalny.*

Dowód. Niech $a \in P$ będzie elementem pierwszym pierścieni całkowitego P. Przypuśćmy, że istnieje rozkład a, czyli
$$a = a_1 \cdot \cdots \cdot a_k \tag{8.6}$$
dla pewnego $k \geq 2$. Wówczas istnieje $i \in \{1, \ldots, k\}$ takie, że $a|a_i$. Ponieważ (na mocy (8.6)) $a_i|a$, elementy a oraz a_i są stowarzyszone.
Wykażemy teraz, że jeśli dwa elementy x, y są stowarzyszone w pierścieniu całkowitym

[4]Odkrycie tego zaskakującego faktu zawdzięczamy niemieckiemu matematykowi Ernestowi Kummerowi (1810-1893), jednemu z twórców algebraicznej teorii liczb (wspólnie z Dedekindem i Kroneckerem). Kummer jest także znany jako ten, kto wykazał Ostatnie Twierdzenie Fermata dla najbardziej obszernej klasy liczb aż do kompletnego dowodu tego słynnego twierdzenia w 1993 roku przez Andrew Wilesa (1953 -).

P, powiedzmy $x|y$ i $y|x$, wówczas $x = yz$, gdzie z jest jednością.
Rzeczywiście,

$$\left.\begin{array}{ll} x|y \Rightarrow & \exists z \in P: \quad y = zx \\ y|x \Rightarrow & \exists t \in P: \quad x = ty \end{array}\right\} \Rightarrow y = zty$$

Stąd i z faktu, że P jest pierścieniem całkowitym (a więc z jedynką i prawem skracania) wnioskujemy łatwo, że $zt = 1$, czyli, że z i t są stowarzyszone z jedynką, czyli jednościami pierścienia P.
Odnosząc te rozważania do a i a_i otrzymujemy $a = a_1 \cdot \cdots \cdot a_{i-1}a_{i+1} \cdot \cdots \cdot a_k a_i = a_i z$, przy czym z jest jednością. Korzystając z przemienności i ponownie z prawa skracania otrzymujemy, że $a_1 \cdot \cdots \cdot a_{i-1}a_{i+1} \cdot \cdots \cdot a_k = z$, a więc, jak łatwo zauważyć, także $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k$ są jednościami, co kończy dowód. ■

Bardzo znanym przykładem na to, że twierdzenie odwrotne do twierdzenia 8.10 nie jest prawdziwe, jest **pierścień Dedekinda** $\mathbb{Z} < \sqrt{5}i >= \{a + bi\sqrt{5} | a, b \in \mathbf{Z}\}$.
Wykażemy wpierw, że liczba 2 jest elementem nierozkładalnym pierścienia Dedekinda.
rzeczywiście,

$$2 = (a + bi\sqrt{5})(c + di\sqrt{5})$$

daje układ równań

$$\begin{array}{rcl} ac - 5bd & = & 2 \\ bc + ad & = & 0 \end{array}$$

Traktując ten układ jako układ o niewiadomych c i d otrzymamy

$$c = \frac{2a}{a^2 + 5b^2} \qquad d = \frac{-2b}{a^2 + 5b^2}$$

(zauważmy, że a i b nie mogą być równocześnie równe zero).
Ponieważ c i d są całkowite, zachodzi $a^2 + 5b^2 \leq 2|a|$ (lub $a = 0$). Stąd

$$|a| \leq 2$$

i wobec tego

$$a \in \{0, -1, 1, -2, 2\}$$

- Gdyby $a = 0$ wówczas mielibyśmy $ac = 0$ i w konsekwencji $2 = -5bd$, co dla całkowitych b i d jest niemożliwe.
- Gdyby $a = 1$ mielibyśmy $c = \frac{2}{1+5b^2}$, a więc $b = 0$ i w konsekwencji $c = 2$ i $d = 0$. Nasz rozkład byłby więc z konieczności postaci $2 = 1 \cdot 2$, a więc nie byłby rozkładem właściwym (jeden z czynników jest jednością).
- Gdyby $a = 2$ wówczas mielibyśmy $c = \frac{4}{4+5b^2}$ a stąd wnioskujemy łatwo, że $b = 0, c = 1, d = 0$ i wobec tego $2 = 2 \cdot 1$ – sprzeczność z przypuszczeniem, że rozkład liczby 2 (w $\mathbf{Z} < \sqrt{5}i >$) jest właściwy.
- Podobnie jak powyżej sprawdzamy, że a nie może być równe ani -1 ani -2.

Zauważmy teraz, że

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

Wobec tego $2|6$. Łatwo także sprawdzić, że 2 nie dzieli ani $1 + \sqrt{5}$ ani $1 - \sqrt{5}$. Sprawdziliśmy, że w pierścieniu Dedekinda $\mathbf{Z} < \sqrt{-5} >$ liczba 2 jest elementem nierozkładalnym, który nie jest elementem pierwszym.

9,
2.2011

8.7 Charakterystyka pierścienia

Charakterystyką pierścienia P nazywamy najmniejszą dodatnią liczbę całkowitą taką, że $na = 0_P$ dla każdego elementu $a \in P$, o ile taka liczba n istnieje. W przeciwnym przypadku mówimy, że charakterystyką P jest 0 lub, że P nie ma charakterystyki. Dla pierścieni mających charakterystykę (lub o charakterystyce dodatniej) mamy więc

$$\text{char } (P) = \min\{n \in \mathbb{N} - \{0\} | nP = \{0\}\}$$

Rzędem elementu a **pierścienia** P nazywamy jego rząd w addytywnej grupie P (stąd, dla przypomnienia tego faktu i uniknięcia bałaganu spowodowanego istnieniem dwóch działań w pierścieniu, będziemy też mówić o **addytywnym rzędzie elementu pierścienia**. Podobnie jak w przypadku rzędów elementów w grupach, rząd elementu $a \in P$ oznaczamy przez $|a|$.

Przykład 8.2

Twierdzenie 8.11 *Jeśli P jest pierścieniem z jedynką 1_P i rzędem 1_P jest n, wówczas char $(P) = n$.*

Dowód. Rzeczywiście, powiedzmy, że rzędem (addytywnym) jedynki 1_P pierścienia P jest n. Wtedy $n \cdot 1_P = 0_P$ i n jest najmniejszą liczbą naturalną o tej własności. Wówczas dla każdego $a \in P$ mamy $n \cdot a = (n \cdot 1_P)a = 0_P a = 0$, a więc n jest charakterystyką pierścienia P. ■

Twierdzenie 8.12 *Jeśli P jest pierścieniem całkowitym o charakterystyce p, wówczas p jest liczbą pierwszą.*

Dowód. Gdyby charakterystyka pierścienia P była liczbą złożoną, powiedzmy char $(P) = mn$, $n, m \in \mathbb{N}, n, m > 1$, wówczas mielibyśmy $0 = (mn) \cdot 1_P = (m \cdot 1_P)(n \cdot 1_P)$ (por. 8.11). Ponieważ założyliśmy, że P jest pierścieniem całkowitym, a więc bez dzielników zera, mielibyśmy $m \cdot 1_P = 0$ lub $n \cdot 1_P = 0$, a to sprzeczne z twierdzeniem 8.11. Stąd charakterystyka pierścienia całkowtego musi być liczbą pierwszą. ■

Twierdzenie 8.13 *Jeśli pierścień P jest całkowity to rzędy dowolnych dwóch elementów różnych od zera są identyczne. (Inaczej: $\forall a, b \in P - \{0\} : |a| = |b|$.)*

Dowód. Przypuśćmy, że $a, b \in P - \{0_P\}$, gdzie P jest pierścieniem całkowitym i $|a| = m$, $|b| = n$. Mamy $0_P = (m \cdot a)b = a(m \cdot b)$. Stąd i z faktu, że w P nie ma dzielników zera wynika, że $m \cdot b = 0_P$. Bardzo podobnie wykazujemy, że $n \cdot a = 0_P$. Gdyby $n \neq m$, powiedzmy $m < n$, druga z tych równości oznacza sprzeczność z przyjętym założeniem $|b| = n$. ■

8.8 Zadania

Zadanie 8.1 Sprawdź, że zbiory:

- $\mathbf{Z} < \sqrt{-1} >= \{a + ib | a, b \in \mathbf{Z}\}$
- $\mathbf{Z} < \sqrt{3} >= \{a + \sqrt{3}b | a, b \in \mathbf{Z}\}$

z działaniami dodawania i mnożenia w zbiorze liczb zespolonych lub rzeczywistych, są pierścieniami. Podaj przykłady innych, podobnie skonstruowanych pierścieni.

Zadanie 8.2 W pierścieniu P oznaczmy przez P' zbiór dzielników zera pierścienia P. Sprawdź, że w zbiorze $P - P'$ mnożenie jest działaniem.
Zbadaj własności mnożenia w $P - P'$ dla pierścienia $\mathbf{Z}/(\text{mod } 6)$

Zadanie 8.3 Element a pierścienia P nazywamy **nilpotentnym**, jeżeli istnieje liczba całkowita l taka, że $a^p = 0$. Jeśli dodatkowo zachodzi $a^{l-1} \neq 0$, to l nazywamy **rzędem** elementu nilpotentnego $a \neq 0$. Rzędem elementu nilpotentnego 0 jest z definicji 1.
Co można powiedzieć o elementach nilpotentnych w pierścieniu całkowitym?
Zbadaj elementy nilpotentne pierścienia $\mathbf{Z}/(\text{ mod } 12)$.
Wykaż, że suma i iloczyn elementów nilpotentnych jest nilpotenna. Co można powiedzieć o ich rzędzie (nilpotencji)?

Zadanie 8.4 W przykładzie pierścieni $\mathbf{Z}/mod(n)$ wystąpiły sformułowania *łatwo sprawdzić* i *nietrudno wykazać*. Sprawdź więc i wykaż. Przyjrzyj się pierścieniom $\mathbf{Z}/mod(6)$ i $\mathbf{Z}/mod(7)$ (wypisz elementy tych pierścieni, utwórz tabelki ziałań, wskaż dzielniki zera (o ile istnieją)).

Zadanie 8.5 Udowodnij twierdzenie 8.2

Zadanie 8.6 Udowodnij twierdzenie 8.4.

Zadanie 8.7 Sprawdź, że $16\mathbb{Z}$ jest ideałem pierścienia $2\mathbb{Z}$. Z którym pierścieniem jest izomorficzny pierścień ilorazowy $2\mathbb{Z}/16\mathbb{Z}$?

Zadanie 8.8 Wykaż, że jeśli I i J są ideałami pierścienia P wówczas $I+J = \{a+b | a \in I, b \in J\}$ jest także ideałem pierścienia P.

Zadanie 8.9 $< \mathbf{x}^2 + 1 >$ oznacza ideał generowany przez wielomian $\mathbf{x}^2 + 1$ w pierścieniu $\mathbb{R}[\mathbf{x}]$. Wykaż, że $\mathbb{R}[\mathbf{x}]/ < \mathbf{x}^2 + 1 >$ jest pierścieniem elementów (klas) postaci $v+ < \mathbf{x}^2 + 1 >$, gdzie v jest wielomianem stopnia co najwyżej pierwszego.
Sprawdź, że $\mathbf{x}^2+ < \mathbf{x}^2 + 1 >$.

Zadanie 8.10 Opisz pierścień ilorazowy $\mathbb{Z}[i]/ < 3 + i >$. Wypisz wszystkie jego elementy.

Zadanie 8.11 Wykaż, że jeśli $n, m \in \mathbb{Z}, a \in P$ (gdzie P jest pewnym pierścieniem, wówczas

$$n(ma) = (nm)a$$

Zadanie 8.12 Udowodnij, że homomorfizm f pierścieni jest monomorfizmem wtedy i tylko wtedy gdy Ker $f = \{0\}$.

Zadanie 8.13 Wykaż, że jeśli $f : P \to Q$ jest homomorfizmem pierścieni wówczas Ker f jest ideałem pierścienia P.

Rozdział 9

Pierścienie Gaussa

W niniejszym rozdziale będziemy wszystkie rozważane pierścienie są całkowite (przemienne, bez dzielników zera i z jedynką) chyba, że zostanie to wyraźnie zaznaczone.

Definicja 9.1 *Pierścień P nazywamy* **pierścieniem z rozkładem** *jeżeli każdy element $a \in P$ nie będący jednością pierścienia P da się przedstawić jako iloczyn skończonej liczby elementów nierozkładalnych w P.*
Dwa rozkłady elementu a:

$$a = a_1 \cdot ... \cdot a_m \quad a = b_1 \cdot ... \cdot b_n$$

nazywamy **jednakowymi** *jeżeli*

1. $m = n$,
2. *istnieje permutacja $\sigma : [1, m] \to [1, m]$ taka, że elementy a_i oraz $b_{\sigma(i)}$ są stowarzyszone.*

Pierścień całkowity P nazywamy **pierścieniem Gaussa** [1] *jeśli każdy nie będący jednością element pierścienia P ma rozkład jednoznaczny (tzn. ma rozkład na iloczyn elementów nierozkładalnych i każde dwa rozkłady dowolnego elementu na iloczyn elementów nierozkładalnych są jednakowe).*

Przykład 9.1 **Z**, *$K[x]$ - gdzie K jest dowolnym ciałem, są pierścieniami Gaussa (dowód tych faktów będzie nieco później).*
Pierścień Dedekinda nie jest pierścieniem Gaussa (np. rozkład liczby 6 w tym pierścieniu nie jest jednoznaczny: $6 = 3 \cdot 2 = (1 + \sqrt{-5})((1 - \sqrt{-5}))$.

Twierdzenie 9.1 *Pierścień całkowity z rozkładem P jest pierścieniem Gaussa wtedy i tylko wtedy gdy każdy element nierozkładalny $a \in P$ jest w P elementem pierwszym.*

[1] Carl Friedrich Gauss (1777-1855). Nawet pobieżne wymienienie matematycznych osiągnięć Gaussa wykracza poza ramy niniejszego skryptu. Warto jednak wspomnieć, że uważa się go także za niemniej wybitnego fizyka, astronoma i geodetę. Ciekawostką jest, że podobnie jak najwybitniejszy polski matematyk Stefan Banach, nigdy nie ukończył studiów matematycznych i swój doktorat uzyskał bez zdawania obowiązkowego egzaminu doktorskiego.

Dowód.

- Przypuśćmy, że P jest pierścieniem Gaussa, $a \in P$ jest elementem nierozkładalny oraz $a \mid bc$ $(b, c \in P)$. Wówczas istnieje $d \in P$ takie, że $bc = ad$. Niech

$$\begin{aligned} b &= b_1 \cdot ... \cdot b_n \\ c &= c_1 \cdot ... \cdot c_m \\ d &= d_1 \cdot ... \cdot d_k \end{aligned}$$

będą rozkładami elementów b, c i d. Wówczas

$$b_1 \cdot ... \cdot b_n \cdot c_1 \cdot ... \cdot c_m = a \cdot d_1 \cdot ... \cdot d_k$$

Z jednoznaczności rozkładu w pierścieniu Gaussa wynika, że a jest stowarzyszone z jednym z elementów b_i (wówczas $a \mid b$) lub a jest stowarzyszone z jednym z c_j (i wtedy $a \mid c$). Tak więc $a \mid b$ lub $a \mid c$, dla dowolnych $b, c \in P$ takich, że $a = bc$, a to oznacza, że a est elementem pierwszym w P.

- Przypuśćmy teraz, że każdy element nierozkładalny jest elementem pierwszym pierścienia P. Wykażemy, że P jest pierścieniem Gaussa czyli, że każdy rozkład dowolnego elementu $a \in P$ na iloczyn elementów nierozkładalnych jest jednoznaczny.
Załóżmy, że

$$a = a_1 \cdot ... \cdot a_m = b_1 \cdot ... \cdot b_n \tag{9.1}$$

gdzie $a_1, ..., a_m, b_1, ..., b_n$ są elementami nierozkładalnymi. Wykażemy, że te rozkłady elementu a są jednakowe, za pomocą indukcji matematycznej.
Jeśli $m = n = 1$ otrzymujemy $a = a_1 = b_1$ i rozkłady jednakowymi oczywiście są.
Załóżmy teraz, że każde dwa rozkłady (9.1) takie, że $m, n \leq k$ są jednakowe i niech

$$a = a_1 \cdot ... \cdot a_k \cdot a_{k+1} = b_1 \cdot ... \cdot b_n \tag{9.2}$$

gdzie $n \leq k + 1$. Zatem a_{k+1} dzieli iloczyn $b_1 \cdot ... \cdot b_n$. Element a_{k+1} jest nierozkładalny z założenia, a więc pierwszy w P. Stąd dzieli jeden z elementów $b_1, ..., b_n$, powiedzmy, dla ustalenia uwagi, że $a_{k+1} \mid b_n$, a więc istnieje element $\alpha \in P$ taki, że $b_n = \alpha a_{k+1}$. Zauważmy, że b_n jest elementem nierozkładalnym, a więc α jest jednością. Wstawiając αa_{k+1} w miejsce b_n otrzymujemy (korzystając z przemienności)

$$a_1 \cdot ... \cdot a_k \cdot a_{k+1} = \alpha b_1 \cdot ... \cdot b_{n-1} a_{k+1}$$

Teraz korzystamy z prawa skracania i oznaczamy αb_1 przez b_1' (zauważmy, że skoro b_1 jest nierozkładalne, także b_1' jest nierozkładalne) i otrzymujemy

$$a_1 \cdot ... \cdot a_k = b_1' \cdot b_2 \cdot ... \cdot b_{n-1} \tag{9.3}$$

Wzór (9.3) to równość dwóch rozkładów elementu na iloczyny co najwyżej k elementów nierozkładalnych a więc, z założenia indukcyjnego, rozkłady (9.3) są

jednakowe. Poniważ na dodatek elementy b_n i a_{k+1} są stowarzyszone, rozkłady (9.2) są jednakowe. ■

Pierścień $\mathbb{Z}[\sqrt{-5}]$ jest pierścieniem liczbowym, który nie jest pierścieniem Gaussa. Rzeczywiście w tym pierścieniu element 6 ma dwa różne rozkłady na iloczyny czynników nierozkładalnych[2]:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

9.1 Pierścienie wielomianów

Dla wielomianu $v = v_0 + v_1 x + \cdots \in P[x]$ największe k_0 dla którego $v_{k_0} \neq 0$ nazywamy **stopniem wielomianu** v i oznaczmy przez $\partial(v)$. Stopniem wielomianu zerowego jest $-\infty$[3]. Współczynnik v_{k_0} nazywamy wtedy **współczynnikiem dominującym** wielomianu v.

Z łatwością można sprawdzić, prawdziwość następujących dwóch twierdzeń.

Twierdzenie 9.2 *Dla dowolnego pierścienia P zbiór $P[\mathbf{x}]$ jest pierścieniem. Jeśli P jest pierścieniem całkowitym, wówczas także $P[\mathbf{x}]$ jest pierścieniem całkowitym.* ■

Twierdzenie 9.3 *Dla dowolnego pierścienia P i wielomianów $v, w \in P[\mathbf{x}]$ zachodzą wzory:*

$$\partial(v + w) \leq \max\{\partial v, \partial w\}$$

$$\partial(vw) \leq \partial v + \partial w$$

Co więcej, druga z tych nierówności jest równością o ile P jest pierścieniem (przemiennym) bez dzielników zera. ■

Zauważmy, że z każdym wielomianem $w \in P[\mathbf{x}]$, $w = w_0 + w_1\mathbf{x} + \cdots + w_n\mathbf{x}^n$ można skojarzyć **funkcję wielomianową**:

$$w : P \ni x \to w(x) = w_0 + w_1 x + \cdots + w_n x^n \in P$$

Zbiór funkcji wielomianowych o współczynnikach w pierścieniu P oznaczamy przez $P(x)$. Jest oczywiste, że także $P(x)$ jest pierścieniem (przemiennym jeśli P jest przemienny, całkowitym, jeśli P jest całkowity).

[2] Czytelnikowi pozostawiam samodzielne wykazanie, że elementy $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ są w pierścieniu $\mathbb{Z}[\sqrt{-5}]$ (por. zadanie 9.1).

[3] Zauważmy, że wielomian zerowy $v = 0$ nie ma współczynnika $v_{k_0} \neq 0$. Można więc postąpić na dwa sposoby: albo nie definiować w ogóle stopnia wielomianu zerowego, albo zdefiniować go jako $-\infty$ i definiując $a + -\infty = 0$, $\max\{a, -\infty\} = a$, dla dowolnego $a \in \mathbf{Z}$, by wzory na stopień sumy i iloczynu wielomianów pozostały prawdziwe (sprawdź, że rzeczywiście tak jest!).

Twierdzenie 9.4 *Niech P będzie pierścieniem całkowitym i niech $p \in P[\mathbf{x}]$ będzie wielomianem którego współczynnik dominujący jest odwracalny. Dla każdego wielomianu $v \in P[\mathbf{x}]$ istnieją wielomiany $q, r \in P[\mathbf{x}]$ takie, że*

$$v = qp + r, \quad \partial r < \partial p \text{ lub } r = 0 \tag{9.4}$$

Wielomiany q i r o tych własnościach wyznaczone są jednoznacznie.

Dowód. Wykażemy wpierw istnienie wielomianów p oraz r.
Oznaczmy przez k stopień wielomianu v i przez m stopień wielomianu p. Dowód poprowadzimy przez indukcję ze względu na k.
Twierdzenie jest prawdziwe dla $k < m$. Rzeczywiście, wówczas $v = 0p + v$, $k = \deg v < \deg p = m$.
Przypuśćmy, że $k \geq m$ a także, że jeśli $v^* \in P[\mathbf{x}]$ jest wielomianem stopnia $k' < k$ wówczas istnieją wielomiany q^* oraz r^* takie, że $v^* = q^*p + r^*$, $\deg r^* < \deg p$ lub $r = 0$.
Oznaczmy przez v_k i p_m współczynniki dominujące wielomianów v i p. Z założenia element p_m jest odwracalny. Wielomian $\bar{v} = v - v_k p_m^{-1} \mathbf{x}^{k-m} p$ jest stopnia mniejszego od k. Z założenia indukcyjnego istnieją więc wielomiany $\bar{q}$ oraz r takie, że $\bar{v} = \bar{q}p + r$, $\deg r < \deg p$ lub $r = 0$. Wówczas $v - v_k p_m^{-1} \mathbf{x}^{k-m} p = \bar{q}p + r$, a zatem $v = (v_k p_m^{-1} \mathbf{x}^{k-m} + \bar{q})p + r$, co kończy dowód istnienia wielomianów q i r.

Pozostaje wykazać jedyność wielomianów q i r spełniających warunki (9.4). Przypuśćmy, że

$$v = qp + r$$

oraz

$$v = \bar{q}p + \bar{r}$$

przy czym $\partial r < \partial p$ lub $r = 0$ i $\partial \bar{r} < \partial p$ lub $\bar{r} = 0$. Wówczas $r - \bar{r} = (\bar{q} - q)p$, $\partial(r - \bar{r}) < \partial p$ lub $r - \bar{r} = 0$. Stąd już łatwo wywnioskować, że $\bar{q} = q$ i $r = \bar{r}$. ∎

9
1.2012

Wniosek 9.5 *Niech P będzie pierścieniem z jedynką. Reszta z dzielenia wielomianu $v \in P[\mathbf{x}]$ przez wielomian $\mathbf{x} - c$ jest równa $v(c)$.*

Dowód. Na mocy twierdzenia 9.4 możemy napisać

$$v = q(\mathbf{x} - c) + r$$

gdzie $\deg r = 0$ lub $r = 0$. Wówczas $v(c) = q(c)(c - c) + r(c)$, co oznacza, że $r(c) = v(c)$. Ponieważ zaś wielomian r może mieć jedynie współczynnik r_0 różny od zera (mówimy, że r *jest stały*), $r_0 = v(c)$. ∎

Element c pierścienia P nazywamy **pierwiastkiem wielomianu** $v \in P[\mathbf{x}]$ jeśli $v(c) = 0$.
Niech $v \in P[\mathbf{x}]$, gdzie P jest pewnym pierścieniem całkowitym, $v = q(\mathbf{x} - c) + r$, gdzie r jest wielomianem stopnia zero. Z wniosku 9.5 wynika, że c jest pierwiastkiem wielomianu v wtedy i tylko wtedy, gdy $\mathbf{x} - c$ dzieli v. Zapiszmy to spostrzeżenie

Wniosek 9.6 *Niech P będzie pierścieniem całkowitym. Wielomian $v \in P[\mathbf{x}]$ jest podzielny przez wielomian $\mathbf{x}-c$ wtedy i tylko wtedy, gdy c jest pierwiastkiem wielomianu v.* ■

Z wniosku 9.6 bardzo łatwo można wykazać jeszcze jeden, bardzo ważny wniosek.

Wniosek 9.7 *Niech P będzie pierścieniem całkowitym. Dowolny wielomian $v \in P[\mathbf{x}]$ stopnia k ma co najwyżej k pierwiastków.* ■

Twierdzenie 9.8 *Pierścień wielomianów $\mathbf{K}[\mathbf{x}]$ nad dowolnym ciałem $\mathbf{K}$ jest pierścieniem głównym.*

Dowód. Niech B będzie ideałem pierścienia $\mathbf{K}[\mathbf{x}]$. Jeśli $B = \{0\}$, to B jest oczywiście ideałem głównym, $B = (0)$. Przypuśćmy więc, że $B \neq \{0\}$. Wtedy w B są wielomiany niezerowe. Niech d będzie wielomianem niezerowym, minimalnego stopnia w B. Wykażemy, że $B = (d)$. W tym celu wystarczy wykazać, że dla dowolnego $b \in B$ istnieje $q \in \mathbf{K}[\mathbf{x}]$ takie, że $b = qd$.

Z twierdzenia o dzieleniu wielomianów (twierdzenie 9.4) wynika, że istnieją takie wielomiany $q, r \in \mathbf{K}[\mathbf{x}]$, że

$$b = qd + r \quad \deg r < \deg d$$

Stąd $r = b - qd \in B$. Jednak w ideale B jedynym wielomianem stopnia silnie mniejszego niż $\deg d$ jest wielomian $r = 0$, a więc $b = qd$, co należało udowodnić. ■

9.2 Pierścienie główne

Mówimy, że ciąg ideałów (I_n) pierścienia P jest *wstępujący* jeżeli

$$I_1 \subset I_2 \subset ... \subset I_k \subset ...$$

Dla dowolnego ciągu wstępującego ideałów (I_n) także ich mnogościowa suma $\bigcup_{n=1}^{+\infty} I_n$ jest ideałem. Rzeczywiście, jeśli $a, b \in I$, wówczas istnieją $i, j \in \mathbb{N}$ takie, że $a \in I_i, b \in I_j$. Bez straty ogólnoći można założyć, że $i \leq j$. Wówczas $a, b \in I_j$ i $a - b \in I_j$ a stąd oczywiście wynika, że $a - b \in I$. Dla dowolnego $\alpha \in P$ (i przy założeniu, że jak poprzednio, $a \in I_i$) $\alpha a \in I_i$ a więc $\alpha a \in I$.

Twierdzenie 9.9 *W pierścieniu głównym P każdy wstępujący ciąg ideałów*

$$I_1 \subset I_2 \subset \cdots \subset I_k \subset \ldots$$

jest stacjonarny, tzn. istnieje $k_0 \in \mathbf{N}$ takie, że

$$I_{k_0} = I_{k_0+1} = \ldots$$

Dowód. Wiemy już, że suma ideałów $C = \bigcup_{i=1}^{\infty} C_i$ iest ideałem. Ponieważ P, z założenia, jest pierścieniem głównym, istnieje $a \in P$ takie, że $I = (a)$. Oczywiście $a \in I$, a więc istnieje $k_0 \in \mathbf{N}$ takie, że $a \in I_{k_0}$.
Z definicji I (jako mnogościowej sumy I_i, $i \in \mathbf{N}$), wynika, że $I_{k_0} \subset I$. Z drugieje strony, skoro $a \in I_{k_0}$, to z definicji ideału $(a) \subset I_{k_0}$, a więc $I \subset I_{k_0}$ i ostatecznie: $I = I_{k_0}$. ■

10
2.2011

Największym wspólnym dzielnikiem elementów a i b pierścienia całkowitego P nazywamy element $d \in P$ spełniający warunek:

$$d|a,\ d|b \quad \text{oraz dla każdego } c \in P: \quad c|a, c|b \Rightarrow c|d$$

Ta definicja jest podobna do definicji największego wspólnego dzielnika dwóch liczb całkowitych z rozdziału 1. Największy wspólny dzielnik elementów a i b oznaczamy przez $\mathrm{NWD}(a, b)$ lub przez (a, b).

Jeżeli największym wspólnym dzielnikiem elementów a i b jest jedynka pierścienia (inaczej: jeżeli $(a, b) = 1$), wówczas mówimy, że a i b są **względnie pierwsze**. Wówczas jedynymi wspólnymi dzielnikami a i b są 1 i elementy stowarzyszone z 1 (a więc, elementy odwracalne pierścienia). Zamiast pisać $(a, b) = 1$ często piszemy $a \perp b$.

W pierścieniach głównych największy wspólny dzielnik dwóch elementów zawsze istnieje i można go zapisać w specjalnej postaci. Twierdzenie które o tym mówi nazwiemy **twierdzeniem o NWD w pierścieniu głównym**.

Twierdzenie 9.10 *Każde dwa elementy a, b pierścienia całkowitego i głównego P mają największy wspólny dzielnik $d \in P$ który jest ich kombinacją liniową, tzn. istnieją $s, t \in P$ takie, że*

$$d = sa + tb$$

Dowód. Rozważmy zbiór

$$S = \{s_1 a + t_1 b | s_1, t_1 \in P\}$$

Sprawdźmy wpierw, że S jest ideałem. Rzeczywiście, jeżeli $s, t \in S$ wówczas istnieją w P elementy $\alpha_1, \alpha_2, \beta_1, \beta_2$ takie, że $s = \alpha_1 a + \beta_1 b$ oraz $t = \alpha_2 a + \beta_2 b$ i wobec tego

$$s - t = (\alpha_1 + \alpha_2)a + (\beta_1 + \beta_2)b \in S$$

Dla dowolnego $c \in P$ zachodzi

$$cs = c(\alpha_1 a + \beta_1 b) = (c\alpha_1)a + (c\beta_1)b \in S$$

Ponieważ z założenia P jest pierścieniem głównym, ideał S jest główny, a więc istnieje $d \in P$ takie, że $S = (d)$. Element a można zapisać w postaci $a = 1a + 0b$ (pamiętamy, że P jest pierścieniem całkowitym), a więc $a \in S$. Podobnie wykazujemy,

że $b \in S$. Stąd wynika pczywiście, że $d|a$ oraz $d|b$.
Jeśli $c|a$ i $c|b$ wtedy istnieją $\alpha, \beta \in P$ takie że $a = \alpha c$ oraz $b = \beta c$. Wówczas

$$d = sa + tb = s\alpha c + t\beta c = (a\alpha + t\beta)c$$

i wobec tego $c|d$. ■

Jeżeli największym wspólnym dzielnikiem elementów a i b jest jedynka pierścienia (inaczej: jeżeli $(a, b) = 1$), wówczas mówimy, że a i b są **względnie pierwsze**. Wówczas jedynymi wspólnymi dzielnikami a i b są 1 i elementy stowarzyszone z 1 (a więc, elementy odwracalne pierścienia). Zamiast pisać $(a, b) = 1$ często piszemy $a \perp b$ (podobnie jak to robiliśmy dla liczb całkowitych).

Wniosek 9.11 *W dowolnym pierścieniu całkowitym i głównym*

$$(a, b) = 1 \Leftrightarrow \exists \alpha, \beta \in P : \alpha a + \beta b = 1$$

9.3 Pierścienie euklidesowe

Dla dowolnego pierścienia P oznaczmy przez P^* zbiór $P - \{0\}$.

Definicja 9.2 *Pierścień całkowity P nazywamy* **euklidesowym** *jeśli istnieje funkcja $h : P^* \to \mathbb{N}^+$ taka, że dla wszystkich $a \in P, b \in P^*$ istnieją $q, r \in P$ takie, że*

1. $a = bq + r$
2. *oraz albo* $r = 0$ *albo* $h(r) < h(b)$.

Potocznie mówimy, że pierścienie euklidesowe to *pierścienie całkowite z operacją dzielenia z resztą.*

Przykład 9.2 *Zbiór liczba całkowitych $\mathbb{Z}$ z funkcją $h(n) = |n|$ jest z pewnością najlepiej znanym przykładem pierścienia Euklidesa.*

Przykład 9.3 *Zbiór wielomianów $K[x]$, gdzie K jest pewnym ciałem, z funkcją $h(v) = \partial(v)$ jest, jak można łatwo sprawdzić, pierścieniem euklidesowym.*

Przykład 9.4 (Pierścień całkowitych liczb zespolonych) Niech $\mathbb{Z} < i >= \{a + bi : a, b \in \mathbb{Z}\}$ zaś $h(a + bi) = a^2 + b^2$. Wykażemy, że funkcja h tak zdefiniowana rzeczywiście spełnia postulaty definicji pierścienia euklidesowego.
Niech $a + bi \in \mathbb{Z}[i]$ i niech $c + di \in \mathbb{Z}[i]^*$. Oczywiście $\frac{a+bi}{c+di} = e + fi$, gdzie e i f są liczbami wymiernymi (żeby to zobaczyć wystarczy wymnożyć licznik i mianownik wyrażenia $\frac{a+bi}{c+di}$ przez $c - di$ i wykonać dzielenie). Wybierzmy teraz e_0 oraz f_0 tak, by $|e - e_0| \leq \frac{1}{2}$ i $|f - f_0| \leq \frac{1}{2}$.
Przyjrzyjmy się liczbie

$$r = a + bi - (c + di)(e_0 + f_0 i)$$

Oczywiście $a+bi = (c+di)(e_0+f_0i)+r$. Pozostaje więc wykazać, że $h(r) < |c+di|^2$.

$$h(r)| = |r|^2 = |a+bi-(c+di)(e_0+f_0i)|^2 =$$

$$= |(c+di)(e+fi)-(c+di)(e_0+f_0i)|^2 \leq |c+di|^2|e+fi-e_0-f_0i|^2 =$$

$$= |c+di|^2((e-e_0)^2+(f-f_0)^2) \leq |c+di|^2(\frac{1}{4}+\frac{1}{4}) = \frac{1}{2}(c^2+d^2) = h(c+di)$$

Wartość $h(a+ib) = a^2+b^2$ nazywana jest często *normą* $z = a+ib$.
Dla przykładu, niech $z_1 = 5+4i, z_2 = 1+2i$. Wtedy

$$\frac{z_1}{z_2} = \frac{5+4i}{1+2i} = \frac{(5+4i)(1-2i)}{(1+2i)(1-2i)} = \frac{13}{5}+\frac{-6}{5}i$$

Stosując oznaczenia używane powyżej mamy $e_0 = 3, f_0 = -1$ i wobec tego $r = 5+4i-(1+2i)(3-i) = -i$.
Ostatecznie $5+4i = (3-i)(1+2i)-i$. Oznacza to, że ilorazem $5+4i$ przez $1+2i$ jest $3-i$, przy czym resztą jest $r = -i$. $h(1+2i) = 5 < h(-i) = 1$.
Warto zauważyć, że $q = 3-2i$ oraz $r = 2$ także spełniają warunki oba warunki definicji 9.2, dla wynik dzielenia $5+4i$ przez $1+2i$ w pierścieniu $\mathbb{Z} < i >$ nie jest więc jednoznaczny.

Powyżej wykazaliśmy następujące twierdzenie.

Twierdzenie 9.12 *Pierścień $\mathbb{Z}[i]$ całkowitych liczb zespolonych jest euklidesowy.*

To zaś twierdzenie jest szczególnie istotne ze względu na następne.

Twierdzenie 9.13 *Każdy pierścień euklidesowy jest pierścieniem głównym.*

Dowód. Niech I będzie dowolnym ideałem pierścienia euklidowskiego P. Wykażemy, że I jest ideałem głównym. Gdyby $I = \{0\}$ wówczas mielibyśmy $= (0)$, czyli I byłby ideałem generowanym przez 0 (i zawierającym 0 jako swój jedyny element. Możemy więc przypuścić, że $I \neq \{0\}$ czyli, że I zawiera elementy niezerowe. Niech m będzie najmniejszą liczbą dodatnią w zbiorze $h(I-\{0\})$, gdzie $h : P^* \to \mathbb{N}^+$ jest funkcją jak w definicji 9.2 pierścienia euklidesowego. Niech $b \in I$ będzie takie, że $h(b) = m$. Naturalnie $b \neq 0$. Wykażemy, że $I = (b)$.
Ponieważ I jest ideałem i $b \in I$ mamy $(b) \subset I$.
Wystarczy więc wykazać, że każdy element $a \in I$ jest krotnością elementu b. Rzeczywiście, skoro $b \in P^*$ i P jest pierścieniem euklidesowym istnieją $q, r \in P$ takie, że $a = bq+r$, $h(r) < h(b)$ albo $r = 0$.
Jeśli $r = 0$, to a jest krotnością b i dowód jest zakończony. Przypuśćmy więc, że $r \neq 0$. Wtedy $r = a-bq$. Ponieważ $b \in I$, to $bg \in I$ (z definicji ideału). Wobec tego $r = a-bq \in I$, a to sprzeczne z założeniem o minimalności $h(b)$. ■

W pierścieniach euklidesowych funkcjonuje algorytm Euklidesa podobny do tego, który znamy dla liczb całkowitych.

ALGORYTM EUKLIDESA W PIERŚCIENIU EUKLIDESOWYM

Niech P będzie pierścieniem euklidesowym, $a, b \in P$.
Określmy rekurencyjnie następujący ciąg (r_i).

- $r_0 = a, r_1 = b$
- $r_i = q_{i+1}r_{i+1} + r_{i+2}$ gdzie $h(r_{i+2}) < h(r_{i+1})$

Oczywiście mamy wtedy $h(r_1) < h(r_2) < ...$, a ponieważ funkcja h na mocy definicji (pierścienia euklidesowego) przyjmuje wartości naturalne, ciąg (r_i) jest skończony. Powiedzmy, że ostatnim niezerowym wyrazem ciągu (r_i) jest r_k (oznacza to, że $r_{k+1} = 0$ i r_{k+1} jest ostatnim wyrazem ciągu (r_i)). Mamy wtedy równość $r_{k-1} = q_k r_k$.
Zauważmy także, że z równości

$$r_i = q_{i+1}r_{i+1} + r_{i+2}$$

wynika, że

- jeśli jakiś element $d \in P$ dzieli r_i oraz r_{i+1} wówczas d dzieli r_{i+2}
- jeśli $d \in P$ dzieli r_{i+1} oraz r_{i+2} wówczas d dzieli r_i

Stąd łatwo wywnioskować, że $r_r = NWD(r_{k-1}, r_{k-2}) = ... = NWD(r_1, r_0) = NWD(a, b)$.
Co więcej, korzystając z ciągu równości $r_i = q_{i+1}r_{i+1} + r_{i+2}$ łatwo wyliczyć wartość $r_k = NWD(a, b)$.

9.4 Zasadnicze Twierdzenie Arytmetyki

Następujące twierdzenie nazywa się Zasadniczym Twierdzeniem Arytmetyki lub Twierdzeniem o Jednoznacznej Faktoryzacji.

Twierdzenie 9.14 *Każdy całkowity pierścień główny jest pierścieniem Gaussa.*

Dowód. Musimy udowodnić dwa fakty. Po pierwsze, że każdy pierścień główny jest pierścieniem z rozkładem a po drugie, że w pierścieniu głównym rozkład na iloczyn elementów nierozkładalnych jest jednoznaczny.
Dowód istnienia rozkładu. Dla dowodu nie wprost, przypuśćmy, że a jest elementem pierścienia głównego P takim, który nie ma faktoryzacji. Oczywiście a nie jest elementem nierozkładalnym (bo wtedy miałby jednoelementowy rozkład). Istnieją więc $a_1, b_1 \in P$ takie, że

$$a = a_1 b_1$$

i jeden z czynników, na przykład a_1 nie jest nierozkładalny (w przeciwnym przypadku $a = a_1 b_1$ byłoby rozkładem na czynniki nierozkładalne. Mamy więc, powiedzmy, $a_1 = a_2 b_2$ a stąd

$$a = a_2 b_2 b_1$$

i znowu, jeden z czynników, na przykład a_2 nie jest rozkładalny. Takie rozumowanie można powtarzać dowolną liczbę razy otrzymując

$$a = a_n b_n b_{n-1} \cdot ... \cdot b_2 b_1$$

przy czym jeden z elementów $a_n, b_n, ..., b_1$ jest rozkładalny (można przyjąć, że tym rozkładalnym elementem jest a_n (jeśli nie, to odpowiednio korygujemy oznaczenia). W efekcie otrzymujemy nieskończony ciąg ideałów głównych

$$(a) \subset (a_1) \subset ... \subset (a_n) \subset ...$$

przy czym każde zawieranie jest silne (to znaczy $(a_i) \neq (a_{i+1})$. A to sprzeczne z twierdzeniem 9.9.

Dowód jednoznaczności, jak zobaczymy, wynika z twierdzenia 9.1.

Rzeczywiście, na mocy twierdzenia 9.1 wystarczy wykazać, że dowolny element nierozkładalny $p \in P$ jest w P elementem pierwszym. Przypuśćmy, że $p \mid ab$ i p nie dzieli ani a ani b. Zauważmy, że stąd wynika natychmiast, że p nie jest jednością, bowiem każda jedność dzieli dowolny element pierścienia.

Zarówno a jak i b nie dzielą p, bowiem p jest nierozkładalne. Oba te elementy są więc względnie pierwsze z p, czyli

$$(a, p) = 1$$

oraz

$$(b, p) = 1$$

A więc, na mocy wniosku 9.11, istnieją $\alpha, \beta, \gamma, \delta \in P$ takie, że

$$\alpha a + \beta p = 1$$

oraz

$$\gamma b + \delta p = 1$$

Po wymnożeniu powyższych równości stronami (i uporządkowaniu) otrzymujemy

$$\alpha\gamma ab + p(\beta\gamma b + \alpha\delta a + \beta\delta p) = 1$$

Skoro jednak $p \mid ab$, $p \mid 1$. A więc p byłoby jednością co, jak stwierdziliśmy wyżej, nie jest prawdą. ■

Oczywiście, skoro każdy pierścień euklidesowy jest pierścieniem głównym (na mocy twierdzenia 9.13), prawdziwy jest następujący wniosek.

Wniosek 9.15 *Każdy pierścień Euklidesa jest pierścieniem Gaussa.* ■

Stąd zaś i z twierdzenia 9.12 łatwo otrzymujemy następny.

Wniosek 9.16 *Pierścień liczb całkowitych zespolonych $\mathbb{Z}[i]$ jest pierścieniem Gaussa.*

9.5 Ciało ułamków pierścienia całkowitego

Skoro pojęcie pierścienia zostało już przyswojone, definicję ciała 8.1 można krótko przypomnieć następująco. Zbiór F wyposażony w dwa działania: addytywne i multyplikatywne nazywamy **ciałem** jeżeli z tymi działaniami

- F jest pierścieniem całkowitym oraz
- każdy element $a \in F$ różny od zera ma element odwrotnny ze względu na działanie oznaczone multyplikatywnie (a więc istnieje $a^{-1} \in F$ takie, że $a \cdot a^{-1} = 1$).

Każdy niepusty podzbiór F' ciała F, który z działaniami w F jest ciałem, nazywamy **podciałem** ciała F. Z pewnością najlepiej znanym nam ciałem jest ciało liczb rzeczywistych $\mathbb{R}$, którego podciałem jest ciało liczb wymiernych $\mathbb{Q}$. Z kolei ciało $\mathbb{R}$ jest podciałem ciała liczb zespolonych $\mathbb{C}$[4].

Łatwym ćwiczeniem może być udowodnienie następującego warunku koniecznego i wystarczającego dla podciał.

Twierdzenie 9.17 *Niepusty podzbiór F' ciała F jest podciałem wtedy i tylko wtedy gdy*

- *dla dowolnych $a, b \in F' : a - b \in F'$*
- *dla dowolnych $a, b \in F'$ takich, że $b \neq 0 : ab^{-1} \in F'$*

Niech P będzie pierścieniem całkowitym, $P^* = P - \{0\}$. W zbiorze $Q = P \times P^*$ zdefiniujmy dwa działania:

$$(a, b) + (c, d) = (ad + bc, bd) \tag{9.5}$$

$$(a, b) \cdot (c, d) = (ac, bd) \tag{9.6}$$

oraz relację R:

$$(a, b)R(c, d) \iff ad = bc \tag{9.7}$$

Twierdzenie 9.18 *Dla dowolnego pierścienia całkowitego P relacja R zdefiniowana wzorem (9.7) jest relacją równoważności zgodną z działaniami (9.5) i (9.6).*

Dzięki twierdzeniu 9.18 w zbiorze ilorazowym $P \times P^*/R$ można wprowadzić działania dodawania i mnożenia:

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)] \tag{9.8}$$

$$[(a, b)] \cdot [(c, d)] = [(ac, bd)] \tag{9.9}$$

[4] Tu traktujemy liczby rzeczywiste jako liczby zespolone o części urojonej równej zero.

Twierdzenie 9.19 (O ciele ułamków) *Dla dowolnego pierścienia całkowitego P zbiór $P \times P^*/R$ z działaniami zdefiniowanymi wzorami 9.8 i 9.9 jest ciałem przemiennym.*

Ciało występujące w tezie twierdzenia 9.19 nazywamy **ciałem ułamków** pierścienia P. Z oczywistch powodów będziemy raczej stosowali zapis $\frac{a}{b}$ zamiast $[(a,b)]$ dla elementów ciała ułamków. Elementy ciała ułamków zapisujemy więc dokładnie tak samo jak doskonale nam znane ułamki (elemty ciała liczby wymiernych).

9.6 Homomorfizmy pierścieni

Odwzorowanie $h : P \to Q$ pierścienia P w pierścień Q jest **homomorfizmem** jeśli spełnia warunki

1. $h(a+b) = h(a) + h(b)$
2. $h(ab) = h(a)h(b)$

dla dowolnych $a, b \in P$. $Im\ h = h(P)$ nazywamy **obrazem** zaś $Ker\ h = h^{-1}[0]$ **jądrem** homomorfizmu h.

Twierdzenie 9.20 *1. Obraz homomorfizmu pierścieni $h : P \to Q$ jest podpierścieniem pierścienia Q.*

2. Jądro homomorfizmu pierścieni $h : P \to Q$ jest ideałem pierścienia P.

Dowód twierdzenia 9.20 jest pozostawiony Czytelnikowi jako zadanie 9.3.

Twierdzenie 9.21 *Jeśli P jest pierściniem a I jego ideałem, wówczas odwzorowanie $k : P \to P/I$ zdefiniowane wzorem*

$$k(a) = a + I$$

jest homomorfizmem (zwanym **homomorfizmem kanonicznym***).*

Twierdzenie 9.22 *Dla dowolnych pierścieni P, Q homomorfizm pierścieni $h : P \to Q$ jest monomorfizmem wtedy i tylko wtedy, gdy $Ker\ \ h = \{0\}$.*

Dowód. Dla dowolnego homomorfizmu pierścieni $h : P \to Q$ zachodzi $h(0) = h(0+0) = h(0) + h(0)$ i stąd $h(0) = 0$.
Jeśli h jest monomorfizmem, wówczas jedynym elementem a pierścienia P, dla którego $h(0) = 0$ jest $a = 0$ i stąd już wynika, że Ker $k = \{0\}$.
Jeśli Ker $h = \{0\}$ i $h(a) = h(b)$, wówczas $h(a-b) = 0$ i stąd $h(a) - h(b) = 0$. To zaś oznacza, że $h(a) = h(b)$, skąd wynika, że h jest monomorfizmem. ■

Twierdzenie 9.23 (Podstawowe o izomorfizmie pierścieni) *Jeśli $h : P \to Q$ jest epimorfizmem pierścienia na pierścień Q, wówczas zachodzi wzór*

$$h = \tilde{h} \circ k$$

gdzie $k : P \to P/Ker\ h$ jest homomorfizmem kanonicznym, zaś $\tilde{h} : P/Ker\ h \to Q$ izomorfizmem przyporządkowującym każdej klasie elementów $P/Ker\ h$ ich wspólną wartość w homomorfizmie k.

Dow. ...

Twierdzenie 9.23 można wypowiedzieć inaczej tak: *każdy epimorfizm pierścieni można przedstawić jako złożenie homomorfizmu kanonicznego i pewnego izomorfizmu.* w. 11 11.12.2012

9.7 Wielomiany nad pierścieniami Gaussa

Niech P będzie pierścisniem Gaussa (a więc pierścieniem całkowitym z rozkładem jednoznacznym) i niech $v \in P[\mathbf{x}]$. Wiemy, że $P[\mathbf{x}]$ jest pierścieniem całkowitym a także, że zbiór elementów stowarzyszonych z jednością w pierścieniu $P[\mathbf{x}]$ jest grupą (z działaniem mnożenia). Grupa ta jest identyczna z grupą jedności pierścienia P. Wielomian $v \in P[\mathbf{x}]$ jest rozkładalny jeżeli można napisać go w postaci $v = pq$, gdzie $p, q \in P[\mathbf{x}]$ i żaden z wielomianów p, q nie jest jednościĄ. Stąd na przykład wielomian $5\mathbf{x}^2 + 5 \in \mathbb{Z}[\mathbf{x}]$ jest rozkładalny. Mamy bowiem $5\mathbf{x}^2 + 5 = 5(\mathbf{x}^2 + 1)$ i żaden z wielomianów $p = 5$, $q = \mathbf{x}^2 + 1$ nie jest odwracalny w $\mathbb{Z}[\mathbf{x}]$.

Mówimy, że wielomian $p = a_0 + a_1\mathbf{x} + \cdots + a_n\mathbf{x}^n$ jest **pierwotny** jeżeli $(a_0, a_1, \ldots, a_n) = 1$ (współczynniki wielomianu p są względnie pierwsze).

Każdy wielomian nierozkładalny jest pierwotny. Wielomian $\mathbf{x}^2 + 2\mathbf{x} + 1 \in \mathbb{Z}[\mathbf{x}]$ jest przykładem wielomianu pierwotnego, który nie jest nierozkładalny.

Twierdzenie 9.24 *Niech P będzie pierścieniem Gaussa. Jeśli wielomian $p \in P[\mathbf{x}]$ jest pierwotny, $a \mid bp$ (dla pewnych $a, b \in P, p \neq 0$) wówczas $a \mid b$.*

Dowód. Rzeczywiście, jeśli $a \mid bp$ wówczas a dzieli wszystkie współczynniki wielomianu bp, czyli dzieli b. ■

Warto zwrócić uwagę, jak w tym prostym rozumowaniu, które jest dowodem twierdzenia 9.24 interweniuje fakt, że P jest pierścieniem Gaussa. W rzeczywistości korzystamy tu z faktu, że a można jednoznacznie zapisać jako iloczyn elementów nierozkładalnych (a więc pierwszych, bowiem pierścień jest Gaussa), powiedzmy $a = a_1, ..., a_k$, z których każdy dzieli b (bo nie dzieli któregoś ze spółczynników wielomianu p. poprawić- uzupełnić

Z twierdzenia 9.24 natychmiast wynika następujący wniosek.

Wniosek 9.25 *Jeśli $p, q \in P[\mathbf{x}]$ są wielomianami pierwotnymi, P pierścieniem Gaussa oraz $ap = bq$ $(a, b \neq 0)$ wówczas a i b są elementami stowarzyszonymi.*

Twierdzenie 9.26 *Każdy element pierwszy dowolnego pierścienia Gaussa P jest także elementem pierwszym $P[x]$.*

Dowód. Niech $a \in P$ będzie elementem pierwszym pierścienia P i przypuśćmy, że $a \mid pq$, gdzie $p, q \in P[\mathbf{x}]$, $p = a_0 + a_1\mathbf{x} + ... + a_n\mathbf{x}^n, q = b_0 + b_1\mathbf{x} + ... + b_m\mathbf{x}^m$. Przypuśćmy, że $a \not| p$ i $a \not| q$. Wtedy istnieją indeksy i, j takie, że $a \not| a_i$ oraz $a \not| b_j$. Niech i_0 oraz j_0 będą minimalne z tą własnością. Oznacza to, że

$$a \mid a_0, ..., a \mid a_{i_0-1}, a \not| a_{i_0}, \quad a \mid b_{j_0}, ..., a \mid b_{j_0-1}, a \not| b_{j_0}$$

Współczynnikiem przy $\mathbf{x}^{i_0+j_0}$ wielomianu pq jest

$$c_{i_0+j_0} = a_0b_{i_0+j_0} + a_1b_{i_0+j_0-1} + ... + a_{i_0-1}b_{j_0+1} + a_{i_0}b_{j_0} + a_{i_0+1}b_{j_0-1} + ... + a_{i_0+j_0}b_0$$

Ponieważ

$$a \mid a_0b_{i_0+j_0} + a_1b_{i_0+j_0-1} + ... + a_{i_0-1}b_{j_0+1}$$
$$a \mid a_{i_0+1}b_{j_0-1} + ... + a_{i_0+j_0}b_0$$

oraz, z założenia

$$a \mid c_{i_0+j_0}$$

otrzymujemy

$$a \mid a_{i_0}b_{j_0}$$

Wiemy jednak, że a jest elementem pierwszym w P i stąd mamy $a \mid a_{i_0}$ lub $a \mid b_{j_0}$. Otrzymana sprzeczność kończy dowód twierdzenia. ■

Twierdzenie 9.27 (Lemat Gaussa) *Jeśli P jest pierścieniem Gaussa, $p, q \in P[x]$ są wielomianami pierwotnymi to iloczyn pq jest wielomianem pierwotnym.*

Dowód. Rzeczywiście, jeśli pq nie byłby wielomianem pierwotnym, to byłby podzielny przez pewien element pierwszy, powiedzmy $a \in P$, pierścienia P, a wtedy na mocy twierdzenia 9.26 $a|p$ lub $a|q$. ■

Następny wniosek jest prostą, dającą się łatwo udowodnić przez indukcję, konsekwencją Lematu Gaussa.

Wniosek 9.28 *Iloczyn dowolnej liczby wielomianów pierwotnych nad pierścieniem Gaussa jest wielomianem pierwotnym.*

Powiedzmy, że P jest pewnym pierścieniem całkowitym. Przez F oznaczmy ciało ułamków pierścienia P. Możemy wtedy każdy element a pierścienia P uważać za element ciała F. W rzeczy samej, ciało F jest także pierścieniem, pierścień P jest izomorficzny z pierścieniem $A = \{\frac{a}{1} : a \in P\}$ - izomorfizmem pierścieni P i A jest

$$f : P \ni a \longrightarrow \frac{a}{1} \in A$$

Niech $p \in P[\mathbf{x}]$ będzie pewnym wielomianem o współczynnikach w pierścieniu P. Na zasadzie wyżej opisanego izomorfizmu możemy wielomian p traktować jako wielomian o współczynnikach z F, czyli $p \in F[\mathbf{x}]$.

Okazuje się, że każdy wielomian nierozkładalny w $P[\mathbf{x}]$ jest nierozkładalny w $F[\mathbf{x}]$. To twierdzenie, które niezupełnie jest zgodne z pierwszą intuicją. Co więcej, cytowany powyżej wielomian $5\mathbf{x}+5$ jest przykładem wielomianu rozkładalnego w $\mathbb{Z}[\mathbf{x}]$ natomiast nierozkładalnym nad ciałem ułamków $\mathbb{Q}$ pierścienia $\mathbb{Z}$.

Twierdzenie 9.29 *Niech P będzie pierścieniem Gaussa zaś F ciałem ułamków pierścienia P. Jeśli $p \in P[\mathbf{x}]$ jest wielomianem nierozkładalnym w $P[\mathbf{x}]$, wówczas p jest także nierozkładalny w $F[\mathbf{x}]$.*

Dowód. Przypuśćmy, że $p \in P[\mathbf{x}]$ jest nierozkładalny w $P[\mathbf{x}]$ i ma w $F[\mathbf{x}]$ rozkład właściwy postaci

$$p = p_1 \cdot p_2 \cdot ... \cdot p_k$$

gdzie $p_1, ..., p_k \in F[\mathbf{x}], k > 1$. Wielomiany $p_1, ..., p_k$ są nierozkładalne w $F[\mathbf{x}]$ i każdy z nich można napisać w postaci $p_i = \frac{a_i}{b_i} q_i$, gdzie $q_i \in P[\mathbf{x}]$ jest wielomianem pierwotnym (q_i jest wspólnym mianownikiem wszystkich współczynników wielomianu q_i natomiast a_i największym wspólnym dzielnikiem liczników tych współczynników). Mamy więc

$$p = \frac{a}{b} q_1 \cdot ... \cdot q_k$$

czyli

$$bp = aq_1 \cdot ... \cdot q_k$$

gdzie $q_1, ..., q_k$ są wielomianami pierwotnymi.

Na mocy Lematu Gaussa (twierdzenie 9.27 i wniosek 9.28) wielomian $q_1 \cdot ... \cdot q_k$ jest pierwotny. Korzystając z twierdzenia 9.24 b dzieli a, a więc $c = \frac{a}{b} \in P$ i $p = cq_1 \cdot ...q_k$ jest właściwym rozkładem p w $P[\mathbf{x}]$, a to sprzeczne z założeniem, że p jest wielomianem nad P nierozkładalnym. Ta sprzeczność kończy dowód twierdzenia. ■

Wniosek 9.30 *Niech P będzie pierścieniem Gaussa. Każdy wielomian nierozkładalny w $P[x]$ jest elementem pierwszym pierścienia $P[x]$.*

Dowód. Załóżmy, że $p \in P[\mathbf{x}]$ jest wielomianem nierozkładalnym. załóżmy, że $p \mid u \cdot v$, gdzie $u, v \in P[\mathbf{x}]$. Skoro P jest pierścieniem Gaussa, wielomian p jest także nierozkładalny nad ciałem F ułamków pierścienia P (twierdzenie 9.29). Pierścień $F[\mathbf{x}]$ jest, jak wiemy, pierścieniem Gaussa - wynika to bezpośrednio z twierdzeń 9.8 i 9.14 (Zasadnicze Twierdzenie Arytmetyki). Zatem p jest w $F[\mathbf{x}]$ elementem pierwszym i wobec tego p (w pierścieniu $F[\mathbf{x}]$!) dzieli jeden z wielomianów u, v. Powiedzmy, że $p|u$, czyli istnieje wielomian $q \in F[\mathbf{x}]$ taki, że $u = pq$. Rozumując podobnie jak w dowodzie twierdzenia 9.29 można znaleźć $a, b \in P$ takie, że $q = \frac{a}{b} w$, gdzie $w \in P[\mathbf{x}]$ jest wielomianem pierwotnym. Mamy wtedy

$$bu = apw$$

Iloczyn pw wielomianów pierwotnych jest, na mocy Lematu Gaussa, wielomianem pierwotnym. Z twierdzenia 9.24 wynika, że b dzieli element a, powiedzmy $c = \frac{a}{b}$. Zatem $u = cpw$ co oznacza, że wielomian p dzieli u w $P[\mathbf{x}]$. ■

9.8 Twierdzenie Gaussa

Twierdzeń udowodnionych przez Gaussa jest bardzo wiele, z niektórymi z nich zetknęliśmy się już poprzednio. Jednak nazwę *twierdzenie Gaussa* odnosi się zazwyczaj do twierdzenia następującego[5].

Twierdzenie 9.31 (Gauss) *Pierścień wielomianów nad pierścieniem Gaussa jest pierścieniem Gaussa.*

Dowód. Niech P będzie pierścieniem Gaussa. Przypomnijmy wpierw, że udowodniliśmy, (twierdzenie 9.1), iż pierścień z rozkładem jest pierścieniem Gaussa wtedy i tylko wtedy, gdy każdy jego element nierozkładalny jest także elementem pierwszym. Dalej, wykazaliśmy (wniosek 9.30), że dowolny wielomian nierozkładalny nad pierścieniem Gaussa P jest elementem pierwszym $P[\mathbf{x}]$[6]. Do wykazania naszego twierdzenia pozostaje więc udowodnić, że $P[\mathbf{x}]$ jest pierścieniem z rozkładem.
Wiemy już jednak, że $F[\mathbf{x}]$ jest pierścieniem z rozkładem, widzieliśmy bowiem, że dla dowolnego ciała K pierścień $K[\mathbf{x}]$ jest pierścieniem euklidesowym, każdy pierścień euklidesowy jest główny, a każdy pierścień główny jest Gaussa (Twierdzenie Zasadnicze Arytmetyki)..
Niech $p \in P[\mathbf{x}]$. Mamy

$$p = p_1 \cdot ... \cdot p_k$$

gdzie $p_1, ..., p_k \in F[\mathbf{x}]$ są wielomianami nierozkładalnymi w $F[\mathbf{x}]$ (a więc także nierozkładalnymi w $P[\mathbf{x}]$). Dokładnie tak, jak to zrobiliśmy w dowodzie twierdzenia 9.29 możemy napisać

$$p = cq_1 \cdot ... \cdot q_k$$

gdzie $c \in P$, natomiast $q_1, ..., q_k$ są wielomianami pierwotnymi i nierozkładalnymi w $P[\mathbf{x}]$. Oczywiście c także można rozłożyć na iloczyn czynników nierozkładalnych w P. Rzeczywiście, pierścień P jest Gaussa, a więc każdy jego element ma jednoznaczny rozkład na iloczyn elementów nierozkładalnych, które, na dodatek, są elementami pierwszymi w P - a jako elementy pierwsze w pierścieniu P są pierwsze w $P[\mathbf{x}]$ (twierdzenie 9.26), a więc w $P[\mathbf{x}]$ nierozkładalne. ■

9.9 Wielomiany nieprzywiedlne

Niech v będzie wielomianem o współczynnikach w pewnym pierścieniu całkowitym P. Taki wielomian można w dość oczywisty sposób traktować jako wielomian nad ciałem ułamków F pierścienia P. Można sformułować pytanie, kiedy element $\frac{a}{b}$ ciała F może być pierwiastkiem v? Okazuje się, że jeśli P jest pierścieniem Gaussa odpowiedź na to tytanie jest taka, jak w znanym zeszkoły średniej twierdzeniu dotyczącym wielomianów o współczynnikach całkowitych.

[5] Gauss udowodnił to twierdzenie w 1799 roku czyli gdy miał 22 lata. Podał jego kilkanaście dowodów.

[6] Pamiętamy, rzecz jasna, że w dowolnym pierścieniu każdy element pierwszy jest nierozkładalny.

Twierdzenie 9.32 *Jeśli element $\frac{a}{b}$ ciała ułamków F pierścienia Gaussa P, gdzie $a \perp b$, jest pierwiastkiem wielomianu*

$$P[x] \ni v = a_0 + a_1\mathbf{x} + \cdots + a_n\mathbf{x}^n$$

stopnia n, wówczas a dzieli a_0 i b dzieli a_n.

Dowód. Przypuśćmy, że $\frac{a}{b}$ jest pierwiastkiem wielomianu v (w ciele ułamków F). Oznacza to, że

$$a_0 + a_1\frac{a}{b} + ... + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + a_n\frac{a^n}{b^n} = 0$$

Mnożąc tę równość przez b^n otrzymujemy

$$a_0b^n + a_1ab^{n-1} + ... + a_{n-1}a^{n-1}b + a_na^n = 0$$

Oznaczmy przez $\alpha = a_0b^n + a_1ab^{n-1} + ... + a_{n-1}a^{n-1}b$ i przez $\beta = a_1ab^{n-1} + ... + a_{n-1}a^{n-1}b + a_na^n = 0$. Skoro b dzieli α oraz $\alpha + a_na^n$ (bo $\alpha + a_na^n = 0$), a na dodatek $a \perp b$, to b dzieli także a_n[7].
Podobnie z faktu, że a dzieli β wynika, że a dzieli a_0. ■

Bardzo często zamiast mówić, że wielomian jest nierozkładalny mówimy, że jest **nieprzywiedlny**. Kryterium Eisensteina[8] bardzo ważnym, często stosowanym warunkiem wystarczającym nieprzywiedlności wielomianów nad pierścieniem Gaussa.

Twierdzenie 9.33 *Niech P będzie pierścieniem Gaussa, $v \in P[x]$, $v = a_0 + a_1\mathbf{x} + \cdots + a_n\mathbf{x}^n$. Jeśli istnieje element pierwszy a w P taki, że*

1. $a|a_0,\ a|a_1,\ \ldots, a|a_{n-1}$,
2. $a \not| a_n$,
3. $a^2 \not| a_0$

wówczas v jest nierozkładalny w P .

Dowód. Twierdzenie udowodnimy metodą nie wprost. Przypuśćmy, że istnieją wielomiany $u = b_0 + b_1\mathbf{x} + \cdots + b_k\mathbf{x}^k$ oraz $w = c_0 + c_1\mathbf{x} + \cdots + c_l\mathbf{x}^l$ w $P[\mathbf{x}]$ takie, że $v = uw$. Wówczas

$$a_0 = b_0c_0$$

[7]Zauważmy, że to właśnie w tym miejscu korzystamy z faktu, że P jest pierścieniem Gaussa. Rzeczywiście, skoro a i b nie mają wspólnych (nietrywialnych) dzielników, to także b i a^n nie mają wspólnych dzielników. Skoro więc $b \mid a_na^n$, to b dzieli a_n.

[8]Ferdinand Eisenstein (1823-1852) jest postacią ze wszech miar godną uwagi. Pochodził z bardzo skromnej rodziny, był pochodzenia żydowskiego. Wiele zawdzięczał Aleksandrowi von Humboldtowi, który odkrył jego talent i pomagał mu w karierze. W roku 1844 dwudziestojednoletni Eisenstein opublikował 23 artykuły naukowe i rok później otrzymał honorowy doktorat Uniwersytetu we Wrocławiu (jeszcze przedtem nim uzyskał habilitacje, w wieku lat 24 w Berlinie). Był członkiem Akademii w Getyndze i w Berlinie. Gauss miał o nim powiedzieć, że *było tylko trzech matematyków o epokowym znaczeniu: Archimedes, Newton i Eisenstein.*

Ponieważ $a|a_0$ i a jest elementem pierwszym, a dzieli jeden z elementów b_0, c_0. Co więcej, a nie może dzielić zarówno b_0 jak i c_0, w przeciwnym bowiem przypadku a dzieliłoby a_0^2. Bez straty ogólności możemy założyć, że $a|b_0$ i $a \not| c_0$.
Oczywiście $a_1 = b_0c_1 + b_1c_0$. Ponieważ $a|a_1$ i $a|b_0$ więc $a|b_1c_0$. Skoro jednak $a \not| c_0$, a dzieli b_1. Wykażemy, że a dzieli wszystkie współczynniki wielomianu v.
Przypuśćmy, że wykazaliśmy już, że

$$a|b_0, a|b_1, \cdots, a|b_{j-1}$$

dla pewnego $j \leq n$. Z faktu, że $a_j = b_0c_j + a_1c_{j-1} + \cdots + b_jc_0$, $a|b_0, a|b_1, \cdots, a|b_{j-1}, a|a_j$ wynika, że $a|b_jc_0$ a stąd $a|b_j$ (pamiętamy, że $a \not| c_0$).
Teraz już oczywistym jest, że udowodniliśmy (metodą indukcji), że $a|b_k$. Ponieważ jednak $b_kc_l = a_n$, korzystając kolejny raz z założenia, że a jest elementym pierwszym pierścienia P, dochodzimy do wniosku, że $a|a_n$. Ta sprzeczność kończy dowód twierdzenia. ■

Zauważmy, że dla dowolnego $n \geq 1$ wielomian $\mathbf{x}^n + 2$ jest nierozkładalny w $\mathbb{Z}[\mathbf{x}]$ na mocy kryterium Eisensteina. Mamy więc przykład nieskończonego zbioru wielomianów nierozkładalnych.

ład 12
2.2012

9.10 Zadania

Zadanie 9.1 Udowodnij, że w pierścieniu całkowitym $\mathbb{Z}[\sqrt{-5}]$ elementy $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ są nierozkładalne (choć nie są elementami pierwszymi tego pierścienia).

Zadanie 9.2 Wykaż, że zbiór **A** wielomianów o współczynnikach wymiernych, których wyraz wolny jest liczbą całkowitą jest pierścieniem całkowitym.

1. Które z elementów
   (a) 5 (b) 6 (c) $\mathbf{x}+3$ (d) $\mathbf{x}+6$ (e) $\mathbf{x}^2$ (f) $\mathbf{x}$
   są, a które nie są rozkładalne w A.

2. Wykaż, że ciąg ideałów głównych $((\frac{1}{3^n}\mathbf{x}))_{n\in\mathbb{N}}$ jest wstępujący (to znaczy $(\frac{1}{3^n}\mathbf{x}) \subset (\frac{1}{3^{n+1}}\mathbf{x})$ dla dowolnego $n \in \mathbb{N}$) i niestacjonarny.

3. Wykaż , że **A** jest pierścieniem bez rozkładu (oznacza to w szczególności, że A nie jest pierścieniem Gaussa).
   Wskazówka. Rozważ wielomiany $\mathbf{x}$, $\frac{1}{3}\mathbf{x}$, $\frac{1}{3^2}\mathbf{x}, ...$

4. Udowodnij, że dowolny element nierozkładalny w A jest pierwszy.

Zadanie 9.3 Udowodnij, że dla dowolnego homomorfizmu pierścieni $h : P \to Q$ obraz h jest podpierścieniem pierścienia Q a jądro h ideałem pierścienia P (twierdzenie 9.20).

Zadanie 9.4 Wykaż, że zbiór **A** wielomianów o współczynnikach wymiernych, których wyraz wolny jest liczbą całkowitą jest pierścieniem całkowitym.

1. Które z elementów
   (a) 5 (b) 6 (c) $\mathbf{x}+3$ (d) $\mathbf{x}+6$ (e) $\mathbf{x}^2$ (f) $\mathbf{x}$
   są, a które nie są rozkładalne w A.

2. Wykaż, że ciąg ideałów głównych $((\frac{1}{3^n}\mathbf{x}))_{n\in\mathbb{N}}$ jest wstępujący (to znaczy $(\frac{1}{3^n}\mathbf{x}) \subset (\frac{1}{3^{n+1}}\mathbf{x})$ dla dowolnego $n \in \mathbb{N}$) i niestacjonarny.

3. Wykaż , że **A** jest pierścieniem bez rozkładu (oznacza to w szczególności, że A nie jest pierścieniem Gaussa).
   Wskazówka. Rozważ wielomiany $\mathbf{x}$, $\frac{1}{3}\mathbf{x}$, $\frac{1}{3^2}\mathbf{x}, ...$

4. Udowodnij, że dowolny element nierozkładalny w A jest pierwszy.

Rozdział 10

Wielomiany wielu zmiennych

Niech będzie dany pierścień P całkowity. Wówczas $(P[\mathbf{x}])[\mathbf{y}]$ nazywamy **pierścieniem wielomianów dwóch zmiennych**. Pierścień ten oznaczamy przez $P[\mathbf{x}, \mathbf{y}]$.

Użycie powyżej nazwy *pierścień* dla *zbioru* wielomianów dwóch zmiennych jest pozornym nadużyciem. Nie udowodniliśmy przecież, że $P[\mathbf{x}, \mathbf{y}]$ jest rzeczywiście pierścieniem. Jednak wiemy już, że $P[\mathbf{x}]$ jest pierścieniem i to całkowitym. Wobec tego $P[\mathbf{x}, \mathbf{y}]$ jako zbiór wielomianów (zmiennej $\mathbf{y}$) o współczynnikach w pierścieniu całkowitym $P[\mathbf{x}]$ jest pierścieniem (całkowitym).
Wielomianem n zmiennych $\mathbf{x_1}, ..., \mathbf{x_n}$ nazywamy każdy element zdefiniowanego rekurencyjnie pierścienia pierścienia wielomianów n zmiennych:

$$P[\mathbf{x_1}, ..., \mathbf{x_n}] = \mathbf{P}[\mathbf{x_1}, ..., \mathbf{x_{n-1}}][\mathbf{x_n}]$$

Bardzo łatwo stwierdzić, że ogólna postać wielomianu $v \in P[\mathbf{x_1}, ..., \mathbf{x_n}]$ jest następująca

$$v(\mathbf{x_1}, ..., \mathbf{x_n}) = \sum \mathbf{a_{i_1,...,i_n}} \mathbf{x^{i_1}} \cdot ... \cdot \mathbf{x^{i_n}}$$

($a_{i_1,...,i_n} \in P$ nazywamy współczynnikami wielomianu v).

10.1 Wielomiany symetryczne

Twierdzenie 10.1 (Wzory Viety) *Niech P będzie pierścieniem całkowitym. Jeśli $v = a_0 + a_1\mathbf{x} + \cdots + a_n\mathbf{x}^n \in P[\mathbf{x}]$ jest wielomianem stopnia n o n pierwiastkach $\alpha_1, \ldots, \alpha_n$ (niekoniecznie różnych) należących do pewnego pierścienia $L \supset P$, wówczas*

$$v = k(\mathbf{x} - \alpha_1) \cdot \cdots \cdot (\mathbf{x} - \alpha_n)$$

i zachodzą wzory (zwane **wzorami Viety**[1]*):*

$$a_n = k$$

[1] François Viète 1540-1603.

$$a_{n-1} = -k(\alpha_1 + \cdots + \alpha_n)$$
$$a_{n-2} = k(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n)$$
$$\cdots$$
$$a_0 = k(-1)^n \alpha_1 \cdot \cdots \cdot \alpha_n$$

Dowód twierdzenia 10.1 jest praktycznie oczywisty: wystarczy porównać współczynniki wielomianu we wzorze

$$a_0 + a_1\mathbf{x} + \cdots + a_n\mathbf{x}^n = k(\ x - \alpha_1) \cdot \cdots \cdot (\mathbf{x} - \alpha_n)$$

■

Może się zdarzyć tak, że pierwiastkami wielomianu $v = a_0 + ... + a_n\mathbf{x}^n$ o współczynnikach w pewnym pierścieniu są elementy innego, obszerniejszego niż P zbioru. Przykłady takich sytuacji znamy bardzo dobrze.

1. Pierwiastkiem wielomianu $2\mathbf{x} + 1$ o współczynnnikach całkowitych jest liczba wymierna $-\frac{1}{2}$.
2. Pierwiastkami wielomianu $\mathbf{x}^2 + 1 \in \mathbb{Z}[\mathbf{x}]$ są liczby zespolone i oraz $-i$.

Z twierdzenia o wzorach Viety wynika jednak następujący, ważny wniosek.

Wniosek 10.2 *Jeśli wielomian $v \in P[\mathbf{x}]$ ma pierwiastki $\alpha_1, \ldots, \alpha_n$ należące do pierścienia L zawierającego P (pierścień P jest podpierścieniem pierścienia L), wówczas*

$$\sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} \alpha_{i_1} \cdot \cdots \cdot \alpha_{i_k} \in P$$

dla każdego $k \le n$. ■

r-tym podstawowym wielomianem symetrycznym $S_r(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ nazywamy wielomian n zmiennych $\mathbf{x}_1, \ldots, \mathbf{x}_n$ który jest sumą wszystkich różnych iloczynów r różnych zmiennych.

Przykład.
$n = 5, r = 1$: $S_1(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4, \mathbf{x}_5) = \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 + \mathbf{x}_4 + \mathbf{x}_5$
$n = 4, r = 3$: $S_3(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4) = \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_2\mathbf{x}_4 + \mathbf{x}_1\mathbf{x}_3\mathbf{x}_4 + +\mathbf{x}_2\mathbf{x}_3\mathbf{x}_4$

Wniosek 10.3 (Inna postać tw.Viety) *Jeżeli $\alpha_1, \ldots, \alpha_n \in L$ są pierwiastkami wielomianu $v \in P[\mathbf{x}]$ (gdzie pierścień P jest podpierścieniem pierścienia L), $v = \mathbf{x}^n + a_{n-1}\mathbf{x}^{n-1} + \cdots + a_0$ to*

$$a_r = (-1)^{n-r} S_{n-r}(\alpha_1, \ldots, \alpha_n)$$

dla $r = 0, 1, ..., n$.

Stąd wynika kolejny ważny wniosek.

Wniosek 10.4 *Jeśli $\alpha_1, \ldots, \alpha_n \in L$ są pierwiastkami wielomianu $v \in P[\mathbf{x}]$ (gdzie P jest podpierścieniem pierścienia L), to*

$$S_r(\alpha_1, \ldots, \alpha_n) \in P$$

dla każdego $r, 1 \leq r \leq n$.

10.2 Twierdzenie Wilsona

Twierdzenie Wilsona[2]. Dotyczy ono rozpoznawania liczb pierwszych, jest więc ważne chociażby ze względu na zastosowania w teori szyfrowania. Niestety ze względu na liczbę operacji arytmetycznych jakie trzeba wykonać, nie za bardzo widać jak można by je stosować do rozpoznawania bardzo dużych liczb pierwszych (przez *duże* liczby rozumiemy liczby naturalne o co najmniej setkach miejsc znaczących).

Twierdzenie 10.5 (Twierdzenie Wilsona) *Liczba $p \in \mathbf{N}$ jest pierwsza wtedy i tylko wtedy, gdy*

$$(p-1)! + 1 \equiv 0 \ (mod\ p) \tag{10.1}$$

Dowód. Przypuśćmy wpierw, że p jest liczbą pierwszą. Z Małego Twierdzenia Fermata wiemy, że

$$x^{p-1} \equiv 1 \ (\text{mod } p) \ \text{ dla każdego } x \in \mathbb{Z}_p^*$$

A więc, elementy $1, 2, ..., p-1 \in \mathbb{Z}_p^*$ są pierwiastkami wielomianu stopnia $p-1$: $\mathbf{x}^{p-1}-1$ i wobec tego wielomian ten nad pierścieniem $\mathbb{Z}_p$ jest postaci

$$\mathbf{x}^{p-1} - 1 = (\mathbf{x}-1)(\mathbf{x}-2)...(\mathbf{x}-(p-1))$$

Stąd i z wniosku 10.3 wynika, że

$$S_k(1, 2, ..., p-1) \equiv 0 \ (\text{mod p}) \text{ dla } \ k = 1, 2, ..., p-2$$

oraz

$$S_{p-1}(1, 2, ..., p-1) \equiv -1(\text{mod p})$$

Ta ostatnia równość oznacza, że

$$(-1)(-2) \cdot ... \cdot (-(p-1)) = (-1)^{p-1}(p-1)! \equiv -1 \ \ (\text{mod } p)$$

Ponieważ jednak p jest liczbą pierwszą, $p-1$ jest liczbą parzystą lub $p = 2$. Dla $p > 2$ otrzymujemy żądaną równość $(p-1)! \equiv -1 \ (\text{mod } p)$. Dla $p = 2$ twierdzenie bardzo

[2]John Wilson (1741-1793), z którego nazwiskiem w sposób trwały związane jest omawiane tu twierdzenie 10.5 nie udowodnił, a jedynie odkrył to twierdzenie. Lepiej byłoby powiedzeć, że raczej podejrzewał, że jest prawdziwe. Przypisanie twierdzenia Wilsona Wilsonowi więc jest nie do końca słuszne. Tym bardziej, że twierdzenie to było znane już Alhazenowi który żył w latach 965-1040 i był, jak przystało na średnowiecze, uczonym arabskim. Pierwszy znany dowód *twierdzenia Wilsona* podał Lagrange w 1773 roku.

łatwo można sprawdzić bezpośrednio.
Udowodnimy teraz, metodą nie wprost, że jeśli spełniony jest wzór (10.1) wówczas p jest liczbą pierwszą.

Przypuśćmy, że $p \in \mathbb{N}$ nie jest liczbą pierwszą, czyli istnieje takie $m \in \mathbb{N}$, że $1 < m < p$ i m dzieli p. Skoro $1 < m < p$, mamy

$$(p-1)! = m \cdot t$$

dla pewnego $t \in \mathbb{Z}$ i wobec tego, na mocy wzoru (10.1)

$$m \cdot t \equiv -1 \pmod{p}$$

Istniałoby więc $k \in \mathbb{Z}$ takie, że $mt = -1 + kp$, a więc prawdziwa byłaby równość $(-t)m + kp = 1$. Stąd zaś $m \perp p$, a przecież m wybraliśmy tak, by było dzielnikiem p. Ta sprzeczność kończy dowód twierdzenia Wilsona. ■

10.3 Podstawowe twierdzenie o wielomianach symetrycznych

Wielomian $v \in P[\mathbf{x_1}, ..., \mathbf{x_n}]$ nazywamy **symetrycznym** jeżeli dla dowolnej permutacji $\sigma \in S_n$ zachodzi wzór

$$v(\mathbf{x}_{\sigma 1}, ..., \mathbf{x}_{\sigma n}) = v(\mathbf{x}_1, ..., \mathbf{x}_n)$$

Przedstawione poniżej **podstawowe twierdzenie o wielomianach symetrycznych** znane jest od XVIII wieku.

Twierdzenie 10.6 *W dowolnym pierścieniu z jedynką P dla każdego wielomianu symetrycznego $v \in P[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ istnieje dokładnie jeden wielomian $w \in P[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ taki, że*

$$v(\mathbf{x}_1, \ldots, \mathbf{x}_n) = w(S_1(\mathbf{x}_1, \ldots, \mathbf{x}_n), \ldots, S_n(\mathbf{x}_1, \ldots, \mathbf{x}_n)) \tag{10.2}$$

Dowód[3] w sposób dość naturalny składa się z dwóch części: dowodu istnienia i dowodu jednoznaczności wielomianu w.
Dla dowodu istnienia wielomianu w o postulowanej w twierdzeniu własności, wprowadzimy w zbiorze jednomianów *porządek leksykograficzny* $\prec$. Piszemy:

$$\mathbf{x}_1^{a_1} \ldots \mathbf{x}_n^{a_n} \prec \mathbf{x}_1^{b_1} \ldots \mathbf{x}^{b_n}$$

(mówimy: $\mathbf{x}_1^{a_1} \ldots \mathbf{x}_n^{a_n}$ *poprzedza* $\mathbf{x}_1^{b_1} \ldots \mathbf{x}^{b_n}$) jeżeli

$a_1 + \cdots + a_n < b_1 + ... + b_n$ lub

$a_1 + ... + a_n = b_1 + ... + b_n$ oraz

[3] Przedstawiony tu dowód twierdzenia został podany w 1816 roku przez Gaussa.

$a_1 < b_1$ lub

$a_1 = b_1$ i $a_2 < b_2$ lub

$a_1 = b_1, a_2 = b_2$ i $a_3 < b_3$ lub

...

$a_1 = b_1, a_2 = b_2, ..., a_{n-2} = b_{n-2}, a_{n-1} < b_{n-1}$ lub

$a_1 = b_1, a_2 = b_2, ..., a_{n-1} = b_{n-1}, a_n = b_n$

Dla przykładu: $\mathbf{x}_1\mathbf{x}_2^2\mathbf{x}_3^2 \prec \mathbf{x}_1^2\mathbf{x}_2\mathbf{x}_3^4$ (bo stopień pierwszego jednomianu jest równy 5 a drugiego 7) ale $\mathbf{x}_1^2x_2\mathbf{x}_3^3 \prec x_1^2\mathbf{x}_2^2\mathbf{x}_3^2$. Idea tej części dowodu polega na dość oczywistej obserwacji, że dla dowolnego jednomianu istnieje tylko skończona liczba jednomianów, które są od niego mniejsze w porządku leksykograficznym (pomijamy tu współczynnik przy jednomianie, czyli porównujemy tylko jednomiany postaci $\mathbf{x}_1^{c_1}\dots\mathbf{x}_n^{c_n}$).

Niech składniki wielomianu $v(\mathbf{x}_1, ..., \mathbf{x}_n)$ będą wypisane **malejąco** (!) w porządku leksykograficznym $\prec$ i niech $c\mathbf{x}_1^{a_1}\dots\mathbf{x}_n^{a_n}$ będzie pierwszym z nich[4], czyli największym w sensie relacji $\prec$. Zauważmy, że

$$a_1 \geq a_2 \geq \dots \geq a_n$$

Rzeczywiście, przypuśćmy, że istnieje i, $1 \leq i < n$ takie, że $a_i < a_{i+1}$. Ponieważ wielomian v jest symetryczny, jednym z jego składników jest

$$c\mathbf{x}_1^{a_1}\dots\mathbf{x}_i^{a_{i+1}}\mathbf{x}_{i+1}^{a_i}\dots\mathbf{x}_n^{a_n}$$

Skoro jednak $a_i < a_{i+1}$, zachodzi

$$\mathbf{x}_1^{a_1}\dots\mathbf{x}_i^{a_{i+1}}\mathbf{x}_{i+1}^{a_i}\dots\mathbf{x}_n^{a_n} \succ \mathbf{x}_1^{a_1}\dots\mathbf{x}_i^{a_i}\mathbf{x}_{i+1}^{a_{i+1}}\dots\mathbf{x}_n^{a_n}$$

co jest sprzeczne z wyborem $c\mathbf{x}_1^{a_1}\dots\mathbf{x}_n^{a_n}$ jako największego jednomianu składowego v w porządku leksykograficznym.
Rozważmy teraz wielomian symetryczny

$$w_1(S_1, ..., S_n) = cS_1^{a_1-a_2}S_2^{a_2-a_3}\dots S_{n-1}^{a_{n-1}-a_n}S_n^{a_n}$$

(pamiętajmy, że dla każdego $i \in \{1, \dots, n\}$ przez S_i rozumiemy tu wielomian podstawowy wielomian symetryczny zmiennych wielomianowych $\mathbf{x}_1, \dots, \mathbf{x}_n$, $S_i = S_i(\mathbf{x}_1, \dots, \mathbf{x}_n)$). Największym, w porządku leksykograficznym, składnikiem tego wielomianu jest

$$\begin{gathered} c\mathbf{x}_1^{a_1-a_2}(\mathbf{x}_1\mathbf{x}_2)^{a_2-a_3}(\mathbf{x}_1\mathbf{x}_2\mathbf{x}_3)^{a_3-a_4}\dots(\mathbf{x}_1\dots\mathbf{x}_{n-1})^{a_{n-1}-a_n}(\mathbf{x}_1\dots\mathbf{x}_n)^{a_n} \\ = c\mathbf{x}_1^{a_1}\mathbf{x}_2^{a_2}\dots\mathbf{x}_n^{a_n} \end{gathered}$$

a więc pierwszy (największy) składnik wielomianu v.
Oznaczmy teraz przez v_1 wielomian

$$v_1(\mathbf{x}_1, \dots, \mathbf{x}_n) = v(\mathbf{x}_1, \dots, \mathbf{x}_n) - w_1(S_1, \dots, S_n)$$

[4]Współczynnik $c \neq 0$ nie odgrywa tu żadnej roli, zakładamy, że jeśli pewien jednomian $\mathbf{x}_1^{a_1}\dots\mathbf{x}_n^{a_n}$ w wielomianie v występuje ze współczynnikiem $c \neq 0$, to występuje w ten sposób tylko jeden raz.

(także w tym przypadku należy rozumieć S_i jako wielomiany podstawowe zmiennych $\mathbf{x}_1, \ldots, \mathbf{x}_n$). Oczywiście wielomian v_1 jest symetryczny. Także ten wielomian zapisujemy w porządku leksykograficznym. Powiedzmy, że jego największym składnikiem jest

$$b\mathbf{x}_1^{b_1} \ldots \mathbf{x}_n^{b_n}$$

przy czym analogicznie jak poprzednio, $b_1 \geq \cdots \geq b_n$, oraz

$$\mathbf{x}_1^{b_1} \ldots \mathbf{x}_n^{b_n} \prec \mathbf{x}_1^{a_1} \ldots \mathbf{x}_n^{a_n}$$

Powtarzamy procedurę zastosowaną uprzednio do wielomianu v do wielomianu v_1 i otrzymujemy wielomian w_2 a następnie wielomian

$$v_2(\mathbf{x}_1, ..., \mathbf{x}_n) = v(\mathbf{x}_1, \ldots, \mathbf{x}_n) - w_1(S_1, ..., S_n) - w_2(S_1, \ldots, S_n)$$

o największym jednomianie silnie mniejszym (w sensie porządku leksykograficznego) od $b\mathbf{x}_1^{b_1} \ldots \mathbf{x}_n^{b_n}$. Kontynuujemy otrzymując ciąg wielomianów

$$\begin{gathered} v(\mathbf{x}_1, \ldots, \mathbf{x}_n) \\ v(\mathbf{x}_1, \ldots, \mathbf{x}_n) - w_1(S_1, \ldots, S_n) \\ v(\mathbf{x}_1, \ldots, \mathbf{x}_n) - w_1(S_1, \ldots, S_n) - w_2(S_1, \ldots, S_n) \\ v(\mathbf{x}_1, \ldots, \mathbf{x}_n) - w_1(S_1, \ldots, S_n) - w_2(S_1, \ldots, S_n) - \cdots - w_p(S_1, \ldots, S_n) \end{gathered}$$

o silnie malejących największych składnikach, aż otrzymamy wielomian zerowy

$$v(\mathbf{x}_1, \ldots, \mathbf{x}_n) - w_1(S_1, \ldots, S_n) - w_2(S_1, \ldots, S_n) - \cdots - w_m(S_1, \ldots, S_n) = 0$$

Stąd zaś otrzymujemy poszukiwaną postać wielomianu v:

$$v(\mathbf{x}_1, \ldots, \mathbf{x}_n) = w_1(S_1, \ldots, S_n) - w_2(S_1, \ldots, S_n) - \cdots - w_m(S_1, \ldots, S_n)$$

Dowód jednoznaczności. Niech wielomian w spełnia warunek 10.2 twierdzenia i niech p będzie największym jednomianem wielomianu w (*największym* w takim sensie, w jakim to zostało zdefiniowane podczas dowodu istnienia). Powiedzmy, że

$$p(S_1, S_2, ..., S_n) = cS_1^{\beta_1} S_2^{\beta_2} ... S_n^{\beta_n}$$

Wówczas największym jednomianem wielomianu

$$w(S_1(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n), S_2(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n), ..., S_n(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n))$$

jest

$$c\mathbf{x}_1^{\beta_1+\beta_2+...+\beta_n} \mathbf{x}_2^{\beta_2+\beta_3+...+\beta_n} \cdot ... \cdot \mathbf{x}_n^{\beta_n}$$

Wynika stąd, że największy jednomian zmiennych $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n$ wielomianu w (a więc i wielomianu v!) powstaje w ten sposób z największego jednomianu zmiennych $S_1, S_2, ..., S_n$ wielomianu w. Mamy więc

$$c\mathbf{x}^{\alpha_1} \cdot \mathbf{x}^{\alpha_2} \cdot ... \cdot \mathbf{x}^{\alpha_n} = c\mathbf{x}_1^{\beta_1+\beta_2+...+\beta_n} \cdot \mathbf{x}_2^{\beta_2+\beta_3+...+\beta_n} \cdot ... \cdot \mathbf{x}_n^{\beta_n}$$

Pamiętamy, że w pierwszej części dowodu przyjęliśmy, że największym jednomianem wielomianu v jest $c\mathbf{x}^{\alpha_1} \cdot \mathbf{x}^{\alpha_2} \cdot ... \cdot \mathbf{x}^{\alpha_n}$. Stąd zaś wynika, że α_i oraz β_i spełniają następujący układ równań.

$$\begin{array}{ccccccccc} \beta_1 & + & \beta_2 & + & ... & + & \beta_n & = & \alpha_1 \\ & & \beta_2 & + & ... & + & \beta_n & = & \alpha_2 \\ & & & & ... & & & & \\ & & & & & & \beta_n & = & \alpha_n \end{array}$$

Ten układ ma rozwiązania wyznaczone jednoznaczne. ■

Niech v będzie wielomianem stopnia n o współczynnikach w pierścieniu całkowitym P i niech $\alpha_1, ..., \alpha_n \in L$ będą pierwiastkami wielomianu v należącymi do pewnego pierścienia L, $P \subset L$. Na mocy wniosku 10.4, dla każdego $i \in \{1, \ldots, n\}$, $S_i(\alpha_1, \ldots, \alpha_n) \in P$. Stąd i z twierdzenia 10.6 wynika następujący wniosek.

Wniosek 10.7 *Dla każdego wielomianu (jednej zmiennej) $v \in P[\mathbf{x}]$ nad pierścieniem całkowitym P stopnia n mającym pierwiastki $\alpha_1, ..., \alpha_n$ w pewnym pierścieniu L ($P \subset L$) i dla każdego wielomianu symetrycznego n zmiennych $s \in P[\mathbf{x}_1, ..., \mathbf{x}_n]$ zachodzi*

$$s(\alpha_1, ..., \alpha_n) \in P$$

■

10.4 Zadania

Zadanie 10.1 Rozpoznaj wielomiany symetryczne:
$\mathbf{x}_1^2\mathbf{x}_2\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3^2$
$\mathbf{x}_1^3\mathbf{x}_2^2\mathbf{x}_3\mathbf{x}_4 + \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3^2\mathbf{x}_4^3$
$\mathbf{x}_1^2\mathbf{x}_2\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_2^2\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3^2$

Zadanie 10.2 Uzupełnij wielomian symetryczny
$\mathbf{x}_1\mathbf{x}_2^3\mathbf{x}_3 + \mathbf{x}_1^2\mathbf{x}_2\mathbf{x}_3 + ...$

Zadanie 10.3 Ile składników ma wielomian symetryczny 6 zmiennych, którego jednym ze składników jest $\mathbf{x}_1\mathbf{x}_2^2\mathbf{x}_3^4\mathbf{x}_4^6\mathbf{x}_5^7$ a ile wielomian 5 zmiennych zawierający ten sam składnik?

Zadanie 10.4 Wypisz wzory Viety dla $n = 2$ i $n = 3$.

Zadanie 10.5 Dla każdego z wielomianów symetrycznych z zadań 10.1 i 10.2 wskaż wielomian w taki, że $v(\mathbf{x}_1, ...) = w(S_1(\mathbf{x}_1, ..., \mathbf{x}_n), ...)$.

Zadanie 10.6 Udowodnij, że dla dowolnego jednomianu $\mathbf{x}_1^{a_1} \cdot \cdots \cdot \mathbf{x}_n^{a_n}$ istnieje skończona liczba jednomianów o współczynniku 1, mniejszych w sensie porządku leksykograficznego zdefiniowanego w dowodzie twierdzenia 10.6.

Zadanie 10.7 Wyznacz wielomian w taki, że $v(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) = w(S_1(x_1, x_2, \mathbf{x}_3), ...)$ dla wielomianu symetrycznego $v(\mathbf{x}_1, \mathbf{x}_2\mathbf{x}_3) = 2\mathbf{x}_1^3\mathbf{x}_2^2\mathbf{x}_3 + \mathbf{x}_1\mathbf{x}_2^2\mathbf{x}_3 - \mathbf{x}_1\mathbf{x}_2\mathbf{x}_3^3 + \dots$ korzystając z metody dowodu twierdzenia 10.6.

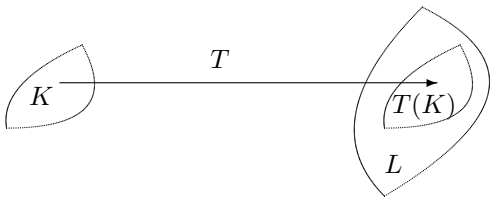
Rozdział 11

Rozszerzenia ciał

Rozszerzeniem ciała K nazywamy każde ciało L takie, że istnieje monomorfizm $T : K \to L$. Piszemy wtedy $L : K$ (taki napis czytamy *ciało L jest rozszerzeniem ciała K*).
Jeśli ciało K jest podciałem ciała L, wówczas $L : K$ i monomorfizm $T : K \to L$ dany jest wzorem $T(x) = x$, dla każdego $x \in K$. Co więcej, z taką sytuacją będziemy mieli do czynienia najczęściej (choć nie zawsze). Czasami ciało K nazywamy *małym* zaś L *dużym*.
Tę sytuację przedstawiono na rysunku 11.1.

Obraz ciała K przez monomorfizm T, oznaczany przez $Im_T K$ (lub $T(K)$) możemy identyfikować z K jako, że $T(K)$ jest ciałem izomorficznym z K. Na zasadzie tego właśnie izomorfizmu możemy traktować K jako podciało ciała L (tak jak przyzwyczailiśmy się to robić dla ciała liczb rzeczywistych, które traktujemy często jak podciało liczb zespolonych mimo, że w sensie formalnym nie jest ono podzbiorem zbioru liczb zespolonych).

Niech $L : K, X \subset L$.
Ciałem generowanym w K przez X nazywamy najmniejsze ciało zawierające X i K (lub $T(K)$ gdy K nie jest podciałem ciała L a więc wtedy, gdy T nie jest identycznością). Takie ciało oznaczamy przez $K(X)$. Jeśli zbiór X jest skończony, na przykład $X = \{a_1, ..., a_n\}$ wówczas piszemy $K(a_1, ..., a_n)$ zamiast $K(\{a_1, ..., a_n\})$.



Rysunek 11.1: $L : K$

Ciało generowane przez $X \subset K$ jest równe:

- przecięciu wszystkich podciał ciała L zawierających $X \cup T(K)$,
- zbiorowi elementów które można otrzymać w ciągu skończonym operacji (działań w ciele) na elementach z X i K.

Przykład 11.1 $\mathbf{Q}(i, \sqrt{2})$

Rozszerzenie ciała K o element $a \in L$ nazywamy **rozszerzeniem prostym** i oznaczamy przez $K(a)$ (zamiast $K(\{a\})$). Element a nazywamy wtedy **elementem prymitywnym** tego rozszerzenia.

Przykład 11.2 Przyjrzyjmy się rozrzerzeniu $\mathbb{Q}(\sqrt{2}, \sqrt{5})$. Wykażemy, że to rozszerzenie ciała liczb wymiernych jest rozszerzeniem prostym a więc, że istnieje taki element $a \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$, że $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(a)$.
Niech $a = \sqrt{2} + \sqrt{5}$. Mamy

$$a^2 = 2 + 2\sqrt{10} + 5 = 7 + 2\sqrt{10}$$

$$a^3 = 2\sqrt{2} + 3 \cdot 2\sqrt{5} + 3 \cdot \sqrt{2} \cdot 5 + 5 \cdot \sqrt{5} = 17\sqrt{2} + 11\sqrt{5}$$

Stąd $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{5})$ i $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Prawdą także jest, że $\sqrt{2} + \sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Wobec tego łatwo już wydedukować, że $\mathbb{Q}(\sqrt{2} + \sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.□

Przypomnijmy poznane już wcześniej pierścienie ilorazowe.
Jeżeli I jest ideałem pierścienia P, wówczas iloraz P/I jest pierścieniem. Pamiętamy, że zerem tego pierścienia jest I zaś elementami zbiory postaci

$$a + I$$

gdzie $a \in P$. Działania w pierścieniu są wtedy określona wzorami:

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I)(b + I) = ab + I$$

Przypomnijmy także, że jeśli K jest ciałem, to $K[\mathbf{x}]$ jest pierścieniem głównym.

Wiemy, że w pierścieniu $K[\mathbf{x}]$ wielomianów nad ciałem K dla dowolnego wielomianu $v \neq 0$ i dla dowolnego wielomianu $w \in K[\mathbf{x}]$ istnieją jednoznacznie wyznaczone wielomiany $q, r \in K[\mathbf{x}]$ takie, że $w = vq + r$ przy czym $\partial(r) < \partial(v)$ lub r jest wielomianem zerowym. Stąd wynika bardzo łatwo następujące twierdzenie.

Twierdzenie 11.1 *Jeśli K jest ciałem, $v \in K[\mathbf{x}]$, $\partial v = n \geq 1$, wówczas*

$$K[\mathbf{x}]/(v) = \{w + (v) : \ w \in K[\mathbf{x}], \partial w \leq n - 1\}$$

■

Jeśli wielomian $v \in K[\mathbf{x}]$ jest rozkładalny, powiedzmy $v = uw$, gdzie $u, w \in K[\mathbf{x}]$, wówczas $[u + (v)] \cdot [w + (v)] = uw + (v) = v + (v) = (v)$. Ponieważ zaś (v) w pierścieniu $K[\mathbf{x}]/(v)$ jest zerem, pierścień ten ma dzielniki zera (są nimi $u + (v)$ i $w + (v)$). Elementy $u + (v)$ i $w + (v)$ są w $K[\mathbf{x}]/(v)$ nieodwracalne.

Twierdzenie 11.2 *Jeśli K jest ciałem a $v \in K[\mathbf{x}]$ wielomianem nierozkładalnym nad K, $\partial(v) \geq 1$, wówczas $K[\mathbf{x}]/(v)$ jest ciałem.*

Dowód. Ponieważ K jest ciałem, jest także pierścieniem całkowitym, a więc (twierdzenie 9.2) $K[\mathbf{x}]$ jest pierścieniem przemiennym z jedynką. Stąd zaś (twierdzenie 8.4) $K[\mathbf{x}]/(v)$ jest pierścieniem przemiennym z jedynką.
Pozostaje wykazać, że dla dowolnego elementu różnego od zera w $K[\mathbf{x}]/(v)$ istnieje element odwrotny (ze względu na mnożenie).
Niech $a + (v)$ będzie różnym od zera elementem $K[\mathbf{x}]/(v)$. Oznacza, że wielomian $a \in K[\mathbf{x}]$ nie jest podzielny przez v. $K[\mathbf{x}]$ jest pierścieniem Gaussa (twierdzenia 9.8 i 9.14), elementy a i v są więc względnie pierwsze i wobec tego (twierdzenie 9.10) istnieją takie wielomiany $u, w \in K[\mathbf{x}]$, że

$$au + vw = 1$$

Stąd mamy $(a + (v))(u + (v)) = 1 + (v)$ co oznacza, że w $K[\mathbf{x}]/(v)$ element $u + (v)$ jest odwrotny do $a + (v)$, co kończy dowód twierdzenia. ■

Ciało $K[\mathbf{x}]/(v)$, którego istnienie gwarantuje twierdzenie 11.2 jest rozszerzeniem ciała K. Rzeczywiście, funkcja

$$\psi : K \ni a \to a + (v) \in K[\mathbf{x}]/(v)$$

jest monomorfizmem ciała K w ciało $K[\mathbf{x}]/(v)$. Mamy bowiem
$\psi(a + b) = a + b + (v)$ i $\psi(a) + \psi(b) = a + (v) + b + (v) = a + b + (v)$
a także
$\psi(a \cdot b) = ab + (v)$ oraz $\psi(a) \cdot \psi(b) = (a + (v))(b + (v)) = ab + (v)$
co oznacza, że ψ jest homomorfizmem K w $K[\mathbf{x}]/(v)$. Co więcej, ψ jest monomorfizmem. Przypuśćmy bowiem, że $\psi(a) = \psi(b)$. Mamy wówczas $a + (v) = b + (v)$, czyli $a - b \in (v)$. a i b są jednak elementami ciała K, wobec czego wielomian (stopnia co najmniej równego 1) $v \in K[\mathbf{x}]$ dzieli $a - b$ tylko wtedy, gdy $a - b = 0$, czyli $a = b$.
Zapiszmy te rozważania w postaci wniosku.

Wniosek 11.3 *Jeżeli $v \in K[\mathbf{x}]$ jest wielomianem nierozkładalnym w $K[\mathbf{x}]$, wówczas ciało $K[\mathbf{x}]/(v)$ jest rozszerzeniem ciała K.*

Rozszerzenia postaci $K[\mathbf{x}]/(v)$ ciała K, gdy $v \in K[\mathbf{x}]$ jest wielomianem nierozkładalnym nad K, spotkamy wielokrotnie jeszcze zarówno w niniejszym rozdziale jak w następnym. W ciałach tych wygodnie jest w zapisywać elementy postaci $w + (v)$ (gdzie $w \in K[\mathbf{x}]$) jako w - w zapisie tym pomijamy (v), co uzasadnione jest także tym, że element (v) jest zerem ciała $K[\mathbf{x}]/(v)$.

Zauważmy, że ciało $K[\mathbf{x}]/(v)$ (gdzie v jest wielomianem nieprzywiedlnym nad K) zawiera podciało izomorficzne z K. Tym podciałem jest zbiór

$$\{a + (v) : a \in K\}$$

Izomorfizmem jest $T : K \ni a \to a + (v)$. Dlatego też $K[\mathbf{x}]/(v)$ jest rozszerzeniem K $(K[\mathbf{x}]/(v) : K)$.

11.1 Ciało rozkładu wielomianu

Naszym nabliższym celem będzie teraz wykazanie, że dla każdego wielomianu v o współczynnikach w ciele K istnieje takie rozszerzenie ciała K, w którym v ma wszystkie $\partial(v)$ pierwiastków (niekoniecznie różnych między sobą). Inaczej mówiąc, udowodnimy, że istnieje rozszerzenie ciała K, w którym v można zapisać w postaci iloczynu wielomianów stopnia pierwszego.

Ciałem rozkładu wielomianu $v \in K[\mathbf{x}]$ nazywamy najmniejsze ciało, w którym v rozkłada się na iloczyn czynników liniowych

$$v = a(\mathbf{x} - b_1) \dots (\mathbf{x} - b_n)$$

Inaczej mówiąc, ciałem rozkładu wielomianu $v \in K[\mathbf{x}]$ jest $K(b_1, \dots, b_n)$

Przykład 11.3 *Dla wielomianu $x^2 - 2$ nad ciałem $\mathbb{Q}$ ciałem rozkładu jest $\mathbb{Q}(\sqrt{2})$ a dla wielomianu $x^2 + 2 \in \mathbb{Q}(\mathbf{x})$ ciałem rozkładu jest $\mathbb{Q}(i\sqrt{2})$.*

Następne twierdzenie nazwiemy **twierdzeniem o ciele rozkładu** lub **twierdzeniem Kroneckera**, który je udowodnił w XIX wieku.

Twierdzenie 11.4 *Dla dowolnego ciała K i wielomianu $v \in K[\mathbf{x}]$ istnieje rozszerzenie $L : K$ w którym v rozkłada się na iloczyn czynników liniowych.*

Poniższy lemat będzie miał kluczowe znaczenie w dowodzie twierdzenia 11.4.

Lemat 11.5 *Jeśli v jest wielomianem nierozkładalnym nad ciałem K, wówczas w ciele $K[\mathbf{x}]/(v)$ element $\mathbf{x} + (v)$ jest pierwiastkiem wielomianu v.*

Dowód lematu 11.5. Na mocy twierdzenia 11.2, $K[\mathbf{x}]/(v)$ jest ciałem, wiemy także, że elementy tego ciała są postaci $w + (v)$, gdzie $w \in K[\mathbf{x}]$. Załóżmy, że wielomian v jest postaci $v = a_n\mathbf{x}^n + a_{n-1}\mathbf{x}^{n-1} + \dots + a_1\mathbf{x} + a_0$. Otrzymujemy wówczas

$$v(\mathbf{x} + (v)) = a_n(\mathbf{x} + (v))^n + a_{n-1}(\mathbf{x} + (v))^{n-1} + \dots + a_1(\mathbf{x} + (v)) + a_0$$

$$= a_n\mathbf{x}^n + a_{n-1}\mathbf{x}^{n-1} + \dots + a_1\mathbf{x} + a_0 + (v) = (v)$$

Pamiętamy, że ideał (v) jest zerem ciała $K[\mathbf{x}]/(v)$. Stąd wynika, że element $\mathbf{x} + (v)$ jest pierwiastkiem wielomianu v w $K[\mathbf{x}]/(v)$. ■

Przykład 11.4 *Funkcjonowanie lematu 11.5 zilustrujemy przykładem. Wielomian* $\mathbf{x}^3 + 2\mathbf{x} - 2$ *jest, na mocy kryterium Eisensteina i twierdzenia 9.29, nierozkładalny nad* $\mathbb{Q}$. *W ciele* $\mathbb{Q}[\mathbf{x}]/(\mathbf{x}^3 + 2\mathbf{x} - 2)$ *elementy będziemy zapisywali jako wielomiany stopnia co najwyżej* 2, *pamiętając, że są to wielomiany modulo* $\mathbf{x}^3+2\mathbf{x}-2$. *Wynik mnożenia wielomianów* $\mathbf{x}^2 + \mathbf{x} + 5$ *i* $2\mathbf{x} - 10$ *modulo wielomian* $\mathbf{x}^3 + 2\mathbf{x} - 2$ *będziemy pisali w postaci*

$$(\mathbf{x}^2 + \mathbf{x} + 5)(2\mathbf{x} - 10) = -8\mathbf{x}^2 - 4\mathbf{x} - 46 \pmod{\mathbf{x}^3 + 2\mathbf{x} - 2}$$

lub, jeśli z kontekstu wynika jasno, że operacje są wykonywane modulo pewien wielomian (w naszym przypadku modulo wielomian $\mathbf{x}^3 + 2\mathbf{x} - 1$*) napiszemy:*

$$(\mathbf{x}^2 + \mathbf{x} + 5)(2\mathbf{x} - 10) = -8\mathbf{x}^2 - 4\mathbf{x} - 46$$

Elementy odwrotne znajdujemy wykorzystując algorytm Euklidesa. Dla przykładu,

$$\frac{1}{\mathbf{x}^2 + 1} = \frac{1}{5}(\mathbf{x} + 1)^2$$

łatwo się bowiem przekonać, że $(\mathbf{x}^2 + 1)(\mathbf{x} + 1)^2 - (\mathbf{x}^3 + 2\mathbf{x} - 2)(\mathbf{x} + 2) = 5$. □

Korzystając z lematu 11.5 wykażemy twierdzenie 11.4 wykorzystując zasadę indukcji matematycznej ze względu na n (stopień wielomianu v).

Dowód twierdzenia o ciele rozkładu przeprowadzimy przez indukcję matematyczną ze względu na stopień n wielomianu v.

- Jeśli $n = 1$, wówczas K jest rozszerzeniem K, w którym v jest iloczynem czynników liniowych.

- Przypuśćmy, że $n > 1$ i twierdzenie jest prawdziwe dla wszystkich $k < n$ to znaczy, że jeśli pewien wielomian jest stopnia $k < n$, to istnieje ciało, będące rozszerzeniem wciała K, w którym można go rozłożyć na czynniki liniowe).

  - Jeśli v jest rozkładalny, powiedzmy $v = uw$, $u, w \in K[\mathbf{x}]$, to stopnie wielomianów u i w są mniejsze niż n a więc, z założenia indukcyjnego, istnieje rozszerzenie L ciała K, w którym u można rozłożyć na czynniki liniowe. Dalej (ciągle z założenia indukcyjnego), istnieje M - rozszerzenie ciała L, w którym w można rozłożyć na czynniki liniowe. Oczywiście w ciele M można rozłożyć wielomian v na czynniki liniowe.
  - Załóżmy teraz, że wielomian v jest nierozkładalny nad K. Na mocy lematu 11.5, v jest rozkładalny nad rozszerzeniem (wniosek 11.3) $K[\mathbf{x}]/(v)$ ciała K. Powiedzmy, że $v = uw$, gdzie u i w są wielomianami o współczynnikach w $K[\mathbf{x}]/(v)$. Skoro stopnie wielomianów u i w są mniejsze od n możemy, podobnie jak w poprzednim przypadku, znaleźć rozszerzenie L ciała $K[\mathbf{x}]/(v)$, w którym v rozkłada się na czynniki liniowe. L jest szukanym rozszerzeniem ciała K. ■

11.2 Zasadnicze Twierdzenie Algebry

Zasadnicze Twierdzenie Algebry mówiące o tym, że każdy wielomian o współczynnikach zespolonych ma pierwiastek zespolony lub, co na jedno wychodzi, że wszystkie pierwiastki wielomianu o współczynnikach zespolonych są zespolone, znane jest od początku XVII wieku, niemniej jego pierwszy uznany za poprawny dowód pochodzi od Gaussa[1]. Gauss podał wiele dowodów Zasadniczego Twierdzenia Algebry. Istnieją także dowody autorstwa innych matematyków. Wszystkie te dowody korzystają w mniejszym lub większym stopniu z wyników analizy matematycznej. Poniżej przedstawiony dowód jest jednym z dowodów pochodzących od Gaussa. Jest on - w porównaniu z innymi dowodami tego twierdzenia - niezbyt trudny i wykorzystuje wcześniej udowodnione twierdzenia 11.4 (o istnieniu ciała rozkładu) oraz 10.6 (o wielomianach symetrycznych) i wniosku 10.7 z tego twierdzenia. Analiza matematyczna, która interweniuje w tym dowodzie jest na bardzo elementarnym poziomie. Wykorzystywany jest jedynie doskonale znany fakt, że każdy wielomian nieparzystego stopnia o współczynnikach rzeczywistych ma rzeczywisty pierwiastek.

Warto wspomnieć, że dowody Zasadniczego Twierdzenia Algebry podawane przez d'Alemberta (1746), Eulera (1749), Lagrange'a (1772), Laplace'a (opublikowany w 1812) były błędne (zob. [20]).

Mówimy, że **ciało K jest algebraicznie zamknięte** jeżeli każdy wielomian $v \in K[\mathbf{x}]$ ma w K wszystkie ∂v pierwiastki w K, czyli

$$v = a(\mathbf{x} - u_1)(\mathbf{x} - u_2) \cdot ... \cdot (\mathbf{x} - u_d)$$

gdzie $d = \partial v$, $u_1, ..., u_d, a \in K$.

Przykład 11.5 Żadne ciało skończone nie jest algebraicznie zamknięte.

Rzeczywiście, niech $K = \{a_1, a_2, ..., a_n\}$ będzie ciałem skończonym o linebreak $n \geq 2$ elementach. Wielomian $v = (\mathbf{x} - a_1)(\mathbf{x} - a_2)...(\mathbf{x} - a_n) + 1$ nie ma w K pierwiastka, bowiem $v(a_i) - 1 \neq 0$ dla dowolnego $a_i \in K$.

Twierdzenie 11.6 *Ciało liczb zespolonych jest algebraicznie zamknięte.*

Dowód twierdzenia podzielimy na dwie części.

1. Wykażemy, że twierdzenie wystarczy wykazać dla wielomianów o współczynnikach rzeczywistych.

Niech $v \in \mathbb{C}[\mathbf{x}]$. Oznaczmy przez $\bar{v}$ wielomian powstały przez zastąpienie wszystkich współczynników v ich sprzężeniami, tzn. jeśli $v(\mathbf{x}) = a_0 + a_1\mathbf{x} + ... + a_d\mathbf{x}^d$ wówczas $\bar{v}(\mathbf{x}) = \bar{a_0} + \bar{a_1}\mathbf{x} + ... + \bar{a_d}\mathbf{x}^d$.

Zauważmy, że wielomian

$$w = v\bar{v}$$

ma współczynniki rzeczywiste. Rzeczywiście, $w(\mathbf{x}) = \sum_{l=0}^{2d} b_l\mathbf{x}^l$, gdzie $b_l = \sum_{i=0}^{l} \bar{a_i}a_{l-i}$ dla $l = 1, \ldots, 2d$. Łatwo sprawdzić, że

[1] Pierwszy dowód Gaussa Zasadniczego Twierdzenia Algebry zawarty był w jego pracy doktorskiej (1799). Gauss miał wtedy 22 lata.

$$\bar{b}_l = \sum_{i=0}^{l} a_i \bar{a}_{l-i} = b_l$$

Czyli $b_l \in \mathbb{R}$ dla wszystkich l.
Jeśli, dla pewnego $u \in \mathbb{C}$ zachodzi $w(u) = 0$, wówczas $\underline{v(u)}\bar{v}(u) = 0$, czyli $v(u) = 0$ lub $\bar{v}(u) = 0$. W drugim przypadku mamy $0 = \bar{v}(u) = \overline{v(\bar{u})}$. A to oznacza, że $\bar{u}$ jest pierwiastkiem wielomianu v.

Z drugiej strony, jeśli $v(u) = 0$ dla pewnego $u \in \mathbb{C}$ wówczas $w(u) = v(u)\bar{v}(u) = 0$.

Tak więc, wielomian v (dowolny wielomian o współczynnikach zespolonych) ma pierwiastek w zbiorze liczb zespolonych wtedy i tylko wtedy, gdy pewien wielomian o współczynnikach rzeczywistych (mianowicie $v\bar{v}$) ma pierwiastek zespolony.

2. Dalsza część dowodu przez indukcję. Niech $v \in \mathbb{R}[\mathbf{x}]$, $\partial v = d = 2^n m$, gdzie m jest liczbą nieparzystą (łatwo zaobserwować, że każdą liczbę naturalną d różną od zera można zapisać w tej postaci). **Indukcję poprowadzimy za względu na** n.
Jeśli $n = 0$, wówczas v jest stopnia nieparzystego - wiemy zaś, że każdy wielomian o współczynnikach rzeczywistych i stopnia nieparzystego ma pierwiastek rzeczywisty.
Przypuśćmy więc, że $n \geq 1$ i niech $u_1, ..., u_d$ będą pierwiastkami wielomianu v w jego ciele rozkładu[2]. Naszym zadaniem będzie wykazanie, że pierwiastki te należą do zbioru liczb zespolonych $\mathbb{C}$.

Mamy w tej sytuacji równość $v(\mathbf{x}) = a(\mathbf{x} - u_1) \cdot ... \cdot (\mathbf{x} - u_d)$ gdzie $a \in \mathbb{R}$. Na mocy twierdzenia 10.1 o wzorach Viety,

$$v(\mathbf{x}) = a\mathbf{x}^d - aS_1(u_1, ..., u_d)\mathbf{x}^{d-1} + ... + (-1)^d aS_d(u_1, ..., u_d)$$

i $S_k(u_1, ..., u_d) \in \mathbb{R}$ dla każdego $k = 1, ..., d$.

Dla dowolnego $h \in \mathbb{Z}$ zdefiniujmy wielomian

$$v_h(\mathbf{x}, \mathbf{x}_1, ..., \mathbf{x}_d) = \prod_{1 \leq i < j \leq d} (\mathbf{x} - \mathbf{x}_i - \mathbf{x}_j - h\mathbf{x}_i\mathbf{x}_j)$$

Oczywiście $v_h \in \mathbb{R}[\mathbf{x}, \mathbf{x}_1, ..., \mathbf{x}_d] = \mathbb{R}[\mathbf{x}][\mathbf{x}_1, ..., \mathbf{x}_d]$. Co więcej, dla ustalonego $h \in \mathbb{Z}$ wielomian v_h jest wielomianem symetrycznym ze względu na zmienne wielomianowe $\mathbf{x}_1, ..., \mathbf{x}_d$. A więc, na mocy Zasadniczego Twierdzenia o Wielomianach Symetrycznych, v_h jest wielomianem $S_1(\mathbf{x}_1, ..., \mathbf{x}_d), ..., S_d(\mathbf{x}_1, ..., \mathbf{x}_d)$ o współczynnikach w $\mathbb{R}[\mathbf{x}]$. Skoro $S_1(u_1, ..., u_d), ..., S_d(u_1, ..., u_d) \in \mathbb{R}$ także wielomian $v_h(\mathbf{x}, u_1, ..., u_d)$ (a więc wielomian zmiennej $\mathbf{x}$) ma współczynniki w $\mathbb{R}$ (dla każdego całkowitego h). Stopień każdego z tych wielomianów (bo dla każdego $h \in \mathbb{Z}$ mamy jeden wielomian v_h) **ze względu na x** wynosi

$$\partial v_h = \binom{d}{2} = \frac{1}{2}d(d-1) = 2^{n-1}m(2^n m - 1)$$

Z założenia indukcyjnego, v_h ma pierwiastek w $\mathbb{C}$ (to, że te wielomiany mają pierwiastki, wiadomo z Twierdzenia o Ciele Rozkładu - ważne jest to, że ten pierwiastek

[2]Tu właśnie korzystamy z Twierdzenia o Ciele Rozkładu.

jest w $\mathbb{C}$).

Wobec tego każdy wielomian v_h (dla każdego $h \in \mathbb{Z}$) ma pierwiastek w $\mathbb{C}$ i to równy $u_i + u_j + hu_iu_j$ dla pewnych i, j, a stąd relacja

$$u_i + u_j + hu_iu_j \in \mathbb{C}$$

jest spełniona dla nieskończonej liczby parametrów h. Indeksów i, j jest zaś skończona liczba (par (i, j) jest co najwyżej d^2). Muszą więc istnieć i_0 oraz j_0 (ustalone) oraz takie h i h', oba całkowite, $h \neq h'$, że

$$u_{i_0} + u_{j_0} + hu_{i_0}u_{j_0} \in \mathbb{C}$$

$$u_{i_0} + u_{j_0} + h'u_{i_0}u_{j_0} \in \mathbb{C}$$

Stąd łatwo wywnioskować, że

$$u_{i_0}u_{j_0} \in \mathbb{C}$$

oraz

$$u_{i_0} + u_{j_0} \in \mathbb{C}$$

A więc $(\mathbf{x} - u_{i_0})(\mathbf{x} - u_{j_0}) \in \mathbb{C}[\mathbf{x}]$. Równanie zaś kwadratowe o współczynnikach zespolonych ma rozwiązania zespolone (a więc $u_{i_0}, u_{j_0} \in \mathbb{C}$). ■

Przypuśćmy, że c jest pierwiastkiem wielomianu $v = a_0 + a_1\mathbf{x} + \cdots + a_n\mathbf{x}^n$ o współczynnikach rzeczywistych. Mamy wówczas

$$v(c) = a_0 + a_1c + \ldots a_nc^n = 0$$

i stąd

$$\overline{v(c)} = a_0 + a_1\overline{c} + ... + a_n\overline{c}^n = \overline{0} = 0$$

co oznacza, że także $\overline{c}$ jest pierwiastkiem v. Wobec tego w rozkładzie v na czynniki liniowe występuje zarówno czynnik $\mathbf{x} - c$ jak i $\mathbf{x} - \overline{c}$. Ponieważ iloczyn

$$(\mathbf{x} - c)(\mathbf{x} - \overline{c}) = \mathbf{x}^2 - (c + \overline{c})\mathbf{x} + c\overline{c}$$

ma współczynniki rzeczywiste, wielomian v można zapisać w postaci

$$v = (\mathbf{x}^2 + a\mathbf{x} + c)w$$

gdzie $a, b \in \mathbb{R}, w \in \mathbb{R}[\mathbf{x}]$. Udowodniliśmy w ten sposób następujący wniosek.

Wniosek 11.7 *Niech $v \in \mathbb{R}[\mathbf{x}]$. Wówczas v ma jednoznaczny rozkład na iloczyn postaci*

$$v = a(\mathbf{x} - c_1) \cdot ... \cdot (\mathbf{x} - c_l)(\mathbf{x}^2 + d_1\mathbf{x} + e_1) \cdot ... \cdot (\mathbf{x}^2 + d_k\mathbf{x} + e_k)$$

gdzie $c_1, ..., c_l, d_1, ..., d_k, e_1, ..., e_k \in \mathbb{R}$, $l + 2k$ jest stopniem wielomianu v, zaś wielomiany stopnia drugiego (trójmiany kwadratowe) są nad $\mathbb{R}$ nierozkładalne i każdy z nich odpowiada pewnemu pierwiastkowi zespolonemu v. ■

11.3 Rozszerzenia o skończoną liczbę elementów

Twierdzenie 11.8 *Niech E będzie rozszerzeniem ciała F $(E : F)$, $a_1, ..., a_n \in E$, $1 \leq k \leq n$. Wówczas*

$$F(a_1, ..., a_k)(a_{k+1}, ..., a_n) = F(a_1, ..., a_n)$$

Dowód. Na mocy definicji ze strony 147, $F(a_1, ..., a_n)$ jest najmniejszym ciałem zawierającym[3] ciało F i elementy $a_1, ..., a_n$. Ciało $F(a_1, ..., a_k)(a_{k+1}, ..., a_n)$ zawiera ciało F i elementy $a_1, ..., a_n$, stąd zawieranie

$$F(a_1, ..., a_n) \subset F(a_1, ..., a_k)(a_{k+1}, ..., a_n)$$

$F(a_1, ..., a_n)$ jest ciałem, zawiera ciało $F(a_1, ..., a_k)$ oraz elementy $a_1, ..., a_k$, na mocy definicji $F(a_1, ..., a_k)(a_{k+1}, ..., a_n)$ jest najmniejszym ciałem o tej własności, skąd wynika zawieranie

$$F(a_1, ..., a_k)(a_{k+1}, ..., a_n) \subset F(a_1, ..., a_n)$$

To kończy dowód twierdzenia 11.8. ■

11.4 Rozszerzenia skończone i algebraiczne

Jeśli E i F są ciałami i $E : F$ i wymiar przestrzeni wektorowej E nad ciałem F wynosi n to piszemy $n = [E : F]$ i mówimy, że n jest **wymiarem rozszerzenia** $E : F$ (lub, że E ma wymiar n nad F). Rozszerzenie E nazywamy wówczas **skończonym**. **Bazą** ciała E nad F nazywamy bazę E (traktowanego jako przestrzeń wektorowa nad F). E jest **rozszerzenienm nieskończonym** E, jeśli nie jest rozszerzeniem skończonym.

Element $a \in E$ nazywamy **algebraicznym** nad F jeśli a jest pierwiastkiem pewnego, nie zerowego wielomianu $v \in F[x]$. **Liczbą algebraiczną** nazywamy dowolny element algebraiczny nad ciałem $\mathbf{Q}$.

Przykład 11.6 Liczby $i, \sqrt{3}, \sqrt{2-\sqrt{3}}$ oraz $i + \sqrt{3}$ są liczbami algebraicznymi. Sprawdźmy, że $a = \sqrt{2-\sqrt{3}}$ jest liczbą algebraiczną.

Rzeczywiście, $a^2 = 2-\sqrt{3}$. Stąd $3 = a^4 - 4a^2 + 4$ i widzimy, że a jest pierwiastkiem wielomianu $\mathbf{x}^4 - 4\mathbf{x}^2 + 1 \in \mathbb{Q}[\mathbf{x}]$.

Rozszerzenie E ciała F nazywamy **algebraicznym** jeżeli każdy element $a \in E$ jest algebraiczny nad F.

Przykład 11.7 Ciało liczb zespolonych jest rozszerzeniem algebraicznym ciała liczb rzeczywistych $\mathbb{R}$, bowiem każda liczba zespolona $a + ib$ (gdzie $a, b \in \mathbb{R}$) jest pierwiastkiem wielomianu $\mathbf{x}^2 - 2a\mathbf{x} + a^2 + b^2$.

[3] Także w tym miejscu upraszczamy nieco sytuację. W rzeczywistości chodzi o najmniejsze ciało zawierające elementy $a_1, ..., a_n \in E$ i podciało ciała E które jest z F izomorficzne (por. przypis ze strony 159).

Wielomian $u \in F[\mathbf{x}]$ nazywamy **wielomianem unormowanym** jeżeli jego **współczynnik dominujący**, to jest współczynnik przy nawyższej potędzie $\mathbf{x}$, jest równy 1_F. Dla przykładu, wielomian $\mathbf{x}^2 + 2\mathbf{x} - 1 \in \mathbb{Q}[\mathbf{x}]$ jest unormowany, natomiast wielomian $2\mathbf{x}^2 + 4\mathbf{x} - 2$ unormowany nie jest.

Twierdzenie 11.9 (O wielomianie minimalnym) *Dla każdego elementu algebraicznego $a \in E$, gdzie $E : F$, istnieje dokładnie jeden wielomian unormowany $v \in F[\mathbf{x}]$ taki, że*

1. *v jest nierozkładalny nad F,*
2. *$v(a) = 0$,*
3. *$w \in F[\mathbf{x}], w(a) = 0 \Rightarrow v|w$*

Wielomian v spełniający warunki (1)-(3) nazywamy **wielomianem minimalnym elementu algebraicznego** *a, zaś ∂v (stopień wielomianu minimalnego elementu a)* **stopniem** *a i oznaczamy przez $\deg_F(a)$.*

Dowód. Dla dowolnego elementu algebraicznego a zbiór wielomianów v spełniających warunki 1. i 2. jest oczywiście niepusty. Niech v będzie wielomianem unormowanym minimalnego stopnia takim, że $v(a) = 0$. Przypuśćmy, że $w \in F[\mathbf{x}]$, $w(a) = 0$. Wiemy, że istnieją wielomiany $q, r \in F[\mathbf{x}]$ takie, że $w = vq + r$ oraz $\partial r < v$ lub $r = 0$. Gdyby jednak $r \neq 0$, wówczas mielibyśmy

$$r(a) = w(a) - v(a)q(a) = 0$$

a to sprzeczne z wyborem wielomianu r (r jest stopnia niższego niż najniższy stopień wielomianu zerującego się na a).

Pozostaje wykazać, że wielomian v jest jedynym o własnościach 1-3.

Niech $v, w \in F[\mathbf{x}] : v(a) = w(a) = 0$, v, w - unormowane i spełniające warunek 3. twierdzenia. Mamy wówczas $v|w$ oraz $w|v$ i stąd $\partial v = \partial w$. Ponieważ v i w są znormalizowane, mamy $\partial(v - w) < \partial v$ oraz $(v - w)(a) = v(a) - w)a) = 0$. Stąd $v|(v - w)$ i wobec tego $v - w = 0$. ■

Przykład 11.8 Znajdziemy wielomian minimalny dla $a = \sqrt{5 - \sqrt{3}}$ nad $\mathbb{Q}$. Mamy $a^2 = 5 - \sqrt{3}$ a stąd $3 = 25 - 10a^2 + a^4$.
Nie jest zbyt trudno wykazać, że nad $\mathbb{Q}$ wielomian $\mathbf{x}^4 - 10\mathbf{x}^2 + 22$ jest nierozkładalny (por. zadanie 11.5). Jest to więc wielomian minimalny elementu a. ■

Twierdzenie o wielomianie minimalnym pozwala opisać rozszerzenia proste i algebraiczne w sposób następujący.

Twierdzenie 11.10 (O rozszerzeniu prostym o element algebraiczny) *Niech $E : F$ będzie rozszerzeniem ciała F, $a \in E$ elementem algebraicznym stopnia n. Wówczas*

1. *$F(a) = \{\alpha_0 + \alpha_1 a + ... + \alpha_{n-1} a^{n-1} | \alpha_i \in F\}$,*

2. $\{1, a, a^2, ..., a^{n-1}\}$ *jest bazą* $F(a)$ *nad* F,

3. $[F(a) : F] = n$ *(inaczej:* $[F(a) : F] = \deg_F(a)$*),*

4. $F(a) \simeq F[\mathbf{x}]/(m)$*, gdzie* m *jest wielomianem minimalnym elementu* a *nad* F*.*

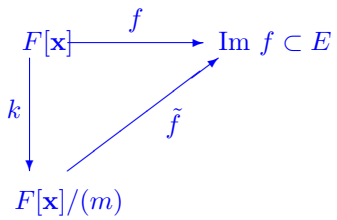
Dowód. Rozważmy następujące odwzorowanie

$$f : F[\mathbf{x}] \ni v \to v(a) \in E$$

f jest oczywiście homomorfizmem pierścieni o jądrze

$$\text{Ker } f = \{v \in F[\mathbf{x}] : v(a) = 0\}$$

Z twierdzenia 11.9 o wielomianie minimalnym wynika, że Ker $f = (m)$, gdzie m jest wielomianem minimalnym elementu a nad F. m jest wielomianem nierozkładalnym nad F a więc, na mocy twierdzenia 11.2, $F[\mathbf{x}]/(m)$ jest ciałem. Z twierdzenia 8.8 (str. 110) o izomorfizmie pierścieni, które tu najwygodniej zacytować w postaci diagramu:



wynika, że pierścień Im f jest izomorficzny z $F[\mathbf{x}]/(m)$ a więc także Im f jest ciałem. $a \in$ Im f, bowiem $a = f(\mathbf{x})$, a więc Im $f \supset F(a)$ (Im f jest ciałem, które zawiera F i a, natomiast $F(a)$ jest, na mocy definicji, najmniejszym ciałem zawierającym F i a). Z drugiej strony, jeśli $b \in$ Im f to $b = v(a)$, gdzie v jest pewnym wielomianem z $F[\mathbf{x}]$, a więc $b \in F(a)$ i ostatecznie $F(a) =$ Im f.
Udowodniliśmy więc punkty (1) i (4) twierdzenia o rozszerzeniu prostym o element algebraiczny.
Z (1) wynika, że elementy $1, a, ..., a^{n-1}$ generują $F(a)$. Pozostaje więc udowodnienie, że są liniowo niezależne a stąd już będziemy mieli zarówno fakt, że stanowią bazę przestrzeni $F(a)$ nad F jak i to, że $[F(a) : F] = \deg_F(a)$ (pamiętamy, że stopień elementu a nad F to stopień wielomianu minimalnego elementu a, czyli n).
Przypuśćmy, że

$$\beta_0 + \beta_1 a + ... + \beta_{n-1} a^{n-1} = 0$$

To oznacza jednak, że a jest pierwiastkiem wielomianu $w = \beta_0 + \beta_0 \mathbf{x} + ... + \beta_{n-1}\mathbf{x}^{n-1}$. Wiemy jednak, że $\deg_F(a) = n$, a stąd wynika, że w jest wielomianem zerowym, to znaczy $\beta_0 = \beta_1 = ... = \beta_{n-1} = 0$, co kończy dowód niezależności liniowej $1, a, ..., a^{n-1}$ i twierdzenia 11.10. ∎

Z punktu 4 twierdzenia 11.10 łatwo wynika następujący wniosek.

Wniosek 11.11 *Jeżeli $a, b \in E : F$ są dwoma pierwiastkami wielomianu nierozkładalnego w $F[\mathbf{x}]$, wówczas rozszerzenia $F(a)$ i $F(b)$ są izomorficzne.* ■

Przykład 11.9 (Rozszerzenie $\mathbb{Q}(1+i) : \mathbb{Q}$) Zapiszmy $a = 1+i$. Wtedy $(a-1)^2 = -1$ a stąd

$$a^2 - 2a + 2 = 0$$

co oznacza, że a jest pierwiastkiem wielomianu $\mathbf{x}^2 - 2\mathbf{x} + 2$. Wielomian ten jest nierozkładalny (nie ma pierwiastka w $\mathbb{Q}$) i stąd $m = \mathbf{x}^2 - 2\mathbf{x} + 2$ jest wielomianem minimalnym a. Na mocy twierdzenia o rozszerzeniu prostym o element algebraiczny

$$\mathbb{Q}(a) = \{\alpha + \beta a : \alpha, \beta \in \mathbb{Q}, a^2 = 2a - 2\}$$

Zauważmy, że o ile dodawanie w $\mathbb{Q}(a)$ jest bardzo proste:

$$(\alpha + \beta a) + (\gamma + \delta a) = (\alpha + \gamma) + (\beta + \delta)a$$

to mnożenie jest nieco bardziej skomplikowane:

$$(\alpha + \beta a)(\gamma + \delta a) = \alpha\gamma + (\alpha\delta + \beta\gamma)a + \beta\gamma a^2 = \alpha\gamma + (\alpha\delta + \beta\gamma)a + \beta\gamma(2a - 2)$$

$$= (\alpha\gamma - 2\beta\gamma) + (\alpha\delta + 3\beta\gamma)a$$

□

Przykład 11.10 Nietrudno sprawdzić, że rozszerzenie ciała liczb wymiernych $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots)$$

jest rozszerzeniem algebraicznym, nie jest natomiast rozszerzeniem skończonym. □

Przykład 11.11 $[\mathbb{R} : \mathbb{Q}]$ Wielomian $\mathbf{x}^n - 2$ jest, na mocy kryterium Eisensteina, nieredukowalny nad $\mathbb{Q}$. Stąd $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ i skoro $\mathbb{R} \supset \mathbb{Q}(\sqrt[n]{2})$ dla każdego n, $[\mathbb{R} : \mathbb{Q}]$ jest nieskończony. □

Przypuśćmy, że $L : K$ jest rozszerzeniem skończonym, powiedzmy $[L : K] = k$, i niech $a \in L$. Ponieważ każde $k+1$ elementy L są liniowo zależne nad K, liniowo zależne są $a^0 = 1, a^1, a^2, \dots, a^k$. Istnieją więc $\alpha, \dots, \alpha_k \in K$ takie, że

$$\alpha_0 + \alpha_1 a + \cdots + \alpha_k a^k = 0$$

To zaś oznacza dokładnie tyle, że a jest pierwiastkiem wielomianu $\alpha_0 + \alpha_1\mathbf{x} + \cdots + \alpha_k\mathbf{x}^k \in K[\mathbf{x}]$, a więc elementem algebraicznym nad K. Wykażemy nieco więcej a mianowicie twierdzenie następujące.

Twierdzenie 11.12 (O rozszerzeniach skończonych) *Każde rozszerzenie skończone jest rozszerzeniem algebraicznym. Co więcej, jeśli $[L : K] = k$ i $a_1, \dots, a_k$ jest bazą L nad K, to $L = K(a_1, \dots, a_k)$ i każdy element $b \in L$ jest elementem algebraicznym stopnia co najwyżej k nad K.*

Dowód. Powyżej wykazaliśmy już, że każdy element rozszerzenia skończonego jest elementem algebraicznym a więc, że każde rozszerzenia skończone jest algebraiczne. Udowodnimy, że jeśli $a_1, a_2, \ldots, a_k$ jest bazą L nad K, wówczas $L = K(a_1, a_2, \ldots, a_k)$. Rzeczywiście, skoro $a_1, \ldots, a_k \in L$, to

$$K(a_1, a_2, \ldots, a_k) \subset L$$

Niech teraz $a \in L$. Wtedy $a = \sum_{i=1}^{k} \beta_i a_i$, gdzie $\beta_i \in K$ dla $i = 1, \ldots, k$ (pamiętamy, że $\{a_1, \ldots, a_k\}$ jest bazą L nad K). Stąd wynika natychmiast, że $a \in K(a_1, \ldots, a_k)$, bowiem w $K(a_1, \ldots, a_k)$ są wyniki wszystkich operacji, które na elementach $a_1, \ldots, a_k$ można wykonać w ciele (a nie tylko ich kombinacje liniowe o współczynnikach w K). ■

Twierdzenie 11.13 (Twierdzenie o iloczynie wymiarów rozszerzeń) *Niech E, F, K będą ciałami, $E : F$, $F : K$.*
Rozszerzenie $E : K$ jest skończone wtedy i tylko wtedy, gdy rozszerzenia $E : F$ i $F : K$ są skończone. Zachodzi wtedy wzór

$$[E : K] = [E : F][F : K] \tag{11.1}$$

i jeśli bazą E nad F jest $e_1, e_2, ...e_m$, bazą F nad K jest $f_1, f_2, ..., f_n$ to bazą $E : K$ jest

$$\{e_i f_j : i = 1, ..., m; j = 1, ..., n\}$$

Twierdzenie 11.13 bywa nazywane także **twierdzeniem o wieży**. Zapewne dlatego, że wzór (11.1) można zapisać w postaci

$$\left[\frac{E}{F}\right] = \frac{\left[\frac{E}{K}\right]}{\left[\frac{F}{K}\right]} \tag{11.2}$$

Dowód twierdzenia 11.13. W dowodzie wygodnie będzie zakładać, że $K \subset F \subset E$, choć w rzeczywistości wiemy tylko, że K jest ciałem izomorficznym z pewnym podciałem ciała F, zaś F jest izomorficzne z pewnym podciałem ciała E[4].

- Jeśli rozszerzenie $E : K$ jest skończone, wówczas także $F : K$ jest skończone bowiem F (ciało traktowane teraz jako przestrzeń wektorowa) jest podprzestrzenią E nad ciałem K. Podobnie, E jest skończenie wymiarową przestrzenią wektorową nad F. Rzeczywiście każda baza E nad K generuje E a więc, na mocy znanego twierdzenia z algebry liniowej[5], można z niej wybrać bazę E nad F.

[4] Takie uproszczenie jest uproszczeniem opisu jedynie a nie idei całej sytuacji jaką w tym momencie mamy. To jest to samo uproszczenie, które popełniamy gdy mówimy, że *zbiór licb rzeczywistych jest podzbiorem liczb zespolonych.* Oczywiście liczby rzeczywiste nie są liczbami zespolonymi, bowiem nie są parami liczb rzeczywistych. Niemniej można je traktować jako pary, w których drugi element jast równy zeru. Traktując na tej zasadzie liczby rzeczywiste jako zespolone *o części urojonej równej zeru*, o ile tylko robimy to świadomie, nie popełniamy błędu, natomiast nasz wywód staje się mniej skomplikowany.

[5] Chodzi o twierdzenie, które mówi, że z każdego zbioru generującego przestrzeń można wybrać bazę tej przestrzeni.

- Przypuśćmy teraz, że $E : F$ i $F : K$ są rozszerzeniami skończonymi powiedzmy, że $e_1, e_2, ..., e_m \in E$ jest bazą E nad F i $f_1, f_2, ..., f_n \in F$ jest bazą F nad K. Wówczas dla każdego $a \in E$ istnieją $\alpha_1, ..., \alpha_m \in F$ takie, że

$$a = \sum_{i=1}^{m} \alpha_i e_i$$

Podobnie, dla każdego $i \in \{1, 2, ..., m\}$ istnieją $a_{ij} \in K$, że

$$\alpha_i = \sum_{j=1}^{n} a_{ij} f_j$$

Stąd mamy

$$a = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} f_j \right) e_i = \sum_{i,j} a_{ij} e_i f_j$$

co dowodzi, że zbiór $B = \{e_i f_j : i = 1, ..., m; j = 1, ..., n\}$ generuje E nad K. Pozostaje więc udowodnić, że zbiór B jest liniowo niezależny.
Przypuśćmy, że

$$\sum_{i,j} \gamma_{ij} e_i f_j = 0$$

gdzie $\gamma_{ij} \in K$ dla $i = 1, ..., m; j = 1, ..., n$. Mamy wówczas

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} \gamma_{ij} f_j \right) e_i = 0$$

Ponieważ $\gamma_{ij} \in K, f_i \in F$ dla $i = 1, ..., m; j = 1, ..., n$ mamy $\sum_{j=1}^{n} \gamma_{ij} f_j \in F$. Skoro $e_1, ..., e_m$ są liniowo niezależne w E nad F otrzymujemy

$$\sum_{j=1}^{n} \gamma_{ij} f_j = 0 \text{ fla każdego } i = 1, ..., m$$

a więc, wobec liniowej niezależności $f_1, ..., f_n$ nad K otrzymujemy ostatecznie $\gamma_{ij} = 0$ dla $i = 1, ..., m; j = 1, ..., n$.

■

Twierdzenie 11.14 *Niech $E : F$ i niech $a \in E$ będzie elementem algebraicznym nad F. Jeśli $b \in F(a)$ to b jest także elementem algebraicznym nad F i stopień b nad F dzieli stopień a nad F. Inaczej mówiąc*

$$deg_F(b) \mid \deg_F(a)$$

Dowód. Skoro $b \in F(a)$ mamy ciąg zawierań (por. przypis ze strony 159):

$$F \subset F(b) \subset F(a)$$

Na mocy twierdzenia 11.10 rozszerzenie $F(a) : F$ jest skończone. Wobec tego możemy skorzystać z twierdzenia 11.13 o iloczynie wymiarów rozszerzeń, na mocy którego także rozszerzenia $F(a) : F(b)$ i $F(b) : F$ są skończone i

$$[F(a) : F] = [F(a) : F(b)] \cdot [F(b) : F]$$

Z części (3) twierdzenia 11.10 $[F(b) : F] = \deg_F(b)$ i $[F(a) : F] = \deg_F(a)$ co oznacza, że $deg_F(b) \mid \deg_F(a)$. ■

Przykład 11.12 Znajdziemy rozszerzenia $\mathbb{Q}(\sqrt[3]{2})$ i $\mathbb{Q}(\sqrt[3]{4})$ i ich wymiary nad $\mathbb{Q}$. Ponieważ $\sqrt[3]{4} = (\sqrt[3]{2})^2$ mamy $\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$ i wobec tego

$$\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}(\sqrt[3]{4}) \supset \mathbb{Q}$$

Mamy także $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ bowiem wielomian $\mathbf{x}^3 - 2$, którego $\sqrt[3]{2}$ jest pierwiastkiem jest wielomianem nierozkładalnym nad $\mathbb{Q}$. Skoro (twierdzenie 11.14) $[\mathbb{Q}(\sqrt[3]{4}) : \mathbb{Q}]$ dzieli $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ mamy

$$[\mathbb{Q}(\sqrt[3]{4}) : \mathbb{Q}] = 3$$

i w konsekwencji $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{4})$. □

11.5 Rozszerzenia przestępne

Element $a \in E$ nazywamy **elementem przestępnym** nad F (gdzie $E : F$), jeżeli a nie jest algebraiczny nad F. Elementy przestępne nad **Q** nazywamy **liczbami przestępnymi**.

Rozszerzenia proste o element przestąpny charakteryzuje poniższe twierdzenie.

Twierdzenie 11.15 *Jeśli a jest elementem przestępnym nad ciałem F wówczas rozszerzenie proste $F(a)$ jest izomorficzne z ciałem funkcji wymiernych*

$$F(\mathbf{x}) = \left\{ \frac{v(a)}{w(a)} : v, w \in F[\mathbf{x}] \right\}$$

Zbiór elementów przestąpnych ciała $F(a)$ jest równy $F(a) - F$.

Dowód. Łatwy dowód faktu, że odwzorowanie

$$F(\mathbf{x}) \ni \frac{v}{w} \to \frac{v(a)}{w(a)} \in F(a)$$

jest izomorfizmem pierścieni (pamiętamy, że skoro a jest elementem prestępnym F wynika, że dla $w \neq 0$ mamy $w(a) \neq 0$) pozostawiony jest Czytelnikowi.

Wykażemy, że wszystkie elementy algebraiczne ciała $F(a)$ należą do F.
Niech $b = \frac{v(a)}{w(a)}$ będzie elementem algebraicznym $F(a)$. O wielomianach v i w możemy założyć, że są względnie pierwsze (nie mają wspólnych nietrywialnych dzielników).
Skoro b jest elementem algebraicznym, istnieje wielomian $u = \alpha_0 + \alpha_1\mathbf{x} + ... + \alpha_k\mathbf{x}^k$ o współczynnikach $\alpha_i \in F$ $(i = 1, ..., k)$ taki, że $u(b) = 0$. Mamy wówczas

$$\alpha_0 + \alpha_1\frac{v(a)}{w(a)} + ... + \alpha_k\left(\frac{v(a)}{w(a)}\right)^k = 0$$

a po stosownych przekształceniach

$$\alpha_0(w(a))^k + \alpha_1 v(a)(w(a))^{k-1} + ... + \alpha_k(v(a))^k = 0$$

Ponieważ jednak a jest elementem przestępnym musimy mieć

$$\alpha_0(w(\mathbf{x}))^k + \alpha_1 v(\mathbf{x})(w(\mathbf{x}))^{k-1} + ... + \alpha_{k-1}w(\mathbf{x})(v(\mathbf{x}))^{k-1} + \alpha_k(v(\mathbf{x}))^k = 0$$

(a nie jest pierwiastkiem żadnego niezerowego wielomianu z $F[\mathbf{x}]$). Z ostatniej równości wynika, że wielomian v dzieli w^k i wielomian w dzieli wielomian v. Zarówno wielomian v jak wielomian w są więc stopnia zerowego i $\frac{v}{w} \in F$ a stąd już $b = \frac{v}{w} \in F$, co kończy dowód. ■

Wniosek 11.16 *Jeśli a i b są elementami przestępnymi nad ciałem F, wówczas rozszerzenia $F9a)$ i $F(b)$ są izomorficzne.* ■

Przez $F(\mathbf{x})$ oznaczamy ciało ułamków pierścienia $F[\mathbf{x}]$, czyli $F(\mathbf{x}) = \{\frac{u}{v}; u, v \in F[\mathbf{x}], v \neq 0\}$. Element $\mathbf{x} \in F(\mathbf{x})$ nie jest elementem algebraicznym ciała $F(\mathbf{x})$. Rzeczywiście, gdyby dla pewnego wielomianu $v \in F[\mathbf{x}]$ zachodziło $v(\mathbf{x}) = 0$ oznaczałoby to, że wielomian v jest wielomianem zerowym, a taki wielomian nie ma pierwiastków. Udowodniliśmy więc twierdzenie następujące.

Twierdzenie 11.17 *$F(\mathbf{x})$ jest rozszerzeniem prostym przestępnym ciała F.*

Z powyższego twierdzenia wynika, że istnieją rozszerzenia proste, które nie są algebraiczne. Stąd zaś i z twierdzenia 11.12 wynika, że rozszerzenia proste niekoniecznie są skończone.

Dość łatwo zauważyć, że zbiór liczb algebraicznych to zbiór pierwiastków wszystkich wielomianów o współczynnikach całkowitych. Rzeczywiście, wielomian $v = a_0 + a_1\mathbf{x} + ... + a_n\mathbf{x}^n \in \mathbb{Q}[\mathbf{x}]$ zeruje się w a wtedy i tylko wtedy gdy wielomian $w = b_0 + ... + b_n\mathbf{x}^n \in \mathbb{Z}[\mathbf{x}]$, gdzie $w = mv$, zaś m jest wspólnym mianownikiem $b_0, ..., b_n$, zeruje się w a.
Oznaczmy przez W_k zbiór wielomianów postaci $a_0 + a_1\mathbf{x} + ... + a_n\mathbf{x}^n \in \mathbb{Z}[x]$ takich, że $n + |a_0| + |a_1| + ... + |a_n| \leq k$. Dla każdego $k \in \mathbb{N}$ zbiór W_k jest skńczony oraz $\bigcup_{k\in\mathbb{N}} W_k = \mathbb{Z}[\mathbf{x}]$, a więc $\mathbb{Z}[\mathbf{x}]$ jest zbiorem przeliczalnym. Ponieważ zaś każdy wielomian ma skończoną (a więc przeliczalną) liczbę pierwiastków, zbiór wszystkich pierwiastków wszystkich wielomianów o współczynnikach całkowitych jest zbiorem przeliczalnym. Tym samym udowodniliśmy następujące twierdzenie Cantora.

Twierdzenie 11.18 (Cantor) *Zbiór liczb rzeczywistych algebraicznych jest przeliczalny.*

Tym samym liczby przestępne istnieją. Co więcej, zbiór liczb przestępnych nie jest przeliczalny.

11.6 Rząd ciała skończonego

Ciała skończone zostały wprowadzone przez Ewarysta Galois[6] (choć bez nadawania im nazwy, sama nazwa *ciało* jest nieco późniejsza, została wprowadzona przez Dedekinda[7] lub Dirichleta[8]). Stąd ciało skończone nazywamy **ciałem Galois**[9] i oznaczamy przez $G\mathbb{F}(q)$.

Twierdzenie 11.19 (Galois) *Jeśli F jest ciałem skończonym, wówczas $|F| = p^n$, gdzie p jest charakterystyką F (a więc liczbą pierwszą, na mocy twierdzenia 8.12) zaś $n \in \mathbb{N}$.*

Dowód. Niech F będzie ciałem skończonym, $p = \text{char}\,(P)$. Wówczas F zawiera podciało rzędu p o elementach

$$1_F, 1_F + 1_F = 2 \cdot 1_F, ..., (p-1) \cdot 1_f, p \cdot 1_F = 0_F$$

gdzie 1_F i 0_F są, odpowiednio, jedynką i zerem ciała F. Podciało to jest oczywiście generowane przez 1_F i jest izomorficzne z $\mathbb{Z}_p$. Stąd wynika, jak już wspomniano w tekście twierdzenia, że p jest liczbą pierwszą. Oznaczmy przezF_p podciało generowane przez 1_F. Ciało F jest wtedy rozszerzeniem F_p $(F : F_p)$ i jest to rozszerzenie skończone. Oznaczmy przez $n = |F : F_p|$ - stopień rozszerzenia $F : F_p$ i niech $\{b_1, ..., b_n\}$ będzie bazą F nad F_p (warto przypomnieć, że każde ciało jest przestrzenią wektorową nad swoim dowolnym podciałem). Wtedy każdy element $a \in F$ można **jednoznacznie** zapisać w postaci

$$a = \alpha_1 b_1 + ... + \alpha_n b_n$$

gdzie $\alpha_i \in F_p$. Stąd oczywiście wynika, że takich elementów jest dokładnie p^n. ■

[6] Évariste Galois 1821 - 1832. Galois jest legendą matematyki. Zginął w absurdalnym pojedynku mając zaledwie 20 lat. Mimo to jego osiągnięcia w dziedzinie matematyki są ogromne. Pierwszy operował pojęciem grupy abstrakcyjnej. Chętnych do zapoznania się z dorobkiem Galois odsyłam do książek: *I. Stewart, Galois Theory, Chapman & Hall* i/lub *J-P. Tignol, Galois' Theory of Algebraic Equations, World Scientific*. Zainteresowanych burzliwą historią krótkiego życia Galois z pewnością zainteresuje książka *Leopolda Infelda, Wybrańcy Bogów* (wszystkie te książki mają wiele wydań).

[7] Richard Dedekind, 1831-1916. Uczeń Dirichleta.

[8] Johann Dirichlet, 1805-1859.

[9] W istocie wykażemy, że ciało takie istnieje tylko wtedy, gdy q jest potęgą liczby pierwszej i jest wówczas, z dokładnością do izomorfizmu, jedyne.

11.7 Pochodne wielomianów i krotności pierwiastków

Niech F będzie ciałem, $v \in F[\mathbf{x}]$ a $E : F$ dowolnym rozszerzeniem zawierającym ciało rozkładu F. Rozkład v w $E[\mathbf{x}]$ można wtedy zapisać w następujący sposób

$$v = a(\mathbf{x} - a_1)^{k_1} \cdot ... \cdot (\mathbf{x} - a_s)^{k_s}$$

gdzie $a_i \in E$, $a_i \neq a_j$ dla $i \neq j$. Zakładamy, że $k_i \geq 1$ dla wszystkich $i = 1, ..., s$. Mówimy wtedy, że **pierwiastek** a_i **jest** k_i**-krotny**. Jeśli $k_i = 1$ wówczas mówimy, że a_i jest pierwiastkiem jednokrotnym wielomianu v.
W badaniu krotności pierwiastków wielomianów użytecznym pojęciem okazuje się pochodna[10].
Pochodną wielomianu $v = a_0 + a_1\mathbf{x} + ... + a_n\mathbf{x}^n \in P[\mathbf{x}]$, gdzie P jest pewnym pierścieniem przemiennym z jedynką, nazywamy wielomian $v' = a_1 + 2a_2\mathbf{x} + ... + na_n\mathbf{x}^{n-1}$.
Nie jest zbyt trudno sprawdzić, że dla dowolnych wielomianów $u, v \in P[\mathbf{x}]$ spełnione są następujące związki:

$$(u + v)' = u' + v' \tag{11.3}$$

$$(au)' = au' \tag{11.4}$$

dla $a \in P$ oraz

$$(uv)' = u'v + uv' \tag{11.5}$$

Twierdzenie 11.20 *Niech F będzie pewnym ciałem, $a \in F$. $(\mathbf{x}-a)^2$ dzieli wielomian $v \in F[\mathbf{x}]$ wtedy i tylko wtedy gdy $\mathbf{x} - a$ dzieli zarówno v jak i v'.*

Dowód. Jeśli $(\mathbf{x} - a)^2$ dzieli v wówczas $v = (\mathbf{x} - a)^2 w, w \in E[\mathbf{x}]$. Wtedy

$$v' = 2(\mathbf{x} - a)w + (\mathbf{x} - a)^2 w' = (\mathbf{x} - a)(2w + (\mathbf{x} - a)w'$$

Wielomian $\mathbf{x} - a$ dzieli więc zarówno v jak v'.
Załóżmy teraz, że $\mathbf{x} - a$ dzieli v i v'. Wykażemy, że $(\mathbf{x} - a)^2$ dzieli v.
Skoro $(\mathbf{x} - a)|v$ możemy napisać $v = (x - a)w$ i w konsekwencji $v' = w + (\mathbf{x} - a)w'$. Ponieważ $(\mathbf{x}-a)|v'$ i $w = v'-(\mathbf{x}-a)w'$, wielomian $\mathbf{x}-a$ dzieli w, a więc możemy napisaać $w = (\mathbf{x}-a)u$, gdzie $u \in F[\mathbf{x}]$, czyli $v = (\mathbf{x}-a)^2 u$, co kończy dowód twierdzenia. ■

Z twierdzenia 11.20 wynika następujący wniosek.

Wniosek 11.21 *Jeśli F jest dowolnym ciałem, $v \in F[\mathbf{x}]$, wówczas $a \in F$ jest jednokrotnym pierwiastkiem wielomianu v wtedy i tylko wtedy gdy $v(a) = 0$ i $v'(a) \neq 0$.* ■

[10] Pochodna wielomianu tu prezentowana jest pojęciem czysto algebraicznym. Nie korzystamy z takich pojęć jak metryka czy zbieżność a wielomiany nie są funkcjami (choć z każdym wielomianem można pewną funkcję skojarzyć).

11.8 Ciało Galois rzędu p^n

Twierdzenie 11.19 sugeruje następujący problem. *Czy dla dowolnej liczby pierwszej p i liczby naturalnej n istnieje ciało Galois rzędu p^n?*
Odpowiedź na tak postawione pytanie jest pozytywna. Udowodnimy, że ciało rzędu p^n istnieje i jest, z dokładnością do izomorfizmu, jedyne.

Twierdzenie 11.22 *Dla dowolnej liczby pierwszej p oraz dla dowolnej liczby naturalnej n istnieje, jedyne z dokładnością do izomorfizmu, ciało rzędu p^n.*

Dowód. Wpierw udowodnimy istnienie ciała rzędu p^n, gdzie p jest dowolną liczbą pierwszą, $n \in \mathbb{N}$.
Niech E będzie ciałem rozkładu wielomianu

$$v = \mathbf{x}^{p^n} - \mathbf{x} \in \mathbb{Z}_p[\mathbf{x}] \tag{11.6}$$

Wykażemy, że $|E| = p^n$.
Wielomian v (dany wzorem (11.6)) ma w E co najwyżej p^n różnych między sobą pierwiastków. Co więcej, żeby wykazać, że v ma dokładnie p^n pierwiastków wystarczy udowodnić, że wszystkie pierwiastki v są w E jednokrotne.
Dla dowodu tego faktu metodą nie wprost przypuśćmy, że a jest pierwiastkiem (co najmniej) dwukrotnym v.
Wówczas a jest także pierwiastkiem v' (na mocy wniosku 11.21). Mamy więc

$$a^{p^n} = a \tag{11.7}$$

oraz

$$p^n a^{p^n-1} = 1 \tag{11.8}$$

Skoro

$$v = \mathbf{x}(\mathbf{x}^{p^n-1} - 1)$$

i wartość $\mathbf{x}^{p^n-1} - 1$ dla $x = 0$ jest różna od zera można założyć, że $a \neq 0$.
Z równań (11.7) i (11.8) wynika wtedy, że $p^n a^{p^n} = a^{p^n}$ i w konsekwencji $p = 1$, co jest sprzeczne z założeniem o p. Nie jest zbyt trudno udowodnić, że pierwiastki wielomianu v tworzą ciało (por. zadanie 11.20).
Ponieważ E jest ciałem rozkładu wielomianu v a więc najmniejszym ciałem zawierającym wszystkie jego pierwiastki. Z drugiej strony zbiór wszystkich pierwiastków v jest ciałem. Wobec tego E jest zbiorem wszystkich pierwiastków wielomianu v i mamy $|E| = p^n$.

Teraz wykażemy jedyność, z dokładnością do izomorfizmu, ciała rzędu p^n.
Niech K będzie ciałem rzędu p^n. Zbiór $K - \{0\}$ jest grupą multiplikatywną. Stąd, dla dowolnego $a \in K - \{0\}$ mamy $a^{|K|-1} = a^{p^n-1} = 1$. Tak więc każdy element ciała K jest pierwiastkiem wielomianu $\mathbf{x}^n - \mathbf{x}$. Skoro zaś, jak udowodniliśmy, zbiór tych pierwiastków ma p^n elementów, K jest ciałem rozkładu wielomianu $\mathbf{x}^{p^n} - \mathbf{x}$.[11] ■

[11] Pomijamy tu dowód faktu, że ciało rozkładu wielomianu jest, z dokładnością do izomorfizmu, jedyne.

Dla dowolnego ciała Galois $\mathrm{GF}(q)$ przez $\mathrm{GF}^*(q)$ oznaczmy zbiór elementów różnych od zera (elementu neutralnego dla dodawania w ciele $\mathrm{GF}(q)$). Oczywiście $\mathrm{GF}^*(q)$ z działaniem mnożenia jest grupą przemienną.

Twierdzenie 11.23 *Grupa $G\mathbb{F}^*(q)$ jest cykliczna.*

W dowodzie twierdzenia 11.23 wykorzystamy dwa lematy. Oto pierwszy z nich.

Lemat 11.24 *Niech G będzie grupą abelową, $f, g \in G$, $|f| = a, |g| = b$ (zakładamy, że rzędy elementów f i g są skończone). Wówczas istnieje element $h \in G$ taki, że $|h| = \mathrm{NWW}(a, b)$.*

Dowód lematu 11.24. Niech $p_1, ..., p_s$ będą różnymi między sobą liczbami pierwszymi i niech

$$a = p_1^{\alpha_1} \cdot ... \cdot p_s^{\alpha_s}$$

$$b = p_1^{\beta_1} \cdot ... \cdot p_s^{\beta_s}$$

Zdefiniujmy x_i, y_i wzorami

$$x_i = \begin{cases} \alpha_i & \text{jeśli} \quad \alpha_i \geq \beta_i \\ 0 & \text{jeśli} \quad \alpha_i < \beta_i \end{cases}$$

$$y_i = \begin{cases} \beta_i & \text{jeśli} \quad \beta_i > \alpha_i \\ 0 & \text{jeśli} \quad \beta_i \leq \alpha_i \end{cases}$$

Niech teraz

$$x = p_1^{x_1} \cdot ... \cdot p_s^{x_s}$$

$$y = p_1^{y_1} \cdot ... \cdot p_s^{y_s}$$

Oczywiście $x|a$ i $y|b$.
Przyjrzyjmy się jak powyższe wzory funkcjonują na prostym przykładzie: dla $a = 2^4 \cdot 3^3 \cdot 5^2, b = 2^3 \cdot 3^3 \cdot 5^3$ otrzymujemy $x = 2^4 \cdot 3^3$ i $y = 5^3$.

Mamy także $x \perp y$ bowiem jeśli jakaś liczba pierwsza p dzieli x, wówczas nie dzieli y (i na odwrót: jeśli p dzieli y, to nie dzieli x).
Udowodnimy teraz następujący fakt.

Fakt 11.25

$$|f| = x, |g| = y, x \perp y \Rightarrow |fg| = xy$$

Dowód faktu.

- $(fg)^{xy} = (f^x)^y (g^y)^x = 1^y \cdot 1^x = 1$

- Pozostaje wykazać, że dla dowolnego $z \in \mathbb{N}^+$ jeśli $(fg)^z = 1$ wówczas $xy|z$. Przypuśćmy więc, że $(fg)^z = 1$. Mamy wówczas

$$f^z = g^{-z} \tag{11.9}$$

Oznaczmy przez

$$A =< f >$$

$$B =< g >$$

A i B są podgrupami grupy G a więc $A \cap B$ jest podgrupą zarówno grupy A jak i grupy B i wobec tego rząd podgrupy $A \cap B$ dzieli $|A| = x$ i dzieli $|B| = y$. Skoro jednak $x \perp y$, mamy $|A \cap B| = 1$ i w konsekwencji jedynym elementem $A \cap B$ jest element neutralny.
Z (11.9) wynika, że

$$f^z \in A \cap B \text{ oraz } g^z \in A \cap B$$

a więc $f^z = 1$ i $g^z = 1$. Stąd zaś wynika, że $x|z$ i $y|z$ i wobec faktu, że $x \perp y$ otrzymujemy $xy|z$, co kończy dowód faktu 11.25.

□

Teraz możemy dokończyć dowód lematu 11.24.
Wykażemy, że $|f^{a/x}| = x$. Rzeczywiście $(f^{a/x})^x = f^a = 1$. Co więcej, jeśli $(f^{a/x})^z = 1$ to $z \geq x$ (w przeciwnym przypadku mielibyśmy $(f^{\frac{a}{x}})^z = 1$ a to nie jest możliwe bowiem przy założeniu, że $z < x$ mamy $a^{\frac{z}{x}} < a$.)
Identycznie wykazać można, że $|g^{b/y}| = y$.
Na mocy faktu 11.25 (i ponieważ $x \perp y$) otrzymujemy

$$|f^{a/x} g^{b/y}| = xy = \text{NWW}(a, b)$$

co kończy dowód lematu 11.24. □

Lemat 11.26 *Jeśli r jest największym rzędem elementu w grupie abelowej G, wówczas*

$$x^r = 1 \text{ dla dowolnego elementu } x \in G$$

Dowód lematu 11.26. Niech $g \in G$ będzie elementem rzędu r i niech $|f| = t$. Na mocy lematu 11.24 istnieje element $h \in G$ taki, że

$$|h| = \text{NWW}(r, t)$$

Z założenia o maksymalności r: $\text{NWW}(r, t) = r$. Stąd wynika, że $t|r$ i wobec tego $f^r = 1$, co kończy dowód lematu 11.26. □
Dowód twierdzenia 11.23. Niech r będzie największym rzędem elementu w $\text{G}\mathbb{F}^*(q)$. Na mocy lematu 11.26, każdy element grupy $\text{G}\mathbb{F}^*(q)$ jest pierwiastkiem wielomianu

$$\mathbf{x}^r - 1$$

Stąd wynika, że wielomian $\mathbf{x}^r - 1$ ma $q - 1 = |G\mathbb{F}^*(q)|$ pierwiastków i wobec tego

$$r \geq q - 1$$

Z drugiej strony jednak, na mocy wniosku z twierdzenia Lagrange'a[12], mamy

$$r|q - 1$$

A więc $r = q - 1$ co oznacza, że element, który ma największy rząd w grupie $G\mathbb{F}^*(q)$ generuje tę grupę. ■

Z twierdzenia 11.23 wynika, że ciało $G\mathbb{F}(p^n)$, gdzie p jest liczbą pierwszą, ma element prymitywny nad $\mathbb{Z}_p$, to znaczy, że istnieje w $G\mathbb{F}(p^n)$ element a taki, że $G\mathbb{F}(p^n) = \mathbb{Z}_p(a)$. Tym elemenem prymitywnym jest element $G\mathbb{F}^*(p^n)$, który w grupie $G\mathbb{F}^*(p^n)$ ma najwyższy rząd. Zapiszmy to jako wniosek.

Wniosek 11.27 *Jeśli p jest liczbą pierwszą, wówczas istnieje element $a \in G\mathbb{F}(p^n)$ taki, że $G\mathbb{F}(p^n) = \mathbb{Z}_p(a)$.* ■

Przykład 11.13 Konstrukcja ciała $G\mathbb{F}(8)$.
Wiemy (twierdzenie 11.19), że ciało rzędu 8 istnieje. Co więcej, dzięki wnioskowi 11.27 wiemy także, że ciało to, z dokładnością do izomorfizmu, jest jedyne i jest rozszerzeniem prostym $\mathbb{Z}_2(a)$, gdzie a jest pewnym jego elementem. Aby jednak znaleźć $G\mathbb{F}(8)$ wygodniej będzie się posłużyć twierdzeniem 11.10.
Znajdźmy wpierw wielomian nierozkładalny trzeciego stopnia $v \in \mathbb{Z}_2[\mathbf{x}]$.
Warto zapamiętać, że jeśli wielomian stopnia trzeciego (lub niższego) jest rozkładalny, wówczas jeden z jego czynników jest stopnia pierwszego i stąd wielomian taki musi mieć pierwiastek w ciele, nad którym jest rozkładalny. Wielomian

$$v = \mathbf{x}^3 + \mathbf{x} + 1$$

w $\mathbb{Z}_2$ nie ma pierwiastka ($v(0) = v(1) = 1$), stąd v jest nierozkładalny nad $\mathbb{Z}_2$. Elementami ciała $G\mathbb{F}(8)$ są więc:

$$(\mathbf{x}^3 + \mathbf{x} + 1), 1 + (\mathbf{x}^3 + \mathbf{x} + 1), \mathbf{x} + (\mathbf{x}^3 + \mathbf{x} + 1), \mathbf{x} + 1 + (\mathbf{x}^3 + \mathbf{x} + 1),$$

$$\mathbf{x}^2 + (\mathbf{x}^3 + \mathbf{x} + 1), \mathbf{x}^2 + 1 + (\mathbf{x}^3 + \mathbf{x} + 1), \mathbf{x}^2 + \mathbf{x} + (\mathbf{x}^3 + \mathbf{x} + 1), \mathbf{x}^2 + \mathbf{x} + 1 + (\mathbf{x}^3 + \mathbf{x} + 1)$$

Pomijając, jak to jest w zwyczaju, element zerowy, czyli $0 = (\mathbf{x}^3 + \mathbf{x} + 1)$, otrzymamy te same elementy w nieco wygodniejszej postaci:

$$0, 1, \mathbf{x}, \mathbf{x} + 1, \mathbf{x}^2, \mathbf{x}^2 + 1, \mathbf{x}^2 + \mathbf{x}, \mathbf{x}^2 + \mathbf{x} + 1$$

Pożytecznymi ćwiczeniami dla Czytelnika będzie wypisanie tabel dodawania i mnożenia dla elementów $G\mathbb{F}(8)$, znalezienie elementów odwrotnych mnożenia do elementów różnych od zera (bez posługiwania się tabelą mnożenia) oraz wskazanie generatora grupy $G\mathbb{F}(8)^*$. □

[12] Chodzi tu o wniosek 2.22, na mocy którego rząd dowolnego elementu grupy dzieli rząd grupy.

11.9 Rozszerzenia ciał izomorficznych

Twierdzenie 11.28 *Niech F i $\tilde{F}$ będą ciałami izomorficznymi, $\sigma : F \to \tilde{F}$ izomorfizmem ciał. Niech v $F[\mathbf{x}]$ będzie unormowanym wielomianem nierozkładalnym nad F, $a \in E$ pierwiastkiem v w E oraz $b \in \tilde{E}$ pierwiastkiem σv w $\tilde{E}$ (E i $\tilde{E}$ są rozszerzeniami, odpowiednio, F i $\tilde{F}$). Wówczas odwzorowanie*

$$\phi : F(a) \ni w(a) \to \sigma w(b) \in \tilde{F}(b)$$

jest jedynym izomorfizmem rozszerzenia $F(a)$ na $\tilde{F}(b)$, dla którego $\phi(a) = b$.

Nim przejdziemy do dowodu twierdzenia 11.28, wprowadzimy pojęcie homomorfizmu indukowany $\tilde{f} : F[\mathbf{x}] \to \tilde{F}[\mathbf{x}]$ przez homomorfizm $f : F \to \tilde{F}$ i udowodnimy twierdzenie pomocnicze, które wykorzystamy następnie w dowodzie twierdzenia 11.28.

Niech $f : F \to \tilde{F}$ będzie homomorfizmem ciał. Odwzorowanie

$$\tilde{f} : F[\mathbf{x}] \ni a_0 + a_1\mathbf{x} + ... + a_n\mathbf{x}^n \to f(a_0) + f(a_1)\mathbf{x} + ... + f(a_n)\mathbf{x}^n \in \tilde{F}[\mathbf{x}]$$

nazywamy homomorfizmem indukowanym $F[\mathbf{x}] \to \tilde{F}[\mathbf{x}]$ (oczywiście $\tilde{f}$ jest homomorfizmem pierścieni $F[\mathbf{x}] \to \tilde{F}[\mathbf{x}]$). Dla homomorfizmu f i wielomianu $v \in F[\mathbf{x}]$ będziemy oznaczali często przez fv wartość homomorfizmu $\tilde{f}$ na wielomianie v (zamiast przez $\tilde{f}(v)$). Nietrudno jest udowodnić, że jeśli f jest homomorfizmem, wówczas $\tilde{f}$ także jest homomorfizmem (pierścieni wielomianów). Co więcej,

- jeśli f jest epimorfizmem, wówczas $\tilde{f}$ jest epimorfizmem,

- jeśli f jest monomorfizmem wówczas $\tilde{f}$ także jest monomorfizmem.

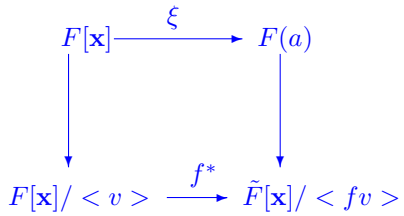
Stąd oczywiście wynika, że jeśli f jest izomorfizmem, wówczas $\tilde{f}$ jest izomorfizmem $F[\mathbf{x}] \to \tilde{F}[\mathbf{x}]$ (podkreślmy raz jeszcze, że f jest w powyższym opisie zawsze homomorfizmem ciał, podczas gdy $\tilde{f}$ jest homomorfizmem pierścieni).
Z poniższego twierdzenia będziemy korzystać w dowodzie twierdzenia 11.28 (prosty dowód twierdzenia pomijamy - por. zadanie 11.21).

Twierdzenie 11.29 *Niech F i $\tilde{F}$ będą ciałami izomorficznymi, $f : F \to \tilde{F}$ izomorfizmem i niech $v \in F[\mathbf{x}]$ będzie unormowanym wielomianem nierozkładalnym nad F. Wówczas fv jest wielomianem unormowanym i nierozkładalnym nad $\tilde{F}$.*
Odwzorowanie $f^* : F[\mathbf{x}]/ < v > \to \tilde{F}[\mathbf{x}]/ < fv >$ zdefiniowane wzorem

$$f^*(w + < v >) = fw + < fv >$$

jest izomorfizmem. ■

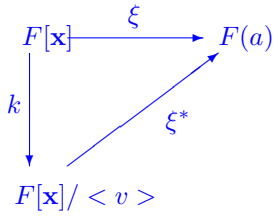
Sytuację opisaną w twierdzeniu 11.29 ilustruje następny diagram, na którym przez ξ oznaczono izomorfizm $\xi : F[\mathbf{x}] \ni w \to w(a) \in F(a)$.



Dowód twierdzenia 11.28.
Zdefiniujmy odwzorowanie

$$\xi : F[\mathbf{x}] \ni w \to w(a) \in F(a)$$

(a jest pierwiastkiem unormowanego i nierozkładalnego wielomianu v). Oczywiście ξ jest epimorfizmem i Ker $\xi =< v >$. Z twierdzenia o izomorfizmie pierścieni (por. diagram poniżej) $\xi^* : w+ < v > \to w(a)$ jest izomorfizmem pierścieni.



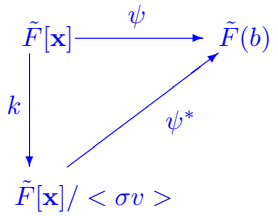
Na mocy twierdzenia 11.29, skoro $\sigma : F \to \tilde{F}$ jest izomorfizmem,

$$\tilde{\sigma} : F[\mathbf{x}]/ < v > \ni w+ < v > \to \sigma w+ < \sigma v > \in \tilde{F}[\mathbf{x}]/ < \sigma v >$$

także jest izomorfizmem.
Korzystając z kolei z twierdzenia o izomorfizmie pierścieni dla

$$\psi : \tilde{F}[\mathbf{x}] \ni w \to w(b) \in \tilde{F}(b)$$

otrzymujemy izomorfizm $\psi^* : \tilde{F}[\mathbf{x}]/ < \sigma v > \to \tilde{F}(b)$.



$F(a)$ i $F(b)$ są więc izomorficzne, jak to ilustruje poniższy schemat, przy czym $(\xi^*)^{-1}$, $\tilde{\sigma}$ i ψ^* są izomorfizmami a ich złożenie także jest izomorfizmem.

$$\begin{array}{ccccccc} F(a) & \overset{(\xi^*)^{-1}}{\to} & F[\mathbf{x}]/ < v > & \overset{\tilde{\sigma}}{\to} & \tilde{F}[\mathbf{x}]/ < \sigma v > & \overset{\psi^*}{\to} & \tilde{F}(b) \\ w(a) & \to & w+ < v > & \to & \sigma w+ < \sigma v > & \to & \sigma w(b) \end{array}$$

Dla $w = \mathbf{x}$ otrzymamy

$$a \quad \rightarrow \quad \mathbf{x}+ < v > \quad \rightarrow \quad \mathbf{x}+ < \sigma v > \quad \rightarrow \quad b$$

a dla $c \in F$

$$c \quad \rightarrow \quad c+ < v > \quad \rightarrow \quad \sigma(c)+ < \sigma v > \quad \rightarrow \quad \sigma(c)$$

Tak więc $\phi = \psi^* \circ \tilde{\sigma} \circ (\psi^*)^{-1}$ jest rozszerzeniem σ na $F(a) \rightarrow \tilde{F}(b)$ takim, że $\phi(a) = b$. Pozostaje wykazanie, że istnieje jedyne rozszerzenie ϕ odwzorowania σ spełniające ten warunek.
Przypuśćmy, że $\gamma : F(a) \rightarrow \tilde{F}(b)$ jest odwzorowaniem takim, że

$\phi(c) = \gamma(c)$ dla każdego $c \in F$ oraz

$\phi(a) = \gamma(a) = b$.

Wykażemy, że $\gamma(s) = \phi(s)$ dla każdego $s \in F(a)$.
Dla $s \in F(a)$ mamy $s = \alpha_0 + \alpha_1 a + ... + \alpha_{n-1} a^{n-1}$, gdzie $\alpha_0, ..., \alpha_{n-1} \in F$ i n jest stopniem elementu a (czyli stopniem jego wielomianu minimalnego). Wtedy

$$\begin{aligned} \gamma(s) &= \gamma(\alpha_0 + \alpha_1 a + ... + \alpha_{n-1} a^{n-1}) \\ &= \gamma(\alpha_0) + \gamma(\alpha_1)\gamma(a) + ... + \gamma(\alpha_{n-1})(\gamma(a))^{n-1} \\ &= \alpha_0 + \alpha)1b + ... + \alpha_{n-1} b^{n-1} \\ &= \phi(\alpha_0) + ... + \phi(\alpha_{n-1}(\phi(a))^{n-1} \\ &= \phi(c) \end{aligned}$$

■

11.10 Zadania

Zadanie 11.1 Niech L będzie rozszerzeniem ciała K, $X \subset L$. Udowodnij, że

- $K(X) = \bigcup_{M:K,X\subset M} M$ (rozszerzenie ciała K o zbiór X jest równe przecięciu wszystkich ciał zawartych w L i zawierających zbiór X i ciało K) (por. str. 148).
- $K(X)$ jest równe zbiorowi elementów które można otrzymać w skończonym ciągu operacji w ciele L na elementach zbioru X i ciała K (por. str. 148).

Zadanie 11.2 Ułóż tabelkę działań dla $\mathbb{Z}_2[\mathbf{x}]/(\mathbf{x}^2+1)$, $\mathbb{Z}_5[\mathbf{x}]/(\mathbf{x}^2+\mathbf{x}+3)$.

Zadanie 11.3 Sprawdź, że $\mathbf{Q}(i,-i,\sqrt{3},-\sqrt{3})$ jest rozszerzeniem prostym.

Zadanie 11.4 Dla jakich wartości $a \in \mathbb{Z}_3$ pierścień ilorazowy $\mathbb{Z}_3[\mathbf{x}]/(\mathbf{x}^2+a)$ jest ciałem?

Zadanie 11.5 Udowodnij, że wielomian $\mathbf{x}^4 - 10\mathbf{x}^2 + 22$ jest nierozkładalny nad $\mathbb{Q}$.

Zadanie 11.6 Wykaż, że jeśli $a, b \in E : \mathbb{Z}_p$, gdzie p jest liczbą pierwszą, wówczas

$$(a+b)^p = a^p + b^p$$

$$(a-b)^p = a^p - b^p$$

Zadanie 11.7 W ciele $\mathbb{Q}[\mathbf{x}]/(\mathbf{x}^2+\mathbf{x}+1)$ znajdź następujące elementy:

$$a) \quad (\mathbf{x}+2)^2(\mathbf{x}-1)^3 \quad b) \quad \tfrac{\mathbf{x}^2+1}{\mathbf{x}-2} \quad c) \quad \mathbf{x}^2+1$$

Zadanie 11.8 Wykaż, że nad $\mathbb{Z}_3$ wielomian $\mathbf{x}^3+2\mathbf{x}+1$ jest nierozkładalny.
W ciele $\mathbb{Z}_3[\mathbf{x}]/(\mathbf{x}^3+2\mathbf{x}+1)$ znajdź element $\frac{\mathbf{x}^2+\mathbf{x}+1}{\mathbf{x}^2+1}$.

Zadanie 11.9 Dla liczby
a) $\sqrt{3}+1$ b) $\sqrt[6]{3}$ c) $\sqrt[4]{2}-2\sqrt{2}$
znajdź wielomian minimalny v (nad $\mathbb{Q}$).

Zadanie 11.10 Niech a będzie pierwiastkiem wielomainu
a) $v = \mathbf{x}^2+1 \in \mathbb{Z}_3[\mathbf{x}]$ b) $w = \mathbf{x}^3+\mathbf{x}+4 \in \mathbb{Z}_5[\mathbf{x}]$
Znajdź ciało $F(a)$ (dla $F=\mathbb{Z}_3$ i $F=\mathbb{Z}_5$, odpowiednio).

Zadanie 11.11 Znajdź ciała: GF(5), GF(4), GF(9), GF(25).

Zadanie 11.12 Uzasadnij, że wielomian $v = \mathbf{x}^3-2$ jest nierozkładalny nad Q (jasne, że było).
Znajdź ciało E rozkładu v oraz ciała $\mathbb{Q}(a_i)$ dla pierwiastków a_1, a_2, a_3 wielomianu v.
Zilustruj na przykładzie ciał $\mathbb{Q}$, $\mathbb{Q}(a_i)$ oraz E twierdzenie o (niskiej) wieży.

Zadanie 11.13 Dla podanego ciała F zbadaj, czy element a jest algebraiczny czy przestępny? (Zakładamy, że wiemy, że π jest liczbą przestępną.)

a)	$F=\mathbb{Q}$	$a=\sqrt[3]{\pi^2}$	*b)*	$F=\mathbb{Q}(\pi)$	$a=\sqrt[3]{\pi^2}$
c)	$F=\mathbb{C}$	$a=i\sqrt[3]{\pi^2}$	*d)*	$F=\mathbb{C}(\pi)$	$a=i\sqrt[3]{\pi^2}$
e)	$F=\mathbb{Q}$	$a=2+\sqrt{\pi}$	*f)*	$F=\mathbb{Q}(\pi)$	$a=2+\sqrt{\pi}$
g)	$F=\mathbb{Q}$	$a=\pi^3$	*h)*	$F=\mathbb{Q}(\pi)$	$a=\pi^3$
i)	$F=\mathbb{Q}(\pi)$	$a=\sqrt[3]{\pi}$			

Zadanie 11.14 Znajdź wymiar $[E:F]$ i bazę rozszerzenia jeśli

a)	$F=\mathbb{Q}$	$E=\mathbb{Q}(\sqrt{5},\sqrt[3]{2})$	*b)*	$F=\mathbb{Q}(\sqrt{5})$	$E=\mathbb{Q}(\sqrt{5},\sqrt{2})$
c)	$F=\mathbb{Q}$	$E=\mathbb{Q}(\sqrt{2},i)$	*d)*	$F=\mathbb{Q}(i)$	$E=\mathbb{Q}(\sqrt{5},i)$
d)	$F=\mathbb{Q}$	$E=\mathbb{Q}(\sqrt{2})$	*e)*	$F=\mathbb{Q}$	$E=\mathbb{Q}(\sqrt{2},e^{2\pi i/3})$

Zadanie 11.15 Udowodnij, że jeśli $[F(a):F]=m$ i $F((b):F]=n$ wówczas

$$[F(a,b):F]\leq mn \tag{11.10}$$

Wskaż przykłady, w których (11.10) jest równością i takie, w których nierówność (11.10) jest ostra.

Zadanie 11.16 Udowodnij, że $\sqrt{3}\notin\mathbb{Q}(\pi)$.
Rozumowanie, którym się posłużysz uogólnij, by wykazać, że jeśli b jest elementem przestępnym ciała F, to żaden element algebraiczny F nie należy do $F(b)-F$.

Zadanie 11.17 Udowodnij, że π jest elementem algebraicznym ciała $\mathbb{Q}(\pi^3)$. Znajdź bazę i wymiar rozszerzenia $\mathbb{Q}(\pi)$ nad $\mathbb{Q}(\pi^3)$.

Zadanie 11.18 Wskaż ciała rzędów 125 i 121.

Zadanie 11.19 Udowodnij związki (11.3), (11.4) i (11.5).

Zadanie 11.20 Niech p będzie liczbą pierwszą. Udowodnij, że zbiór pierwiastków wielomianu $\mathbf{x}^{p^n}-\mathbf{x}\in\mathbb{Z}[\mathbf{x}]$ jest ciałem (wykorzystaj wzory wykazane w zadaniu 11.6).

Zadanie 11.21 Udowodnij twierdzenie 11.29.

Zadanie 11.22 Wskaż generator grupy G.

$$a)\quad \big(\mathbb{Z}_2[\mathbf{x}]/(\mathbf{x}^2+\mathbf{x}+1)\big)^* \qquad b)\quad \big(\mathbb{Z}_3[\mathbf{x}]/(\mathbf{x}^2+\mathbf{x}+2)\big)^*$$

Rozdział 12

Teoria Galois

12.1 Grupy Galois

Niech $E : F$ będzie rozszerzeniem ciała F. Zbiór wszystkich automorfizmów f (a więc izomorfizmów ciała E na ciało E) takich, że $f(a) = a$ dla każdego elementu $a \in F$ jest, jak łatwo wykazać, grupą (p. zadanie 12.2). Grupę tę oznaczamy przez $\mathrm{Gal}(E : F)$ i nazywamy **grupą Galois rozszerzenia** $E : F$.
O automorfizmach grupy Galois rozszerzenia $E : F$ mówimy, że **ustalają ciało** F.

Przykład 12.1 Jeśli $f \in \mathrm{Gal}(\mathbb{C} : \mathbb{R})$ wówczas $f(a+ib) = f(a)+f(i)f(b) = a+if(b)$, gdzie $a, b \in \mathbb{R}$.
Mamy także $-1 = f(-1) = f(i^2) = (f(i))^2$ i stąd $f(i) = i$ lub $f(i) = -i$. Wobec tego $\mathrm{Gal}(\mathbb{C} : \mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \alpha\}$, gdzie $\alpha(z) = \bar{z}$ dla każdego $z \in \mathbb{C}$.

Oczywiście dla dowolnej grupy Galois $\mathrm{Gal}(E : F)$ mamy $\mathrm{id}_E \in \mathrm{Gal}(E : F)$.

Przykład 12.2 Dla każdego automorfizmu $f \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = \{a+b\sqrt{2} | a, b \in \mathbb{Q}\}$ mamy

$$f(a + b\sqrt{2}) = f(a) + f(b)f(\sqrt{2}) = a + bf(\sqrt{2})$$

Wartości f na dowolnym elemencie $\mathbb{Q}(\sqrt{2})$ są więc zdeterminowane przez wartość f na $\sqrt{2}$.

$$2 = f(2) = f((\sqrt{2})^2) = (f(\sqrt{2}))^2$$

Stąd $f(\sqrt{2}) = \sqrt{2}$ lub $f(\sqrt{2}) = -\sqrt{2}$. Istnieją więc tylko dwa automorfizmy w grupie $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$: identyczność $\mathrm{id}_{\mathbb{R}}$ i $f(a + b\sqrt{2}) = a - b\sqrt{2}$.

Przykład 12.3 Łatwo się przekonać, że aby znaleźć grupę Galois rozszerzenia $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ wystarczy znaleźć wartości jakie automorfizm $f \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ może przyjmąć na $\sqrt[3]{2}$. Mamy tym razem

$$2 = f((\sqrt[3]{2})^3) = (f(\sqrt[3]{2}))^3$$

a więc istnieje tylko jedna możliwość, mianowicie $f(\sqrt[3]{2}) = \sqrt[3]{2}$ i jedynym elementem $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})$ jest $\mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}$.

12.2 Grupa Galois rozszerzenia prostego

Niech $\sigma : F \to \bar{F}$ będzie homomorfizmem ciał i niech $v = a_0 + a_1\mathbf{x} + ... + a_n\mathbf{x}^n \in F[\mathbf{x}]$ będzie wielomianem o współczynnikach w ciele F. Wówczas przez σv będziemy oznaczali wielomian $\sigma(a_0)+\sigma(a_1)\mathbf{x}+...+\sigma(a_n)\mathbf{x}^n$. Łatwo sprawdzić, że odwzorowanie $F[\mathbf{x}] \ni v \to \sigma v \in \bar{F}[\mathbf{x}]$ jest homomorfizmem pierścieni (por zadanie 12.3).

Twierdzenie 12.1 *Niech E i F będą ciałami, $E : F$, $a \in E$, $G = Gal(E : F)$.*

(i) Jeśli $f \in G$ wówczas $fv(a) = v(f(a))$, dla każdego wielomianu $v \in F[\mathbf{x}]$.

(ii) Jeśli a jest elementem algebraicznym nad F, $f, g \in Gal(F(a) : F)$, wówczas

$$f = g \text{ wtedy i tylko wtedy gdy } f(a) = g(a)$$

Dowód.

(i) Dowód pierwszej części twierdzenia wynika natychmiast z faktu, że $f \in \mathrm{Gal}(E : F)$ i definicji rozszerzenia homomorfizmu f na pierścień $F[\mathbf{x}]$.

(ii) Jeśli $f = g$ wówczas oczywiście $f(a) = g(a)$ dla każdego elementu $a \in E$.
Niech teraz $f, g \in \mathrm{Gal}(E : F)$ i przypuśćmy, że

$$f(a) = g(a)$$

Wykażemy, że $f = g$.
Na mocy twierdzenia 11.10, dla dowolnego $b \in E$

$$b = \beta_0 + \beta_1 a + ... + \beta_{n-1}a^{n-1}$$

gdzie $n = \deg_E(a)$ i $\beta_0, ..., \beta_{n-1} \in F$. Wtedy

$$\begin{aligned} f(b) &= f(\beta_0 + \beta_1 a + ... + \beta_{n-1}a^{n-1} \\ &= f(\beta_0) + f(\beta_1)f(a) + ... + f(\beta_{n-1})(f(a))^{n-1} \\ &= \beta_0 + \beta_1 f(a) + ... + \beta_{n-1}(f(a))^{n-1} \\ &= \beta_0 + \beta_1 g(a) + ... + \beta_{n-1}(g(a))^{n-1} \\ &= g(b) \end{aligned}$$

Wykazaliśmy więc, że jeśli $f(a) = g(a)$ $(f, g \in \mathrm{Gal}(F(a) : F))$ to $f = g$, co kończy dowód twierdzenia. ■

Na mocy części (i) twierdzenia 12.1 $v(f(a)) = f(v(a))$ dla dowolnego wielomianu $v \in F[\mathbf{x}]$ i $f \in \mathrm{Gal}(E : F)$. Jeśli więc a jest pierwiastkiem wielomianu v, wówczas mamy

$$v(f(a) = f(v(a)) = f(0) = 0$$

(pamiętamy, że f jest homomorfizmem, a więc $f(0) = 0$). Stąd wynika następujący wniosek.

Wniosek 12.2 *Jeśli $E : F$ jest rozszerzeniem, $f \in Gal(E : F)$, $a \in E$ i a jest pierwiastkiem $v \in F[\mathbf{x}]$ wówczas $f(a)$ jest także pierwiastkiem wielomianu v.* □

Przypuśćmy, że $a \in E$ jest elementem algebraicznym nad ciałem F (oczywiście zakładamy, że $E : F$). Niech v będzie wielomianem minimalnym elementu a nad F i powiedzmy, że zbiór $\{a = a_1, a_2, ..., a_n\}$ jest zbiorem wszystkich, różnych między sobą, pierwiastków wielomianu v (por. zadanie 12.4).

1. Na mocy części (ii) twierdzenia 12.1 każdy automorfizm $f \in \mathrm{Gal}(F(a) : F)$ jest jednoznacznie wyznaczony przez swoją wartość na elemencie a.

2. Z wniosku 12.2 wynika, że $f(a) \in \{a = a_1, a_2, ..., a_n\}$

Na mocy twierdzenia o rozszerzeniu prostym o element algebraiczny (twierdzenie 11.10) stopień elementu a ($\deg(a)$) i wymiar $F(a)$ nad F (oznaczany przez nas przez $[F(a) : F]$) są sobie równe. Jeśli więc nad ciałem $F(a)$ wielomian minimalny v rozkłada się na czynniki liniowe i pierwiastki v są jednokrotne, to liczba elementów w $\mathrm{Gal}(F(a) : F)$ jest równa stopniowi wielomianu minimalnego.

Podsumujmy te rozważania w postaci twierdzenia.

Twierdzenie 12.3 *Jeśli a jest elementem algebraicznym nad ciałem F, v wielomianem minimalnym a, $a = a_1, a_2, ..., a_n$ są wszystkimi, różnymi między sobą pierwiastkami v w $F(a)$. Wówczas*

$$Gal(F(a) : F) = \{id_{F(a)}, f_2, ..., f_n\}$$

gdzie f_i dla $i = 2, ..., n$, jest automorfizmem $F(a) \to F(a)$ takim, że

$f_i(b) = b$ *dla każdego* $b \in F$

$f_i(a) = a_i$.

Jeśli m rozkłada się w $F(a)$ na iloczyn czynników liniowych, wówczas

$$|Gal(F(a) : F)| = [F(a) : F]$$

□

Twierdzenie 12.4 *Niech p będzie dowolną liczbą pierwszą i niech E będzie pewnym ciałem rzędu p^n ($n \in \mathbb{N}$). Wówczas istnieje taki element $a \in E$, że $E \simeq \mathbb{Z}_p(a)$ (inaczej: a jest generatorem E nad $\mathbb{Z}_p$ (dokładniej: nad ciałem izomorficznym z $\mathbb{Z}_p$)).*

Przykład 12.4 Niech p będzie liczbą pierwszą. Wykażemy, że grupa Galois $\mathrm{Gal}(\mathrm{G}\mathbb{F}(p^n) : \mathbb{Z}_p)$ jest n-elementową grupą cykliczną.
Wiemy, że $\mathrm{G}\mathbb{F}(p^n) = \mathbb{Z}_p(a)$ dla pewnego elementu $a \in E = \mathrm{G}\mathbb{F}(p^n)$ i a jest pierwiastkiem wielomianu minimalnego, który musi być stopnia n. Stąd i z twierdzenia 12.3 wynika, że

$$|\mathrm{Gal}(E : \mathbb{Z}_p)| \leq n$$

Wystarczy więc wskazać n różnych automorfizmów E ustalających $\mathbb{Z}_p$.
Niech $f : E \to E$ będzie automorfizmem Frobeniusa (por. zadanie 12.8).
Można z łatwością sprawdzić (na przykład indukcyjnie, ze względu na k), że dla $k \geq 1$ zachodzi wzór

$$f^k(s) = s^{p^k}$$

Jeśli $f^k = \mathrm{id}_E$ dla pewnego k, to dla dowolnego $s \in E$ mamy $f^k(s) = \mathrm{id}_E(s)$ a więc

$$s^{p^k} = s$$

czyli $s \in E$ jest pierwiastkiem wielomianu

$$\mathbf{x}^{p^k} - \mathbf{x}$$

Mamy więc $k \geq n$ - jeśli istnieje p^n pierwiastków pewnego wielomianu to jego stopień musi wynosić co najmniej p^n. Automorfizmami E ustalającymi $\mathbb{Z}_p$ są więc $f^0 = \mathrm{id}_E, f, ..., f^{n-1}$. □

Kolejne twierdzenie nazwiemy **twierdzeniem o rozszerzeniach skończonych**.

Twierdzenie 12.5 *Rozszerzenie $E : F$ jest skończone wtedy i tylko wtedy, gdy $E = F(a_1, ..., a_n)$, gdzie $a_1, ..., a_n$ są pewnymi elementami algebraicznymi nad F.*

Dowód.

1. Udowodnimy wpierw, że jeśli rozszerzenie $E : F$ jest skończone, wówczas istnieją elementy algebraiczne $a_1, ..., a_n \in E$ takie, że $E = F(a_1, ..., a_n)$. Dowód przeprowadzimy przez indukcją ze względu na wymiar rozszerzenia $[E : F]$.

   - Jeśli $[E : F] = 1$ to $E = F = F(1)$. Element 1 jest oczywiście algebraiczny nad F.
   - Przypuśćmy więc, że $[E : F] > 1$ i twierdzenie jest prawdziwe dla wszystkich rozszerzeń wymiaru mniejszego niż $[E : F]$.
     Skoro $[E : F] > 1$, istnieje element $a \in E - F$. Na mocy twierdzenia 11.13 (twierdzenie o wieży):

     $$[E : F(a)] = [E : F]/[F(a) : F] < [E : F]$$

     Rozszerzenie $E : F(a)$ jest skończone i z założenia indukcyjnego

     $$E = F(a)(a_1, ..., a_n)$$

     Na mocy twierdzenia 11.8

     $$F(a)(a_1, ..., a_n) = F(a, a_1, ..., a_n)$$

     Rozszerzenie $F(a, a_1, ..., a_n) : F$ jako skończone jest algebraiczne a więc elementy $a, a_1, ..., a_n$ są algebraiczne.

2. Przypuśćmy teraz, że $E = F(a_1, ..., a_n)$, gdzie $a_1, ..., a_n$ są elementami algebraicznymi nad F. Wykażemy, że rozszerzenie $E : F$ jest skończone. Także tym razem dowód przeprowadzimy metodą indukcji
Jeśli $n = 1$ wówczas, $E = F(a)$ gdzie a jest elementem algebraicznym i E jest na mocy twierdzenia 11.10 rozszerzeniem skończonym.
Przypuśćmy więc, że $n > 1$ i dla każdego $k < n$ rozszerzenie F o k elementów algebraicznych jest algebraiczne. Oznaczmy przez $K = F(a_1, ..., a_{n-1})$. Na mocy założenia indukcyjnego, $K : F$ jest rozszerzeniem skończonym. Także $E = K(a_n)$ jest rozszerzeniem skończonym nad K, bowiem element a_n algebraiczny nad F jest także algebraiczny nad F. Ponownie korzystamy z twierdzenia 11.13 o wieży
$$[E : F] = [E : K][K : F]$$
Ta ostatnia równość kończy dowód twierdzenia 12.5. ■

Możemy teraz sformułować twierdzenie, które nazwiemy **twierdzeniem o grupie Galois rozszerzenia skończonego**.

Twierdzenie 12.6 *Jeśli $E = F(a_1, ..., a_n)$ jest rozszerzeniem skończonym ciała F, gdzie $a_1, ..., a_n$ są elementami algebraicznymi nad F, dla każdego $i = 1, ..., n$, m_i jest wielomianem minimalnym a_i nad F, $f \in Gal(E : F)$, wówczas*

(i) automorfizm f jest jednoznacznie wyznaczony przez wartości na elementach $a_1, ..., a_n$.

(ii) $f(a_i)$ jest pierwiastkiem wielomianu m_i (dla $i = 1, ..., n$).

Z twierdzenia 12.6 wynika łatwo następujący wniosek.

Wniosek 12.7 *Jeśli $E : F$ jest rozszerzeniem skończonym, $E = F(a_1, ..., a_n)$, gdzie $a_1, ..., a_n$ są elementami algebraicznymi nad F, wówczas grupa $Gal(E : F)$ jest skończona.* ■

Dowód twierdzenia 12.6.

(i) Mamy wykazać następującą implikację
$$f, g \in \mathrm{Gal}(E : F) \wedge f(a_i) = g(a_i) \text{ (dla } i = 1, ..., n) \Rightarrow f = g \qquad (12.1)$$
Dowód przeprowadzimy metodą indukcji matematycznej ze względu na n.
Dla $n = 1$ jest to znany nam już fakt dla rozszerzeń prostych (twierdzenie 12.1).
Przypuśćmy, że $n > 1$ i że automorfizmy $\mathrm{Gal}(F(a_1, ..., a_{n-1}) : F)$ są jednoznacznie wyznaczane przez swoje wartości na elementach $a_1, ..., a_{n-1}$[1]. Implikację

[1] Założenie indukcyjne rozumiemy tu tak: *jeżeli K i L są ciałami takimi, że $L = K(b_1, ..., b_{n-1})$ jest rozszerzeniem skończonym ciała K i $b_1, ..., b_{n-1}$ są elementami algebraicznymi nad K, wówczas każdy automorfizm $h \in Gal(L : K)$ jest jednoznacznie wyznaczony przez swoje wartości na elementach $b_1, ..., b_{n-1}$.* Zauważmy, że skoro w twierdzeniu 12.6 zakładamy, że rozszerzenie jest $E : F$ skończone, elementy $a_1, ..., a_n \in E$ są algebraiczne nad F. Założenie tego faktu w twierdzeniu można więc pominąć.

(12.1) możemy zapisać następująco:

$$f^{-1}g(a_i) = a_i \text{ (dla } i = 1, ..., n) \Rightarrow f = g$$

Mamy

$$F(a_1, ..., a_n) = ((F(a_1))(a_2, ..., a_n)) : F(a_1)$$

Skoro $f^{-1}g$ ustala a_1 oraz F (tak jest, bowiem f i g ustalają F), to ustala także $F(a_1)$. A więc $f^{-1}g \in \text{Gal}(F(a_1)(a_2, ..., a_n) : F(a_1))$. Ponieważ

$$f^{-1}g(a_i) = a_i \quad \text{dla } i = 2, ..., n$$

i na mocy założenia indukcyjnego, $f^{-1}g = \text{id}_{F(a_2,...,a_n)}$. Na dodatek, $f^{-1}g$ ustala $F(a_1)$, a więc $f^{-1}g = \text{id}_{F(a_1,...,a_n)}$ co oznacza, że $f = g$.

(ii) Dla dowolnego $f \in \text{Gal}(E : F)$ i dla a_i $(i = 1, ..., a_n$ policzmy wartość wielomianu minimalnego m_i na $f(a_i)$:

$$m_i(f(a_i)) = f(m_i(a_i)) = f(0) = 0$$

(pamiętamy, że f jest automorfizmem ciała E, więc $f(0) = 0$).

$f(a_i)$ jest więc pierwiastkiem wielomianu m_i. ■

Przykład 12.5 Grupa Galois ciała rozkładu wielomianu $\mathbf{x}^3 - 2$ nad $\mathbb{Q}$
Oznaczmy przez $a = \sqrt[3]{2}$, $b = e^{2\pi i/3}$.
Pierwiastkami $v = \mathbf{x}^3 - 2$ są a, ab oraz ab^2. Ciałem rozkładu wielomianu v jest $\mathbb{Q}(a, ab, ab^2) = \mathbb{Q}(a, b)$.
Wielomianem minimalnym a jest

$$m_1 = \mathbf{x}^3 - 2$$

zaś wielomianem minimalnym b jest

$$m_2 = x^2 + \mathbf{x} + 1$$

Pierwiastkami m_1 są a, ab i ab^2, pierwiastkami m_2 są b i b^2. Łatwo sprawdzić, że

$$\mathbb{Q}(a, ab, ab^2) = \mathbb{Q}(a, b)$$

Automorfizm $g \in \text{Gal}(\mathbb{Q}(a, b) : \mathbb{Q})$ może, zgodnie z twierdzeniem 12.6 przyjmować

- wartości a, ab lub ab^2 na elemencie a

- wartości b lub b^2 na elemencie b.

Stąd grupa $\mathrm{Gal}(\mathbb{Q}(a,b):\mathbb{Q})$ ma 6 elementów:

$e=\mathrm{id}_{\mathbb{Q}(a,b)}$	f	g	h	k	l
$a\to a$	$a\to a$	$a\to ab$	$a\to ab$	$a\to ab^2$	$a\to ab^2$
$b\to b$	$b\to b^2$	$b\to b$	$b\to b^2$	$b\to b$	$b\to b^2$

Zauważmy, że $fh(a)=f(ab)=f(a)f(b)=ab^2$ i $hf(a)=h(a)=ab$, grupa $\mathrm{Gal}(\mathbb{Q}(a,b):\mathbb{Q})$ jest więc nieprzemienna. Wiemy, że istnieją dokładnie dwie grupy 6-elementowe: $\mathbb{Z}_6$, która jest przemienna i S_3 -grupa permutacji zbioru 3-elementowego[2]. Stąd wniosek, że $\mathrm{Gal}(\mathbb{Q}(a,b):\mathbb{Q})\cong S_3$. □

W następnym twierdzeniu (twierdzenie 12.10) opisana jest grupa Galois ciała rozkładu wielomianu. W dowodzie tego twierdzenia wykorzystamy następujący lemat, który nazwiemy *lematem o przedłużaniu izomorfizmów na ciała rozkładu.*

Twierdzenie 12.8 *Niech F będzie ciałem, $v\in F[\mathbf{x}]$ wielomianem nierozkładalnym nad F. Niech $\tilde{F}$ będzie ciałem izomorficznym z F i niech $\sigma:F\to\tilde{F}$ będzie izomorfizmem F na $\tilde{F}$.*
Jeżeli E jest ciałem rozkładu v a $\tilde{E}$ ciałem rozkładu σv, wówczas istnieje izomorfizm $\phi:E\to\tilde{E}$ taki, że $\phi_{|F}=\sigma$ (ϕ jest przedłużeniem σ na E).

W dowodzie twierdzenia 12.8 wykorzystamy następujący lemat o przedłużeniach izomorfizmów na rozszerzenia proste o element algebraiczny.

Lemat 12.9 *Niech $\sigma:F\to\tilde{F}$ będzie izomorfizmem ciał, niech $a\in E:F$ będzie elementem algebraicznym nad F zaś $v\in F[\mathbf{x}]$ wielomianem minimalnym elementu a i niech $b\in\tilde{E}:\tilde{F}$ będzie pierwiastkiem wielomianu $\sigma v\in\tilde{F}$.*
Wówczas istnieje przedłużenie $\phi:F(a)\to\tilde{F}(b)$ takie, że $\phi(a)=b$.

Dowód lematu 12.9. Każdy element c ciała $F(a)$ jest postaci

$$c=\alpha_0+\alpha_1 a+\ldots+\alpha_{n-1}a^{n-1} \tag{12.2}$$

Co więcej, przedstawienie elementu $c\in F(a)$ (12.2) jest jednoznaczne (twierdzenie 11.10). Wielomian σv jest w $\tilde{F}[\mathbf{x}]$ wielomianem unormowanym i nierozkładalnym, a więc minimalnym elementu b, $\partial\sigma v=n$. Stąd każdy element $d\in\tilde{F}$ można jednoznacznie zapisać w postaci

$$d=\beta_0+\beta b+\ldots+\beta_{n-1}b^{n-1}$$

Odwzorowanie $\phi:F(a)\to\tilde{F}(b)$ zdefiniowane wzorem

$$\phi(\alpha_0+\alpha_1 a+\ldots+\alpha_{n-1}a^{n-1})=\sigma(\alpha_0)+\sigma(\alpha_1)b+\ldots+\sigma(\alpha_{n-1}b^{n-1}$$

jest, jak nietrudno udowodnić, izomorfizmem $F(a)\to\tilde{F}(b)$ spełniającym warunki $\phi(\alpha)=\alpha$ dla wszystkich $\alpha\in F$ i $\phi(a)=b$. ■

[2]Łatwo sprawdzić, że grupa S_3 jest izomorficzna z grupą dihedralną D_3.

Dowód twierdzenia 12.8 przez indukcję ze względu na $n = \partial v$.
Jeżeli $n = 1$, wówczas $E = F, \tilde{E} = \tilde{F}$ i szukanym przedłużeniem σ jest σ.
Przypuśćmy więc, że $n > 1$. Niech $a \in E$ będzie pierwiastkiem v i niech $u \in F[\mathbf{x}]$ będzie wielomianem minimalnym elementu a (wiemy, że u jest wielomianem unormowanym i $u|v$). Niech $b \in \tilde{E}$ będzie pierwiastkiem σu. Z lematu 12.9 11.28 wynika istnienie izomorfizm $\tau : F(a) \to \tilde{F}(b)$ takiego, że $\tau(a) = b$ i $\tau(\alpha) = \sigma(\alpha)$ dla każdego $\alpha \in F$.
E i $\tilde{E}$ są ciałami rozkładów, odpowiednio, v i σv, stąd możemy napisać

$$v = (\mathbf{x} - a)w$$

gdzie $w \in F(s)[\mathbf{x}]$ a wobec tego

$$\sigma v = (\mathbf{x} - t)\sigma w$$

i $\sigma w \in \tilde{F}(t)[\mathbf{x}]$.
Nietrudno zauważyć, że E jest ciałem rozkładu wielomianu $w = v/(\mathbf{x} - s)$ nad $F(s)$ i $\tilde{E}$ jest ciałem rozkładu σw nad $\tilde{F}(t)$.
Skoro $\partial w = \partial(\sigma w) = \partial v - 1$, na mocy założenia indukcyjnego izomorfizm $\tau : F(s) \to \tilde{F}(t)$ można przedłużyć do izomorfizmu $\phi : E \to \tilde{E}$, co kończy dowód lematu. ■

Twierdzenie 12.10 *Niech $E : F$ będzie ciałem rozkładu wielomianu $v \in F[\mathbf{x}]$. Przez X oznaczmy zbiór wszystkich pierwiastków wielomianu v w E. Wówczas*

(i) Grupa $G = Gal(E : F)$ jest izomorficzna z pewną podgrupą S_X (grupy wszystkich permutacji zbioru X).

(ii) Jeśli wielomian v jest nierozkładalny w $F[\mathbf{x}]$, wówczas G jest przechodnia na X (to znaczy: dla każdych $a, b \in X$ istnieje automorfizm $f \in G$ taki, że $f(a) = b$).

(iii) Jeśli v nie ma w E pierwiastków wielokrotnych i G jest przechodnia na X, wówczas v jest nierozkładalny nad F.

Dowód.

(i) Pierwsza część twierdzenia wynika niemal natychmiast z twierdzenia 12.6 o grupie Galois rozszerzenia skończonego. Dla dowolnego $f \in \mathrm{Gal}(E : F)$ oznaczmy przez f_X zacieśnienie f do zbioru X. Odwzorowanie

$$T : G \ni f \to f_X \in H = \{g_X : g \in G\}$$

Teraz pozostaje już tylko do udowodnienia, że dla dowolnego $f \in \mathrm{Gal}(E : F)$ mamy $f_X \in S_X$ oraz, że odwzorowanie T jest izomorfizmem (por. zadanie 12.5).

(ii) Niech $a, b \in X$ będą dwoma różnymi pierwiastkami wielomianu v. Na mocy twierdzenia 11.28[3] wiemy, że dla dowolnych dwóch pierwiastków $a, b \in X$ wielomianu nierozkładalnego v istnieje izomorfizm $f : F(a) \to F(b)$ taki, że $f(a) = b$

[3] Twierdzenie 11.28 stosujemy tu do prostej sytuacji kiedy (przy oznaczeniach jak w twierdzeniu 11.28) mamy $\tilde{F} = F$ a rozszerzany na $F(a)$ izomorfizm $\sigma : F \to F$ jest identycznością.

i $f(\alpha) = \alpha$ dla każdego $\alpha \in F$.
Na mocy lematu **??** izomorfizm ten można przedłużyć do izomorfizmu $E \to E$ (z łatwością można stwierdzić, że ten izomorfizm jest automorfizmem E ustalającym F, a więc jest elementem grupy $\mathrm{Gal}(E : F)$).

(iii) Dla dowodu nie w prost przypuśćmy, że grupa $\mathrm{Gal}(E : F)$ działa przechodnio na X, v nie ma pierwiastków wielokrotnych a wielomian v jest rozkładalny nad F, czyli istnieją $u, w \in F[\mathbf{x}]$, $\partial u, \partial w \geq 1$ i

$$v = uw$$

Niech $a, b \in E$ będą takimi pierwiastkami v, że $u(a) = 0$ i $w(b) = 0$. Ponieważ, z założenia, $\mathrm{Gal}(E : F)$ działa przechodnio na X, istnieje $f \in \mathrm{Gal}(E : F)$ takie, że $f(a) = b$. Wtedy $u(b) = u(f(a)) = f(u(a)) = f(0) = 0$ a więc b jest pierwiastkiem u. Ponieważ zaś b jest pierwiastkiem w i $v = uw$, b byłby pierwiastkiem podwójnym v. Ta sprzeczność kończy dowód twierdzenia. ■

12.3 Wielomiany i ciała rozdzielcze

Twierdzenie 12.11 *Niech F będzie dowolnym ciałem i niech $v \in F[\mathbf{x}]$ będzie wielomianem nierozkładalnym nad F. Niech E będzie rozszerzeniem ciała F, w którym v rozkłada się na czynniki liniowe.*
Pierwiastki wielomianu v są między sobą różne[4] *wtedy i tylko wtedy gdy $v' \neq 0$.*

Przypomnijmy, że $v' \neq 0$ oznacza, że v' nie jest wielomianem zerowym a więc ma co najmniej jeden współczynnik różny od zera.

Przykład 12.6 Wielomian $v = \mathbf{x}^2 + \mathbf{x} + 1 \in \mathbb{Z}_2[\mathbf{x}]$ jest nad $\mathbb{Z}_2$ nierozkładalny. Wielomian pochodny $v' = 1$ jest różny od zera i wobec tego i twierdzenia 12.3 w dowolnym ciele, w którym v się rozkłada, ma dwa różne między sobą pierwiastki.
Przykładem wielomianu nie spełniającego w $\mathbb{Z}_2[\mathbf{x}]$ warunku niezerowania pochodnej jest wielomian $w = \mathbf{x}^4 + \mathbf{x}^2 + 1$. □

Dowód twierdzenia 12.11.
Przypuśćmy wpierw, że wielomian $v \in F[\mathbf{x}]$ w rozszerzeniu E nie ma pierwiastków wielokrotnych, $a \in E$ jest pierwiastkiem v i przypuśćmy także, dla dowodu nie wprost, że $v' = 0$. Wówczas jednak $v(a) = v'(a) = 0$ – sprzeczność z wnioskiem 11.21.
Niech teraz $v' \neq 0$ i przypuśćmy, że $a \in E$ jest pierwiastkiem wielokrotnym wielomianu v. Na mocy twierdzenia 11.20 $\mathbf{x} - a$ dzieli zarówno v jak i v'. Wiemy, że wielomian v jest nad F nierozkładalny i $\partial v' < \partial v$. Stąd wynika, że wielomiany v' i v są względnie pierwsze. Istnieją więc wielomiany $u, w \in F[\mathbf{x}]$ takie, że

$$uv' + wv = 1 \tag{12.3}$$

[4] Inaczej: v nie ma pierwiastków wielokrotnych.

Lewa strona równości (12.3 jest podzielna przez $\mathbf{x} - a$ a zatem $\mathbf{x} - a|1$ - sprzeczność, która kończy dowód. ■

Z twierdzenia 12.3 wynika następujący wniosek.

Wniosek 12.12 *Jeśli F jest ciałem a v wielomianem nierozkładalnym nad F wówczas v nie ma pierwiastków wielokrotnych w pewnym ciele, w którym v się rozkłada na czynniki liniowe wtedy i tylko wtedy gdy v nie ma pierwiastków wielokrotnych w żadnym ciele w którym się rozkłada.* ■

Można więc powiedzieć, że fakt posiadania (lub nie) pierwiastków wielokrotnych jest własnością wielomianu a nie ciała, w którym ma współczynniki.

Wielomian nieredukowalny $v \in F[\mathbf{x}]$ nad ciałem F nazywamy **rozdzielczym** nad F jeżeli jego pierwiastki w ciele, w którym się rozkłada na czynniki liniowe, są między sobą różne (lub, co na jedno wychodzi dzięki twierdzeniu 12.11, jego pochodna nie jest równa zero). Dowolny wielomian $v \in F[\mathbf{x}]$ stopnia większego od zera nazywamy **rozdzielczym** jeśli każdy jego czynnik nierozkładalny jest rozdzielczy nad F.
Rozszerzenie $E : F$ jest **rozdzielcze** jeśli

- jest algebraiczne,
- wielomian minimalny każdego elementu jest rozdzielczy nad F.

Przykład 12.7 *Wielomian $\mathbf{x}^4 + 4\mathbf{x}^2 + 4 = (\mathbf{x}^2 + 2)^2$ jest rozdzielczy nad $\mathbb{Q}$.*

Przykład 12.8 $\mathbf{x}^6 + \mathbf{x}^3 + 1 \in \mathbb{Z}_3[\mathbf{x}]$ *jest rozdzielczy chociaż $(\mathbf{x}^6 + \mathbf{x}^3 + 1)' = 0$ bowiem $(\mathbf{x}^6 + \mathbf{x}^3 + 1 = (\mathbf{x}^2 - \mathbf{x} - 1)^3$ i wielomian $w = \mathbf{x}^2 - \mathbf{x} - 1$ jest nierozkładalny nad $\mathbb{Z}_3$. Jego pochdna $w' = 2\mathbf{x} - 1 \neq 0$*

Okazuje się, że wielomiany, które nie są rozdzielcze, można spotkać jedynie w ciałach z charakterystyką.

Twierdzenie 12.13 *Niech v będzie wielomianem nierozkładalnym nad ciałem F, $\partial v > 0$.*

1. *Jeśli F jest bez charakterystyki to v jest rozdzielczy.*
2. *Jeśli $\mathrm{char}\,(F) = p$ to v jest rozdzielczy wtedy i tylko wtedy gdy nie jest postaci $w(\mathbf{x}^p)$ dla pewnego $w \in F[\mathbf{x}]$.*

Dowód twierdzenia 12.13 wynika niemal natychmiast z twierdzenia 12.11 i pozostawiam go do samodzielnego przeprowadzenia jako zadanie 12.1. ■

Wniosek 12.14 *Jeśli ciało F jest bez charakterystyki (lub inaczej: jeśli $\mathrm{char}\,(F) = 0$), to każde rozszerzenie algebraiczne ciała F jest rozdzielcze.* ■

Twierdzenie 12.15 (O liczbie rozszerzeń izomorfizmu) *Niech $v \in F[\mathbf{x}]$ będzie wielomianem rozdzielczym, $\sigma : F \to \bar{F}$ izomorfizmem ciał. Jeśli E i $\bar{E}$ są ciałami rozkładu, odpowiednio, v i σv, wówczas istnieje dokładnie $[E : F]$ izomorfizmów $\bar{\sigma} : E \to \bar{E}$, które rozszerzają σ do izomorfizmu ciał $E \to \bar{E}$.*

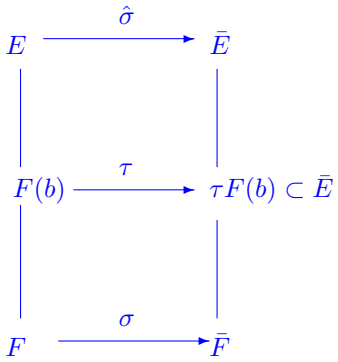
Dowód. Przez indukcję ze względu na $n = [E : F]$.
Jeśli $[E : F] = 1$ to $E = F$, rozkładami v w E i σv w $\bar{E}$ są, odpowiednio

$$v = a(\mathbf{x} - a_1)...(\mathbf{x} - a_n), \quad a, a_i \in F$$

oraz

$$\sigma v = \sigma(a)(\mathbf{x} - \sigma(a_1))...(\mathbf{x} - \sigma(a_n))$$

Oczywiście $\sigma : F \to \bar{F}$ jest jedynym rozszerzeniem $\sigma : F \to \bar{F}$.
Załóżmy więc, że $[E : F] > 1$. Wtedy v nie rozkłada się na iloczyn czynników liniowych w $F[\mathbf{x}]$. Niech $w \in F[\mathbf{x}]$ będzie nierozkładalnym nad F czynnikiem v takim, że $\partial w = k \geq 2$. Niech $b \in E$ będzie pewnym pierwiastkiem w. Oczywiście wtedy w jest wielomianem minimalnym elementu b nad F (czyli $k = \deg_F(b)$).
Sytuację opisuje następujący diagram.



Izomorfizm $\sigma : F \to \bar{F}$ rozszerzamy na monomorfizm $\tau : F(b) \to \bar{E}$. τ jest wtedy izomorfizmem $F(b) \to \tau(F(b))$ (w dalszym ciągu, dla wygody obraz $F(b)$ przez τ zapisujemy $\tau F(b)$). Następnie τ rozszerzamy na $\hat{\sigma} : E \to \bar{E}$.
Można na tę sytuację popatrzeć nieco inaczej: każde rozszerzenie $\hat{\sigma} : E \to \bar{E}$ izomorfizmu $\sigma : F \to \bar{F}$ można zacieśnić do pewnego izomorfizmu $\tau : F(b) \to \tau(F(b))$, które jest pewnym rozszerzeniem izomorfizmu $\sigma : F \to \bar{F}$.
Liczba wszystkich rozszerzeń $\hat{\sigma} : E \to \bar{E}$ izomorfizmu σ jest równa

(liczbie rozszerzeń $\tau : F(b) \to \tau F(b)$ $\times$ (liczba rozszerzeń τ na izomorfizmy $E \to \bar{E}$)

Oczywiście takie rozumowanie jest uzasadnione jeśli odpowiednie rozszerzenia potrafimy wskazać i jeśli dla każdego izomorfizmu $\tau : F(b) \to \tau F(b)$ liczba rozszerzeń na izomorfizm $E \to \bar{E}$ jest taka sama.

Z twierdzenia 11.13 o wieży mamy

$$[E : F(b)] = [E : F]/[F(b) : F] = [E : F]/k < [E : F] \tag{12.4}$$

bowiem w jest nierozkładalny nad F, czyli $[F(b) : F] = k$ (twierdzenie 11.10, część 3). Wiemy także, że $k \geq 2$, stąd we wzorze (12.4) silna nierówność.
E jest ciałem rozkładu a v jest rozdzielczy nad $F(b)$ (część **??** twierdzenia 12.3 - wielomian nierozkładalny rozdzielczy w pewnym ciele ma wszystkie pierwiastki różne w każdym ciele w którym się rozkłada). Jeśli u jest czynnikiem v nierozkładalnym nad $F(b)$, to dzieli pewien wielomian nierozkładalny nad F, który to wielomian nie ma pierwiastków wielokrotnych. A więc i u nie ma pierwiastków wielokrotnych, czyli jest wielomianem rozdzielczym.

Na mocy założenia indukcyjnego każdy izomorfizm $\tau : F(b) \to \tau(F(b)) \subset \bar{E}$ ma $[E : F(b)]$ różnych rozszerzeń.
Odpowiedzmy sobie teraz na pytanie: *ile jest różnych rozszerzeń $\tau : F(b) \to \tau(F(b))$ izomorfizmu $\sigma : F \to \bar{F}$?*
Odwzorowanie

$$\tilde{\sigma} : F[\mathbf{x}] \ni p \to \sigma p \in \bar{F}[\mathbf{x}]$$

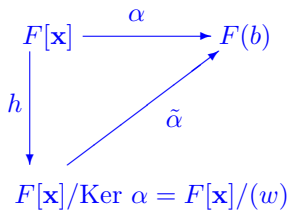
jest izomorfizmem pierścieni, ponieważ σ jest izomorfizmem $F \to \bar{F}$. Skoro więc wieloman w jest nierozkładalny nad F i rozdzielczy, to także wielomian σw jest nierozkładalny nad $\bar{F}$ i rozdzielczy. Powiedzmy, że pierwiastkami w (w E) są $b_1, ..., b_k$ (b jest oczywiście jednym z nich), wszystkie są między sobą różne. Skoro, z założenia, $\bar{E}$ jest ciałem rozkładu wielomianu σv, łatwo sprawdzić, że także σw jest w $\bar{E}$ rozkładalny, powiedzmy, że $c_1, ..., c_k$ są pierwiastkami σw w $\bar{E}$. Rozważmy teraz k homomorfizmów:

$$\tau_i : F(b) \ni p(b) \to \sigma p(c_i) \in \bar{F}(c_i) \quad (i = 1, ..., k) \tag{12.5}$$

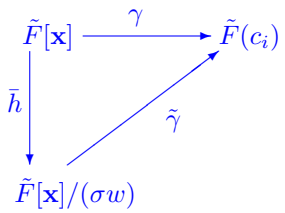
Tak zdefiniowane τ_i są izomorfizmami bowiem każde τ_i $(i = 1, ..., k)$ jest złożeniem trzech izomorfizmów:

$$p(b) \quad \overset{\tilde{\alpha}^{-1}}{\to} \quad p + (w) \quad \overset{\beta}{\to} \quad \sigma p + (\sigma w) \quad \overset{\tilde{\gamma}}{\to} \quad \sigma p(c_i)$$

- $\tilde{\alpha}^{-1}$ jest izomorfizmem wynikającym z twierdzenia 8.8 o izomorfizmie pierścieni dla epimorfizmu $\alpha : F[\mathbf{x}] \ni p \to p(b) \in F(b)$, jak przedstawiono na diagramie (Ker $\alpha = (w)$ - ideał wszystkich wielomianów podzielnych przez w w $F[\mathbf{x}]$).



- Podobnie, na mocy twierdzenia 8.8 istnieje izomorfizm $\tilde{\gamma}$, dla $\gamma : \tilde{F}[\mathbf{x}] \to \tilde{F}(c_i)$ (por. diagram poniżej).



- β jest izomorfizmem zdefiniownym wzorem $\beta(p + (w)) = \sigma p + (\sigma w)$.

Takich izomorfizmów jest oczywiście k, wartością bowiem izomorfizmu każdego τ_i na pierwiastku b wielomianu w musi być pierwiastek wielomianu σw a tych jest k $(c_1, ..., c_k)$. Łatwo też można się przekonać, że innych izomorfizmów $F(b) \to \bar{F}(c_i)$ niż te dane wzorami (12.5) nie ma.

Ostatecznie wszystkich szukanych rozszerzeń izomorfizmu $\sigma : E \to \bar{F}$ jest

$$[E : F(b)] \cdot k = \frac{[E : F]}{[F(b) : F]} \cdot k = \frac{[E : F]}{k} \cdot k = [E : F]$$

■

Celem, dla którego dowodziliśmy twierdzenia 12.15 jest wniosek *o liczności grupy Galois ciała wielomianu rozdzielczego*, który otrzymamy przyjmując w twierdzeniu $\bar{E} = E$, $\bar{F} = F$ i $\sigma = \mathrm{id}_F$[5].

Wniosek 12.16 *Jeśli $E : F$ jest ciałem rozkładu wielomianu rozdzielczego, wówczas*

$$|Gal(E : F)| = [E : F]$$

■

12.4 Twierdzenie o elemencie prymitywnym

Twierdzenie 12.17 *Jeśli E jest skończonym i rozdzielczym rozszerzeniem ciała F wówczas istnieje element $a \in E$ taki, że $E = F(a)$.*

Skoro wszystkie ciała bez charakterystyki są rozdzielcze z twierdzenia 12.17 wynika następujący, spektakularny wniosek.

[5]Powstaje pytanie: *dlaczego dowodzimy tak dużo, skoro potrzeba nam znacznie mniej?* Odpowiedź jest prosta: *nie potrafimy inaczej.*

Wniosek 12.18 *Każde rozszerzenie skończone bez charakterystyki jest rozszerzeniem prostym.* □

Dowód twierdzenia o elemencie prymitywnym.
Jeśli F jest ciałem Galois (to znaczy, przypomnijmy, ciałem skończonym), wówczas także rozszerzenie skończone $E : F$ jest skończone i na mocy twierdzenia **??** grupa $E^* = E - \{0\}$ jest cykliczna, czyli istnieje taki element $a \in E$, że $E^* =< a >$. Stąd oczywiście wynika, że $E = F(a)$.

Przypuśćmy więc, że E jest ciałem nieskończonym. Wiemy, że E jest rozszerzeniem skończonym[6] ciała F a więc, na mocy twierdzenia 11.12 o rozszerzeniach skończonych, $E = F(a_1, ..., a_n)$ dla pewnych $a_1, ..., a_n \in E$. Udowodnimy, że dla dowolnych $a, b \in E$ istnieje $d \in E$ takie, że $F(a, b) = F(d)$ (następnie wystarczy przeprowadzić proste rozumowanie rekurencyjne wykorzystujące wzór $F(a_1, ..., a_n) = F(a_1, ..., a_k)(a_{k+1}, ..., a_n)$, twierdzenie 11.8).
Niech $u \in F[\mathbf{x}]$ i $v \in F[\mathbf{x}]$ będą wielomianami minimalnymi a i b, odpowiednio, oraz niech $a_1 = a, a_2, ..., a_l$ i $b_1 = b, b_2, ..., b_n$ będą, odpowiednio, pierwiastkami u i v w E. Te pierwiastki są różne między sobą bo wielomiany u i v jako minimalne są nierozkładalne nad F a ciało E jest rozdzielcze, stąd u i v są rozdzielcze.

Przyjrzyjmy się zbiorowi

$$A = \left\{ \frac{a - a_i}{b - b_b} | i = 2, ..., l; j = 2, ..., n \right\}$$

(pamiętamy, że $a = a_1, b = b_1$).
Zbiór A jest skończony (ma co najwyżej $(m-1)(n-1)$ elementów). Ponieważ F jest zbiorem nieskończonym, istnieje element

$$c \in F \text{ taki, że } c \notin A, c \neq 0$$

Weźmy teraz element

$$d = a - cb$$

Wykażemy, że

$$F(d) = F(a, b)$$

Ponieważ $d \in F(a, b)$ mamy

$$F(d) \subset F(a, b)$$

Wystarczy wiąc wykazać, że $a, b \in F(d)$. Co więcej, jeśli wykażemy, że $b \in F(d)$ to będziemy mieli $cb \in F(d)$ (bo $c \in F$) i stąd $a = d + cb \in F(d)$).
Niech $m \in F(d)$ będzie wielomianem minimalnym elementu b. Wykażemy, że m jest liniowy skąd już będzie wynikało, że jego pierwiastek b jest elementem $F(d)$ (i to

[6] Można się tu zagubić przez niezbyt fortunne nazewnictwo. Przypomnijmy więc, że **ciało skończone** to ciało o skończonej liczbie elementów, **rozszerzenie skończone** ciała F to takie rozszerzenie, które jako przestrzeń wektorowa nad ciałem F ma wymiar skończony.

będzie koniec naszego dowodu).

Wielomian m dzieli v, bo m jest wielomianem minimalnym elementu b i $v(b) = 0$. A więc wielomian m jest iloczynem wielomianów postaci $\mathbf{x} - b_j$.
Zdefiniujmy teraz wielomian

$$p = u(d + c\mathbf{x}) \in F(d)[\mathbf{x}]$$

(pamiętamy, że u jest wielomianem minimalnym elementu a). Wtedy

$$p(b) = u(d + cb) = u(a) = 0$$

a więc wielomian m dzieli wielomian p (jako, że m jest wielomianem minimalnym elementu b).
Wykażemy, że

$$p(b_j) \neq 0 \text{ dla } j = 2, ..., n$$

Rzeczywiście, przypuśćmy, że dla pewnego $j \in \{2, ..., n\}$ mamy $p(b_j) = 0$. Wtedy mielibyśmy

$$u(d + cb_j) = 0$$

a więc $d + cb_j$ byłoby pierwiastkiem wielomianu u, czyli istniałoby $i \in \{2, ..., l\}$ takie, że $d + cb_j = a_i$ lub $d + cb_j = a$.
Gdyby $d + cb_j = a$ to $\underbrace{a - cb}_{d} + cb_j = a$ i w konsekwencji $c(b - j - b) = 0$. Ponieważ z założenia $c \neq 0$ mielibyśmy $b_j = b$ a to także jest niemożliwe, bo pierwiastki $b, b_2, ..., b_n$ są między sobą różne.
Gdyby $d + cb_j = a_i$, $i \in \{2, ..., l\}$, wówczas wielibyśmy $a - cb + b_j = a_i$ a więc $c(b - b_j) = a - a_I$ i stąd $c = \frac{a - a_i}{b - b_j}$, to zaś jest niemożliwe, bowiem $c \notin A$.
Stwierdziliśmy więc wpierw, że m jest iloczynem wielomianów postaci $\mathbf{x} - b_j$ i $\mathbf{x} - b$ a następnie, że żaden czynnik postaci $\mathbf{x} - b_j$ $(j = 2, ..., n)$ w m nie występuje. Stąd oczywiście wynika, że

$$m = \mathbf{x} - b \in F(d)[\mathbf{x}]$$

co oznacza, że $b \in F(b)$ i dowód jest zakończony. ■

Przykład 12.9 Zilustrujmy metodę dowodu twierdzenia na przykładzie rozszerzenia $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$.
Wielomianem minimalnym $\sqrt{2}$ jest $u = \mathbf{x}^2 - 2$, pierwiastkami tego wielomianu są $a = \sqrt{2}$ i $a_2 = -\sqrt{2}$. Wielomianem minimalnym i jest $v = \mathbf{x}^2 + 1$ a pierwiastkami wielomianu v są $b = i$ oraz $b_2 = -i$. Zbiór $A = \left\{\frac{a - a_2}{b - b_2}\right\} = \left\{\frac{2\sqrt{2}}{2i}\right\} = \{-i\sqrt{2}\}$.
Oczywiście $-1 \notin A$ i stąd $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$. □

12.5 Twierdzenie Dedekinda-Artina

Jeśli $E : F$ jest rozszerzeniem ciaą F, $F \subset E$ i K jest ciałem takim, że $F \subset K \subset E$, wówczas K nazywamy **ciałem pośrednim**[7]. Przekonamy się, że istnieją odpowiedniości pomiędzy ciałami pośrednimi a podgrupami grupy $\mathrm{Gal}(E : F)$. Odpowiedniości te zaobserwował Galois i stanowią one istotę teorii Galois. W formie wyników dotyczących rozszerzeń ciał odpowiedniości te sformułował Dedekind (w 1894 roku).

Niech G będzie grupą, E ciałem, i niech

$$\varphi_1, ..., \varphi_n : G \to E^* = E - \{0\}$$

będą homomorfizmami grupy G w grupę E^*. Takie homomorfizmy nazywane są **charakterami**.
Mówimy, że charaktery $\varphi_1, ..., \varphi_n$ są **niezależne** jeżeli dla dowolnych $\alpha_1, ..., \alpha_n \in E$

$$\alpha_1\varphi_1 + ... + \alpha_n\varphi_n = 0 \Rightarrow \alpha_1 = ... = \alpha_n = 0$$

przy czym, dla $\alpha \in E$, oraz charakterów φ, ψ przez $\alpha\varphi$ rozumiemy charakter, którego wartość na elemencie g grupy G jest równa $\alpha \cdot \varphi(g)$, zaś przez $\varphi + \psi$ charakter, którego wartość na g jest równa $(\varphi + \psi)(g) = \varphi(g) + \psi)g)$.

Lemat 12.19 (Dedekind) *Niech G będzie grupą a E ciałem. Każdy zbiór różnych między sobą charakterów $\varphi_1, ..., \varphi_n$ grupy G w E^* jest niezależny.*

Dowód. Przez indukcję ze względu na n.
Gdy $n = 1$, wówczas z równości $\alpha\varphi(g) = 0$ oraz faktu, że dla dowolnego $g \in G$ mamy $\varphi(g) \neq 0$ (pamiętamy, że $\varphi : G \to E^* = E - \{0\}$) wynika, że $\alpha = 0$.
Przypuśćmy więc, że $n > 1$ i każde co najwyżej $n - 1$ różnych charakterów jest niezależnych. Niech $\varphi_1, ..., \varphi_n : G \to E^*$ będą różnymi charakterami i niech $\alpha_1, ..., \alpha_n \in E$ będą takie, że

$$\alpha_1\varphi_1 + ... + \alpha_n\varphi_n = 0 \tag{12.6}$$

Ponieważ, na mocy założenia indukcyjnego, z zerowania się kombinacji mniej niż n charakterów wynika zerowanie się współczynników tej kombinacji, możemy założyć, że wszystkie współczynniki α_i we wzorze (12.6) są różne od zera.
Ze wzoru (12.6) wynika, że dla dowolnych elementów $g, h \in G$ wartość $\alpha_1\varphi_1 + ... + \alpha_n\varphi_n$ obliczona na g a także na $g \cdot h$ jest równa zero. Mamy więc

$$\alpha_1\varphi_1(g) + ... + \alpha_n\varphi_n(g) = 0 \tag{12.7}$$

oraz

$$\alpha_1\varphi_1(g)\varphi_1(h) + ... + \alpha_n\varphi_n(g)\varphi_n(h) = 0 \tag{12.8}$$

Po przemnożeniu równości (12.7) przez $\varphi_1(h)$ i odjęciu (12.8) stronami otrzymamy

$$\alpha_2\varphi_2(g)(\varphi_1(h) - \varphi_2(h)) + ... + \alpha_n\varphi_n(g)(\varphi_1(h) - \varphi_n(h)) = 0 \tag{12.9}$$

[7] Pamiętamy o przypisie ze strony 159, zgodnie z którym zawierania oznaczają w kontekscie ciał izomorfizmy z podciałem, Ta uwaga stosuje się także w opisywanej teraz sytuacji.

dla każdych g, h - homomorfizmów $G \to E^\circ$. Stąd i z założenia indukcyjnego, dla każdego $i = 2, ..., n$ zachodzi równość

$$\alpha_i(\varphi_1(h) - \varphi_i(h)) = 0$$

Pamiętamy, że $\alpha_i \neq 0$ dla każdego i, mamy więc $\varphi_1(h) = \varphi_i(h)) = 0$ co oznacza, że $\varphi_i = \varphi_1$ dla wszystkich $i = 2, ..., n$, a to sprzeczność z założeniem, że wszystkie $\varphi_1, ..., \varphi_n$ są między sobą różne. Otrzymana sprzeczność kończy dowód lematu. ■

Jeśli zamiast dowolnej grupy G w lemacie Dedekinda przyjmiemy grupę E^*, to otrzymamy następujący wniosek.

Wniosek 12.20 *Każdy zbiór automorfizmów ciała jest niezależny.* □

Lemat Dedekinda wykorzystamy w dowodzie następnego twierdzenia o relacji pomiędzy rzędem grupy Galois a rozmiarem rozszerzenia.

Twierdzenie 12.21 *Niech E będzie skończonym rozszerzeniem ciała F. Wówczas*

$$|Gal(E : F)| \leq [E : F]$$

Dowód. Niech $b_1, ..., b_n$ będzie bazą E nad F (wtedy $[E : F] = n$). Dla dowodu nie wprost przypuśćmy, że w $\mathrm{Gal}(E : F)$ automorfizmy $f_1, ..., f_{n+1}$ są różnymi elementami $\mathrm{Gal}(E : F)$.
Rozważmy następujący układ n równań o $n + 1$ niewiadomych:

$$\begin{array}{ccccccccc} f_1(b_1)x_1 & + & f_2(b_1)x_2 & +...+ & f_{n+1}(b_1)x_{n+1} & = & 0 \\ f_1(b_2)x_1 & + & f_2(b_2)x_2 & +...+ & f_{n+1}(b_2)x_{n+1} & = & 0 \\ & & & ... & & & \\ f_1(b_n)x_1 & + & f_2(b_n)x_2 & +...+ & f_{n+1}(b_n)x_{n+1} & = & 0 \end{array}$$

Mamy więc układ n równań liniowych jednorodnych o $n + 1$ niewiadomych, który wobec tego posiada rozwiązanie niezerowe $x_j = a_j$, co oznacza, że nie wszystkie a_j są równe zeru oraz mamy

$$\sum_{j=1}^{n+1} f_j(b_i)a_j = 0 \quad \text{dla i=1,...,n}$$

Niech teraz a będzie dowolnym elementem E. a można zapisać jako liniową kombinację elementów bazy E nad F to znaczy

$$a = \sum_{i=1}^{n} \alpha_i b_i$$

i stąd otrzymujemy

$$\begin{array}{rcll} \sum_{j=1}^{n+1} a_j f_j(a) & = & \sum_{j=1}^{n+1} a_j f(\sum_{i=1}^{n} \alpha_i b_i) & \\ & = & \sum_{j=1}^{n+1} a_j \left(\sum_{i=1}^{n} \alpha_i f_j(b_i)\right) & \text{(pamiętamy, że } f_j(\alpha_i) = \alpha_i \text{ dla } \alpha_i \in F) \\ & = & \sum_{i=1}^{n} \left(\sum_{j=1}^{n+1} a_j f_j(b_i)\right) & \\ & = & 0 & \end{array}$$

Homomorfizmy $f_1, ..., f_{n+1}$ choć różne między sobą, są liniowo zależne (o $a_1, ..., a_n$ wiemy, że nie wszystkie są równe zeru) co jest sprzeczne z lematem Dedekinda. ■

Powstaje naturalne pytanie: czy i ewentualnie kiedy we wzorze $|\mathrm{Gal}(E : F)| \leq [E : F]$ zamiast nierówności jest równość? Żeby na to pytanie odpowiedzieć wprowadzimy pojęcie **ciała ustalonego przez grupę automorfizmów**.
Niech E będzie ciałem i G grupą automorfizmów $E \to E$. **Ciałem ustalonym przez** G nazywamy

$$E_G = \{a \in E | g(a) = a \text{ dla każdego } g \in G\}$$

Oczywiście, jak można łatwo sprawdzić, E_G jest ciałem, pewnym podciałem ciała E. Bardzo często wygodnie nam będzie oznaczać ciało ustalone przez grupę G przez $G^\dagger$.

Twierdzenie 12.22 (Dedekinda-Artina) *Niech G będzie skończoną grupą automorfizmów ciała E. Wówczas*

$$|G| = [E : E_G]$$

(co oczywiście inaczej można zapisać w postaci $|G| = [E : G^\dagger]$).

Dowód. Oczywiście mamy $G = \mathrm{Gal}(E : E_G)$ a więc, na mocy twierdzenia 12.21,

$$|G| \leq [E : E_G]$$

Wystarczy więc udowodnić, że jeśli $|G| = n$, to w E nie ma $n + 1$ elementów liniowo niezależnych nad E_G.
Przypuśćmy, dla dowodu nie wprost, że $|G| = n$ i $a_1, ..., a_{n+1} \in E$ są liniowo niezależne nad E_G.
Rozważmy układ n równań liniowych jednorodnych o $n + 1$ niewiadomych:

$$g(a_1)x_1 + g(a_2)x_2 + ... + g(a_{n+1})x_{n+1} = 0 \tag{12.10}$$

gdzie $g \in G$. Skoro równań jest mniej niż niewiadomych istnieją rozwiązania niezerowe tego układu. Niech r będzie minimalną liczbą wartości różnych od zera w niezerowym rozwiązaniu układu (12.10). Bez straty ogólności możemy przypuścić, że istnieje rozwiązanie $b_1, ..., b_n \in E$ takie, że

$$\begin{aligned} b_1, ..., b_r &\neq 0 \\ b_{r+1}, ..., b_{n+1} &= 0 \end{aligned}$$

przy czym $r \geq 2$ (rzeczywiście, gdyby $r = 1$ to mielibyśmy $g_1(a_1)b_1 = 0$ i wobec tego, że $b_1 \neq 0$, dla dowolnego $g \in G$ zachodziłaby równość $g(a_1) = 0$, także dla $g = id_E$, czyli $a_1 = 0$ a to sprzeczne z założeniem, że $a_1, ..., a_{n+1}$ jest bazą E nad E_G).
Mamy więc

$$g(a_1)b_1 + ...g(a_r)b_r = 0 \tag{12.11}$$

dla wszystkich $g \in G$. Skoro $b_1 \neq 0$ (podobnie jak wszystkie $b_i \neq 0$ dla $i = 1, ..., r$), układ (12.11) jet równoważny układowi

$$g(a_1) + g(a_2)c_2 + ...g(a_r)c_r = 0 \tag{12.12}$$

gdzie $c_i = b_i/b_1$ dla $i = 1, ..., r$ i $g \in G$. Zastępując w (12.12) g przez identyczność otrzymamy

$$a_1 + a_2c_2 + ... + a_rc_r = 0$$

Ponieważ $a_1, ..., a_r$ są liniowo niezależne nad E_G co najmniej jedno z c_i nie należy do E_G, powiedzmy $c_{k_0} \notin E_G$, $1 < k_0 \leq r$. Wtedy dla pewnego $h \in G$ mamy $h(c_{k_0}) \neq c_{k_0}$. Biorąc teraz wartość h na równaniach (12.12) otrzymamy

$$hg(a_1) + hg(a_2)h(c_2) + ... + hg(a_r)h(c_r) = 0 \quad \text{dla wszystkich } g \in G \tag{12.13}$$

Skoro g przebiega wszystkie elementy grupy G, także hg przebiega wszystkie elementy grupy G, stąd układ (12.13) można zapisać w postaci

$$f(a_1) + f(a_2)h(c_2) + ... + f(a_r)h(c_r) = 0 \tag{12.14}$$

g i f występują dokładnie w tej samej roli w (12.12) i (12.14) a więc zmieniając stosownie kolejność równań w (12.14) i po odejmujęciu równości (12.14) od (12.12) stronami będziemy mieli

$$g(a_2)(c_2 - h(c_2)) + ... + g(a_r)(c_r - h(c_r)) = 0 \quad \text{dla } g \in G \tag{12.15}$$

Pamiętamy jednak, że $c_{k_0} \neq h(c_{k_0})$, to zaś oznacza, że

$$x_1 = 0, x_2 = c_2 - h(c_2), ..., x_r = c_r - h(c_r), x_{r+1} = 0, ..., x_{n+1} = 0$$

jest niezerowym rozwiązaniem układu (12.10), w którym jest o co najmniej jedno zero więcej niż w rozwiązaniu $b_1, ..., b_r, 0, ..., 0$ a to sprzeczne z wyborem r - ta sprzeczność kończy dowód twierdzenia. ■

Przykład 12.10 ($\mathbb{Q}(e^{2\pi i/5})$) Oznaczmy przez $a = e^{2\pi i/5}$. a jest pierwiastkiem wielomianu $v = \mathbf{x}^5 - 1 = (\mathbf{x} - 1)(\mathbf{x}^4 + \mathbf{x}^3 + \mathbf{x}^2 + \mathbf{x} + 1)$. Wielomian $\mathbf{x}^4 + \mathbf{x}^3 + \mathbf{x}^2 + \mathbf{x} + 1$ jest nierozkładalny i rozdzielczy więc $[\mathbb{Q}(a) : \mathbb{Q}] = 4$. Rzeczywiście, elementami grupy G automorfizmów $\mathbb{Q}(a)$ są następujące

$$\begin{array}{lcccc} \mathrm{id}_E: & a \to a & a^2 \to a^2 & a^3 \to a^3 & a^4 \to a^4 \\ f: & a \to a^2 & a^2 \to a^4 & a^3 \to a & a^4 \to a^3 \\ g: & a \to a^3 & a^2 \to a & a^3 \to a^4 & a^4 \to a^2 \\ h: & a \to a^4 & a^2 \to a & a^3 \to a^2 & a^4 \to a \end{array}$$

Każdy element grupy automorfizmów $\mathbb{Q}(a)$ jest, jak łatwo zauważyć, rzędu 2, a więc grupa ta jest grupą Kleina. □

Centralne miejsce w teorii Galois, jej najbardziej istotnym pomysłem, są tak zwane *odpowiedniości Galois*, przez które rozumie się związki jakie istnieją pomiędzy podciałami ciała E a pewnymi grupami Galois.
Niech E i F będą ciałami, $E : F$ i $G = \mathrm{Gal}(E : F)$. Ciało K nazywamy **pośrednim** jeśli $E : K$ i $K : F$. Na zasadzie wyjaśnionej w przypisie na stronie 159 będziemy

wtedy pisać (i rozumieć) $F \subset K \subset E$.
Grupę Galois $\mathrm{Gal}(E : K)$ rozszerzenia $E : K$ oznaczać będziemy przez K°, czyli

$$K^\circ = \{g \in G : g(a) = a \text{ dla każdego } a \in K\}$$

Przez $\mathcal{F}$ oznaczmy zbiór ciał pośrednich zaś przez $\mathcal{G}$ zbór podgrup grupy $G = \mathrm{Gal}(E : F)$. Wtedy można zdefiniować dwa odwzorowania:

$$\circ : \mathcal{F} \ni K \to K^\circ = \mathrm{Gal}(E : K) \leq G$$

oraz

$$\dagger : \mathcal{G} \ni H \to H^\dagger = \{a \in E : g(a) = a \text{ dla każdego } g \in H\}$$

Bardzo łatwo można sprawdzić, że $H^\dagger$ jest podciałem E i $H^\dagger \supset F$, czyli $F \subset H^\dagger \subset E$ ($H^\dagger$ jest ciałem pośrednim). Podobnie, nie jest trudne sprawdzenie prawdziwości następującego twierdzenia.

Twierdzenie 12.23 *Jeśli $E : F$ i K oraz L są ciałami pośrednimi wówczas*

$$K \subset L \Rightarrow K^\circ \supset L^\circ$$

Podobny związek zachodzi dla operacji $\dagger$.

Twierdzenie 12.24 *Jeśli $H_1, H_2 \leq Gal(E : F)$ wówczas*

$$H_1 \subset H_2 \Rightarrow H_1^\dagger \supset H_2^\dagger$$

W związku z twierdzeniami 12.23 i 12.24 mówimy, że odwzorowania $\circ$ i $\dagger$ **odwracają zawierania**. Jeśli $G = \mathrm{Gal}(E : F)$ (gdzie E i F są ciałami) wówczas czywiste są następujące związki:

$$E^\circ = \{\mathrm{id}_E\}$$

$$F^\circ = G$$

$$\{\mathrm{id}_E\}^\dagger = E$$

$$G^\dagger \supset F$$

Ostatnia z powyższych relacji jest tylko zawieraniem i nie musi być wtedy równości. Widzieliśmy już, że $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\sqrt[3]{2})}\}$. W tym więc przypadku $G^\dagger = \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ i równości nie ma.

12.6 Rozszerzenia Galois

Niech ciało E będzie rozszerzeniem ciała F, $G = \mathrm{Gal}(E : F)$. Rozszerzenie $E : F$ nazywamy **rozszerzeniem Galois** jeśli $G^\dagger = F$. Oczywistym jest następujący warunek konieczny i wystarczający by rozszerzenie było rozszerzeniem Galois.

Twierdzenie 12.25 *Rozszerzenie $E : F$ jest rozszerzeniem Galois wtedy i tylko wtedy gdy dla dowolnego elementu $a \in E - F$ istnieje automorfizm $g \in Gal(E : F)$ taki, że $g(a) \neq a$.*

Przykład 12.11 Mieliśmy już okazję zauważyć, że

- $\mathbb{C}$ jest rozszerzeniem Galois $\mathbb{R}$.
- $\mathbb{Q}(\sqrt{2})$ jest rozszerzeniem Galois $\mathbb{Q}$.
- $\mathbb{Q}(\sqrt[3]{2})$ nie jest rozszerzeniem Galois $\mathbb{Q}$.

Na mocy definicji $G = \mathrm{Gal}(E : F)$ mamy $F^\circ = G$ i stąd $G^\dagger = F$ wtedy i tylko wtedy gdy $F^{*\dagger} = F$. Prawdziwe jest więc następujące twierdzenie.

Twierdzenie 12.26 (O rozszerzeniu Galois) *Rozszerzenie $E : F$ ciała F jest rozszerzeniem Galois wtedy i tylko wtedy gdy*

$$F^{*\dagger} = F$$

(mówimy wtedy, że ciało F jest **ciałem domkniętym***).* ■

Twierdzenie 12.27 (O skończonym rozszerzeniu Galois) *Niech $E : F$ będzie rozszerzeniem skończonym ciała F, $G = Gal(E : F)$. Następujące warunki są równoważne.*

(1) $E : F$ jest rozszerzeniem Galois.

(2) Każdy nierozkładalny wielomian $v \in F[\mathbf{x}]$ mający w E pierwiastek jest rozdzielczy i rozkłada się w $E[\mathbf{x}]$.

(3) E jest ciałem rozkładu pewnego wielomianu rozdzielczego z $F[\mathbf{x}]$.

Dowód.

(1) $\Rightarrow$ (2) Niech $v \in F[\mathbf{x}]$ będzie wielomianem nierozkładalnym nad F, niech $a \in E$będzie pierwiastkiem v w E i oznaczmy przez X zbiór $X = \{f(a) : f \in G\}$.
Zbiór X jest skończony bowiem, na mocy wniosku 12.7, grupa G jest skończona.
Oznaczmy przez u następujący wielomian

$$u = (\mathbf{x} - a_1)(\mathbf{x} - a_2) \cdot \ldots \cdot (\mathbf{x} - a_m) \tag{12.16}$$

gdzie $X = \{a_1, ..., a_m\}$.
Dla ustalonego automorfizmu $g \in G$ mamy co następuje:

(i) Elementy $g(a_1), ..., g(a_m)$ są między sobą różne (bo a_i są między sobą różne i g jest auto- a więc i mono-morfizmem).

(ii) $g(a_1), ..., g(a_m) \in X$ (bo $g(a_i) = g(f(a))$ dla pewnego $f \in G$ i stąd $g(a_i) = (gf)(a)$ i oczywiście $gf \in G$).

Wobec tego $\{g(a_1), ..., g(a_m)\} = X$ i

$$gu = (\mathbf{x} - g(a_1))(\mathbf{x} - g(a_2)) \cdot ... \cdot (\mathbf{x} - g(a_m)) = u \qquad (12.17)$$

- czynniki we wzorach (12.16) i (12.17) różnią się tylko kolejnością w jakiej są zapisane. Tak więc każdy automorfizm $g \in G$ ustala wszystkie współczynniki wielomianu u co oznacza, że $u \in F[\mathbf{x}]$.
Wielomian v jest wielomianem minimalnym elementu a. Oczywiście $u(a) = 0$ a więc wielomian v dzieli wielomian u. Wobec tego wielomian v ma w E wszystkie pierwiastki (rozkłada się na iloczyn czynników liniowych, wszystkie jego czynniki są także czynnikami wielomianu u). Stąd wynika zaś (2) (v rozkłada się i ma wszystkie pierwiastki między sobą różne).

(2)⇒ (3) Jeśli $E = F$ to F jest ciałem rozkładu dowolnego wielomianu $v \in F[\mathbf{x}]$ stopnia pierwszego (oczywiściekażdy taki wielomian jest rozdzielczy). Przypuśćmy więc, że $F \neq E$, niech

$$a_1 \in E - F$$

i niech m_1 będzie wielomianem minimalnym a_1.
Na mocy (ii) wielomian m_1 jest rozdzielczy, jeśli więc ciało rozkładu E_1 wielomianu v jest równe, dowód jest zakończony. Przypuśćmy więc, że istnieje element

$$a_2 \in E - E_1$$

i niech $m_2 \in F[\mathbf{x}]$ będzie wielomianem minimalnym elementu a_2. Znowu wykorzystujemy (2): wielomian m_2 jest rozdzielczy, bo ma w E pierwiastek i jest nad F nierozkładalny.
Niech E_2 będzie ciałem rozkładu wielomianu $m_1 \cdot m_2$. Wielomian $m_1 \cdot m_2$ jest nad E_2 rozdzielczy i rozkłada się w $E_2[\mathbf{x}]$, a więc E_2 jest ciałem rozkładu wielomianu rozdzielczego $m_1 \cdot m_2 \in F[\mathbf{x}]$. Oczywiście mamy także $F \subset E_1 \subset E_2 \subset E$.
Jeśli $E_2 = E$ to dowód zakończyliśmy, jeśli nie to kontynuujem w podobny sposób konstruując następne rozszerzenia będące ciałami rozkądów kolejnych wielomianów rozdzielczych z $F[\mathbf{x}]$. Ponieważ rozszerzenie $E : F$ jest skończone a w każdym kroku otrzymujemy rozszerzenie, powiedzmy E_i, $F \subset E_i \subset E$, którego wymiar $[E_i : F]$ jest co najmniej jeden większy niż wymiar rozszerzenia poprzedniego $E_{i-1} : F]$ proces ten musi się zakończyć po skończonej liczbie kroków.

(3)⇒(1) Załóżmy teraz, że E jest ciałem rozkładu wielomianu rozdzielczego nad F (czyli: o współczynnikach w F). Na mocy wniosku 12.16 mamy

$$|\mathrm{Gal}(E : F)| = [E : F]$$

Oczywiście zachodzi ciąg zawierań: $E \supset E_G \supset F$. Na mocy twierdzenia 12.22 Dedekinda-Artina

$$[E : E_G] = |G|$$

i ostatecznie $E_G = F$ (inaczej: $G^\dagger = F$) co oznacza, że $E : F$ jest rozszerzeniem Galois. ■

12.6.1 Wnioski z twierdzenia o skończonym rozszerzeniu Galois

Twierdzenie 12.27 o skończonym rozszerzeniu Galois podaje warunki równoważne by ciało skończone było ciałem Galois. Wygodnie będzie nam korzystać z przedstawionych poniżej wniosków z tego twierdzenia.
W dowodzie implikacji (1)⇒(2) twierdzenia 12.27 wykazaliśmy, że jeśli E jest rozszerzeniem skończonym i Galois ciała F, to jest także rozszerzeniem rozdzielczym. Zapiszmy to w postaci wniosku.

Wniosek 12.28 *Jeśli E jest rozszerzeniem skończonym Galois ciała F to jest także rozszerzeniem rozdzielczym.* ■

Oczywistym jest wniosek następujący.

Wniosek 12.29 *Każde rozszerzenie skończone i Galois ciała F jest ciałem rozkładu pewnego wielomianu $v \in F[\mathbf{x}]$.* ■

Wniosek 12.30 *Jeśli $E : F$ jest rozszerzeniem skończonym i Galois to*

$$[E : F] = |G| \tag{12.18}$$

Dowód. Rzeczywiście, skoro $E : F$ jest rozszerzeniem Galois mamy $E_G = F$ ($G = \mathrm{Gal}(E : F)$). Z twierdzenia Dedekinda-Artina otzymujemy (12.18). ■

Wniosek 12.31 *Jeśli $E : K$, $K : F$ i E jest skończonym rozszerzeniem Galois ciała F to E jest także rozszerzeniem Galois ciała K.*

Dowód. Na mocy twierdzenia 12.27, rozszerzenie skończone $E : F$ jest rozszerzeniem Galois wtedy i tylko wtedy gdy jest ciałem rozkładu pewnego wielomianu rozdzielczego $v \in F[\mathbf{x}]$.
W naszym przypadku $E : F$ jest rozszerzeniem skończonym Galois a więc E jest ciałem rozkładu wielomianu rozdzielczego $v \in F[\mathbf{x}]$. Wtedy jednak $v \in K[\mathbf{x}]$ i v jest rozdzielczy nad K, co oznacza, że $E : K$ jest rozszerzeniem Galois. ■

Wniosek 12.32 *Jeśli E jest rozszerzeniem ciała K i K jest rozszerzeniem skończonym Galois ciała F oraz $g \in Gal(E : F)$ to $g(K) = K$ (to oznacza, że g jest automorfizmem $K : F$ lub inaczej: $g_{|K} \in Gal(K : F)$).*

Dowód. Niech $a \in K$ i niech $v \in F[\mathbf{x}]$ będzie wielomianem minimalnym a (nad F). Niech $g \in \mathrm{Gal}(E : F)$. Mamy

$$v(g(a)) = g(v(a)) = g(0) = 0$$

(przy czym pierwsza z powyższych równości zachodzi dlatego, że g ustala elementy ciała F, a więc wszystkie współczynniki wielomianu v).
Tak więc $g(a)$ jest pierwiastkiem v. Na mocy twierdzenia 12.27 (część (2)) v ma wszystkie pierwiastki w K (K jest rozszerzeniem *skończonym i Galois* ciała F). A więc $g(a) \in K$, czyli wykazaliśmy, że $g(K) \subset K$.
Zauważmy teraz, że jeśli $g \in \mathrm{Gal}(E : F)$ to także $g^{-1} \in \mathrm{Gal}(E : F)$ (rzeczywiście, automorfizmy są odwracalne, co więcej, jeśli g ustala ciało F to g^{-1} także ustala ciało F). Powtarzają powyższe rozumowanie dla g^{-1} otrzymamy, że $g^{-1}(K) \subset K$ a stąd $K \subset g(K)$, co kończy dowód. ■

Mówimy, że ciało pośrednie K rozszerzenia $E : F$ jest **stabilne** w rozszerzeniu $E : F$ jeśli

$$g(K) = K \text{ dla każdego automorfizmu } g \in \mathrm{Gal}(E : F) \tag{12.19}$$

Podobnie jak to widzieliśmy w dowodzie wniosku 12.32, także tu można wykorzystać fakt, że $g \in \mathrm{Gal}(E : F)$ wtedy i tylko wtedy gdy g^{-1}ßGal$(E : F)$ do wykazania, że warunek (12.19) jest równoważny warunkowi

$$g(K) \subset K \quad \text{dla każdego } g \in \mathrm{Gal}(E : F) \tag{12.20}$$

Fakt 12.33 *Niech $E : F$, $G = Gal(E : F)$. Jeśli $H \rhd G$ wówczas ciało $H^\dagger$ jest stabilne w $E : F$.*

Dowód. Mamy wykazać, że jeśli $H \rhd G$ wówczas ciało $H^\dagger$ jest stabilne czyli, zgodnie z warunkiem (12.20), że dal każdego automorfizmu $g \in G$ i dla każdego $b \in g(H^\dagger)$ mamy $b \in H^\dagger$ (czyli $h(b) = b$ dla dowolnego $h \in H$). Weźmy więc element $b = h(a)$, $a \in H^\dagger$. Stąd (i z definicji $H^\dagger$ mamy $h(a) = a$ dla dowolnego $h \in H$.
Ponieważ podgrupa H, z założenia, jest podgrupą normalną grupy G, mamy

$$g^{-1}hg \in H$$

a więc $g^{-1}hg(a) = a$. Stąd

$$hg(a) = g(a)$$

co oznacza, że $g(a) \in H^\dagger$. ■

Fakt 12.34 *Niech $E : F$, $G = Gal(E : F)$. Jeśli K jest stabilnym ciałem pośrednim w rozszerzeniu $E : F$ wówczas K° jest podgrupą normalną G i grupa ilorazowa G/K° jest izomorficzna z*

$$\{g \in Gal(K : F) : \text{ istnieje rozszerzenie } g \text{ do automorfizmu } E\}$$

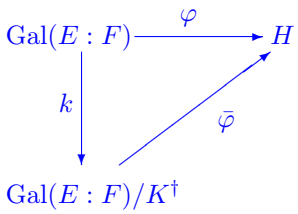
Dowód. K jest ciałem stabilnym w $E : F$, to znaczy $g(K) = K$ dla dowolnego $g \in G$ Oczywiście wtedy $g_{|K}$ jest automorfizmem ustalającym F, czyli $g_{|K} \in \mathrm{Gal}(K : F)$.
Zdefiniujmy przez φ odwzorowanie $\mathrm{Gal}(E : F) \to \mathrm{Gal}(K : F)$ wzorem

$$\varphi(g) = g_{|K}$$

(inaczej: $\varphi(g)$ jest zacieśnieniem g do K.
φ jest oczywiście homomorfizmem grup. Jądrem tego homomorfizmu jest

$$\operatorname{Ker}\varphi = \{g \in G | g_{|K} 0 = \mathrm{id}_K\} = K^\dagger$$

(bo id_K jest elementem neutralnym grupy $\mathrm{Gal}(K : F)$). Sytuacja jest więc jak na poniższym diagramie.



Poszukiwany przez nas izomorfizm

$$\mathrm{Gal}(E : F)/K^\dagger \longrightarrow \mathrm{Gal}(K : F)$$

to $\bar{\varphi}$, którego istnienie zapewnia twierdzenie o izomorfizmie grup 2.33 (str. 37). ■

12.6.2 Zasadnicze twierdzenie teorii Galois

Następujące twierdzenie powszechnie bywa nazywane zasadniczym twierdzeniem teorii Galois.

Twierdzenie 12.35 *Niech E będzie skończonym rozszerzeniem Galois ciała F. Wówczas*

1. *Dla każdego ciała pośredniego K rozszerzenie $E : K$ jest także rozszerzeniem Galois.*
2. *Dla każdego ciała pośredniego K*

$$K^{\circ\dagger} = K$$

(inaczej: ciało K jest domknięte).
Dla każdej podgrupy $H \leq Gal(E : F)$

$$H^{\dagger\circ} = H$$

(grupa H jest domknięta).
Odwzorowania $\circ : K \to K^\circ$ i $\dagger : H \to H^\dagger$ są wzajemnie odwrotne i odwracające zawierania zbiorów, odpowiednio, podciał pośrednich $E : F$ i podgrup grupy $Gal(E : F)$.

3. *Jeśli K_1 i K_2 są ciałami pośrednimi, $K_2 : K_1$ to $[K_2 : K_1] = |K_1^\dagger : K_2^\dagger|$.*
4. *Jeśli $H_1 \leq H_2 \leq Gal(E : F)$ to $|H_2 : H_1| = [H_1^\dagger : H_2^\dagger]$.*
5. *Następujące stwierdzenia są równoważne:*
   (a) *$K : F$ jest rozszerzeniem Galois*
   (b) *K jest podciałem stabilnym w $E : F$ (czyli $g(K) = K$ dla każdego $g \in Gal(E : F)$)*
   (c) *$K^\circ \lhd Gal(E : F)$*
6. *Jeśli $K : F$ jest rozszerzeniem Galois (lub, równoważnie, $K^\circ \lhd Gal(E : F)$) wówczas $G/K^\circ \sim Gal(K : F)$ (grupy $Gal(K : F)$ i ilorazowa G/K° są izomorficzne).*

Dowód części 1 twierdzenia. Część 1. twierdzenia to dokładnie wniosek 12.31.

Dowód części 2 twierdzenia. Fakt, że operacje $\circ$ i $\dagger$ odwracają zawierania jest prosty i został wykazany jako twierdzenia 12.23 i 12.24. Pozostaje więc udowodnić, że każde ciało pośrednie rozszerzenia $E : F$ i każda podgrupa grupy $\mathrm{Gal}(E : F)$ są domknięte a więc, że

$$K^{\circ\dagger} = K \quad \text{i} \quad H^{\dagger\circ} = H$$

jeśli $E : K$, $K : F$ oraz $H \leq \mathrm{Gal}(E : F)$. Rzeczywiście, na mocy definicji K°, dla dowolnego $h \in K$ i $h \in K^\circ$ zachodzi $h(a) = a$. Wobec tego, jeśli $a \in K$ wtedy $a \in (K^\circ)^\dagger$. Wykazaliśmy więc, że

$$K \subset K^{\circ\dagger} \tag{12.21}$$

Podobnie, jeśli $h \in H$, to $h(a) = a$ dla każdego $a \in H^\dagger$ a stąd $h \in H^{\dagger\circ}$. A więc mamy zawieranie:

$$H \subset H^{\dagger\circ} \tag{12.22}$$

Teraz wykażemy, że

$$K^{\circ\dagger\circ} = K^\circ \quad \text{i} \quad H^{\dagger\circ\dagger} = H^\dagger$$

Rzeczywiście, skoro $K \subset K^{\circ\dagger}$ (na mocy (12.21) i - jak już stwierdziliśmy - operacja $\circ$ odwraca zawierania, otrzymujemy $K^{\circ\dagger\circ} \subset K^\circ$. Podobnie ze wzoru (12.22) i faktu, że $\dagger$ odwraca zawierania otrzymujemy $H^{\dagger\circ\dagger} \subset H^\dagger$.
Dla dowolnego ciała pośredniego L właśnie udowodniliśmy zawieranie $L^{\circ\dagger} \supset L$. Wstawiając $L = H^\dagger$ do tej relacji otrzymujemy

$$H^{\dagger\circ\dagger} = (H^\dagger)^{\circ\dagger} \supset H^\dagger$$

a więc, ostatecznie $H^\dagger = H^{\dagger\circ\dagger}$.
Korzystając teraz dwukrotnie (w pierwszej i ostatniej z poniższych równości) z twierdzenia Dedekinda-Artina, otrzymamy

$$|H^{\dagger\circ}| = [E : H^{\dagger\circ\dagger}] = [E : H^\dagger] = |H|$$

i w konsekwencji

$$H = H^{\dagger\circ}$$

Teraz wykażemy, że $K = K^{\circ\dagger}$.
Oznaczmy przez $\tilde{H} = \mathrm{Gal}(E : K)$. Na mocy części 1. twierdzenia $E : K$ jest rozszerzeniem Galois, czyli

$$K = \{a \in E | g(a) = a \text{ dla każdego automorfizmu } g \in \tilde{H}\} = \tilde{H}^{\dagger}$$

Z już udowodnionego $H^{\dagger\circ\dagger} = H^{dag}$ dla każdej podgrupy $H \leq \mathrm{Gal}(E, F)$ otrzymujemy

$$K^{\circ\dagger} = \tilde{H}^{\dagger\circ\dagger} = \tilde{H}^{\dagger} = K$$

Dowód części 3 twierdzenia. Jeśli $K_2 : K_1$ wówczas, na mocy części 1. twierdzenia $E : K_2$ jest rozszerzeniem Galois a więc, z wniosku 12.30 mamy

$$[E : K_2] = |\mathrm{Gal}(E : K_2)| = |K_2^{\circ}|$$

Podobnie

$$[E : K_1] = |K_1^{\circ}|$$

Stąd zaś otrzymujemy

$$[K_2 : K_1] = \frac{[E : K_1]}{[E : K_2]} = \frac{|K_1^{\circ}|}{|K_2^{\circ}|} = |K_1^{\circ}/K_2^{\circ}|$$

Dowód części 4 twierdzenia. Na mocy części 2. twierdzenia (operacja $\dagger$ odwraca zawierania) mamy $H_1^{\dagger} \subset H_2^{\dagger}$. Stąd i na podstawie części 2. twierdzenia mamy

$$H_1^{\dagger\circ} = H_2 \quad \text{i} \quad H_2^{\dagger\circ}$$

a więc

$$|H_2 : H_1| = |(H_2^{\dagger})^{\circ} : (H_2^{\dagger})^{\circ}| = [H_1^{\dagger} : H_2^{\dagger}]$$

Dowód części 5 twierdzenia.

- Jeżeli $K : F$ jest rozszerzeniem Galois wówczas, na mocy wniosku 12.32 podciało K jest stabilne (to znaczy $g(K) = K$ dla każdego $g \in \mathrm{Gal}(E : F)$).
- Przypuśćmy teraz, że K jest podciałem stabilnym i $a \in K - F$. Skoro rozszerzenie $E : F$ jest Galois, istnieje $g \in \mathrm{Gal}(E : F)$ takie, że $g(a) \neq a$ - a to oznacza, że rozszerzenie $K : F$ jest Galois.
- Jeśli podciało K jest stabilne to $K^{\circ} \lhd \mathrm{Gal}(E : F)$ na mocy faktu 12.34. Wynikanie w przeciwną stronę to fakt 12.33.

Dowód części 6 twierdzenia. Fakt 12.34.

■

Ciała skończone

Twierdzenie 12.36 *Niech $E = G\mathbb{F}(p^n)$, gdzie p jest liczbą pierwszą. Wówczas $E : \mathbb{Z}_p$ jest rozszerzeniem Galois i ciałami pośrednimi są te ciała $G\mathbb{F}(p^m)$, dla których $m|n$.*

Dowód. Rząd dowolnego elementu a w multyplikatywnej grupie $\mathrm{G}\mathbb{F}(p^n)^*$ dzieli $|\mathrm{G}\mathbb{F}(p^n)^*| = p^n - 1$. Stąd

$$a^{p^n-1} = 1$$

i wobwc tego dla każdego elementu $b \in \mathrm{G}\mathbb{F}(p^n)$ mamy

$$b^{p^n} - b = a$$

A więc każdy element ciała $\mathrm{G}\mathbb{F}(p^n)$ jest pierwiastkiem wielomianu

$$v = \mathbf{x}^{p^n} - \mathbf{x}$$

Ponieważ na dodatek $v' = p^n\mathbf{x}^{p^n-1} - 1 = -1 \neq 0$ (pamiętamy, że $\mathrm{G}\mathbb{F}(p^n)$ jest rozszerzeniem ciała $\mathbb{Z}_p$), wielomian v jest rozdzielczy[8].

Na mocy twierdzenia **??** część (3), $\mathrm{G}\mathbb{F}(p^n)$ jest rozszerzeniem Galois Z_p. Pamiętamy, że grupa $\mathrm{G}\mathbb{F}(p^n)^*$ jest cykliczna. Wynika stąd, że

$$\mathrm{G}\mathbb{F}(p^n) = \mathbb{Z}(a)$$

gdzie a jest generatorem grupy $\mathrm{G}\mathbb{F}(p^n)^*$. Wielomian minimalny m elementu a jest oczywiście stopnia n i

$$[\mathrm{G}\mathbb{F}(p^n) : \mathbb{Z}_p] = n$$

Niech K będzie ciałem pośrednim. Oczywiście K jako podciało ciała skończonego jest skończone i oczywiście zawiera $1 \in \mathbb{Z}_p$, a więc zawiera $\mathbb{Z}_p$ i st'ad $K = \mathrm{G}\mathbb{F}(p^m)$. Podobnie jak poprzednio łatwo jest sprawdzią, że $[K : \mathbb{Z}_p] = m$.
Na mocy części 5. i 6. zasadniczego twierdzenia teorii Galois mamy

$$\mathrm{Gal}(K : \mathbb{Z}_p) \lhd \mathrm{Gal}(\mathrm{G}\mathbb{F}(p^n) : \mathbb{Z}_p)$$

a więc $m|n$. ∎

[8] To samo można udowodnić inaczej. v jest wielomianem stopnia p^n i ma p^n pierwiastków, którymi są wszystkie elementy $\mathrm{G}\mathbb{F}(p^n)$. Wobec tego pierwiastki v są różne między sobą.

12.7 Zadania

Zadanie 12.1 Udowodnij twierdzenie 12.13.

Zadanie 12.2 Niech $E : F$ będzie rozszerzeniem ciała F. Udowodnij, że zbiór automorfizmów $\mathrm{Gal}(E : F)$ z działaniem składania odwzorowań jest grupą.

Zadanie 12.3 Sprawdź, że jeśli $\sigma : P \to \bar{P}$ jest homomorfizmem pierścieni P i $\bar{P}$, to $\tilde{\sigma} : P[\mathbf{x}] \ni v \to \sigma v \in \bar{P}[\mathbf{x}]$ (gdzie σv jest zdefiniowane jak na stronie 176). jest homomorfizmem pierścieni wielomianów a także, że jeśli σ jest monomorfizmem, epimorfizmem lub izomorfizmem, wówczas $\tilde{\sigma}$ jest także, odpowiednio, monomorfizmem, epimorfizmem lub izomorfizmem.

Zadanie 12.4 Udowodnij, że jeśli wielomian minimalny $m \in F[\mathbf{x}]$ elementu a rozkłada się na iloczyn wielomianów stopnia pierwszego nad $F(a)$, wówczas każdy pierwiastek tego wielomianu należy do $F(a)$.

Zadanie 12.5 Udowodnij, że jeśli $E : F$ jest ciałem rozkładu wielomianu $v \in F[\mathbf{x}]$ wówczas dla dowolnego automorfizmu $f \in \mathrm{Gal}(E : F)$ $f_X \in S_X$ oraz, że odwzorowanie T (zdefiniowane w dowodzie twierdzenia 12.10) jest izomorfizmem).

Zadanie 12.6 Udowodnij, że jeśli p jest liczbą pierwszą, to wielomian

$$v_p = 1 + \mathbf{x} + \mathbf{x}^2 + ... + \mathbf{x}^{p-1}$$

jest nad $\mathbb{Q}$ nierozkładalny.

Zadanie 12.7 Wskaż izomorfizm $\mathbb{Z}_2[\mathbf{x}]/ < \mathbf{x}^3 + \mathbf{x}^2 + 1 >$ i $\mathbb{Z}_2[\mathbf{x}]/ < \mathbf{x}^3 + \mathbf{x} + 1 >$.

Zadanie 12.8 Niech p będzie liczbą pierwszą, E ciałem, rozszerzeniem $\mathbb{Z}_p$ $(E : \mathbb{Z}_p)$. Udowodnij, że funkcja

$$f : E \ni s \to s^p \in E$$

jest automorfizmem ciała E ustalającym $\mathbb{Z}_p$ (automorfizm ten jest zwany automorfizmem Frobeniusa).

Zadanie 12.9 Sprawdź prawdziwość stwierdzeń podanych w przykładzie 12.11.

Rozdział 13

Ewaryst Galois

Rozdział 14

Wskazówki do wybranych zadań

14.1 Rozdział 2

Zadanie ??.

14.2 Rozdział 4

Zadanie 4.1. 22 dla szachownicy jednostronnej i 12 dla dwustronnej.

14.3 Rozdział 5

Zadanie 5.17. Oznaczmy $d = \mathrm{NWD}(|\mathrm{G}|, |\mathrm{H}|)$.
Jeśli grupa GH jest cykliczna wówczas istnieją elementy $a \in G, b \in H$ takie, że $|(a,b)| = |GH|$. Z drugiej strony $(a,b)^{|G||H|/d} = ((a^{|G|})^{|H|/d}, (b^{|H|})^{|G|/d}) = (e,e)$. Stąd $|(a,b)| \leq |G||H|/d$. Skoro $|GH| = |G||H|$, mamy $|G||H| = |(a,b)| \leq |G||H|/d$ a więc $d = 1$.
Załóżmy teraz, że $\mathrm{NWD}(|\mathrm{G}|, |\mathrm{H}|) = 1$. i niech a i b będą generatorami, odpowiednio, G i H. Wówczas $|(a,b)| = \mathrm{NWW}(|G|, |H|) = |G||H| = |GH|$, a więc (a,b) generuje GH.

Zadanie ??. Grupy $H_1 =< (1,2,3) >$ i $H_2 =< (1,2) >$ są podgrupami grupy (nieprzemiennej) S_3. Sprawdź, że $H_1 \cap H_2 = \{(1)(2)(3)\}$. Niemniej grupy H_1H_2 i $H_1 \otimes H_2$ nie są izomorficzne.
Rzeczywiście, iloczyn wewnętrzny $H_1 \otimes H_2 = S_3$, natomiast iloczyn prosty H_1H_2 jest cykliczna.

14.4 Rozdział 6

Zadanie 6.9. 5-podgrup Sylowa jest $n_5 \equiv 1 \mod 5$. Skoro $|S_5| = 5! = 120$, każda z nich ma po 5 elementów, są cykliczne, generowane przez permutacje rzędu 5. Takich

permutacji jest $4! = 24$. W każdej 5-podgrupie Sylowa jest identyczność (1) i 4 inne. Przecięcie dowolnych dwóch 5-podgrup Sylowa jest równe $\{(1)\}$, stąd $n_5 = \frac{24}{4} = 6$. Każda 3 podgrupa Sylowa jest generowana przez element rzędu 3, a więc postaci $(abc)(d)(e)$. Takich permutacji jest $\binom{5}{2} \cdot 2! = 20$. W każdej 5-podgrupie Sylowa jest permutacja identycznościowa i dwie inne, a więc wszystkich 5-podgrup Sylowa jest $\frac{20}{2} = 10$. Warto zauważyć, że $10 \equiv 1 \mod 3$, zgodnie z trzecim twierdzeniem Sylowa.

Zadanie 6.8. Należy sprawdzić, czy przyporządkowanie każdemu elementowi $Hb \in G/H$ klasy (Hb) jest dobrze określone a więc, że jeśli $Hb = Hc$ wówczas $(Hb)h^{-1} = (Hc)h^{-1}$ (dla każdego elementu $h \in H$.

Zadanie 6.10. Pierwszy sposób polega na wykorzystaniu wniosku 6.17.
Na mocy trzeciego twierdzenia Sylowa, istnieje tylko jedna 5-podgrupa Sylowa (nazwijmy ją F) i tylko jedna 7-podgrupa Sylowa grupy rzędu 35 (powiedzmy H) grupy G rzędu 35. Niech $x \in G - (F \cup H)$. Oczywiście $|x| = 15$ i wobec tego $G =< x >$.

14.5 Rozdział 7

Zadanie 7.2. Fakt, że $G' \leq G$ jest niemal natychmiastowy, wykażemy więc tylko, że G' jest podgrupą normalną grupy G.
Niech $g \in G, h \in G'$ Wtedy $ghg^{-1} = \underbrace{ghg^{-1}h^{-1}}_{\in G'} h \in G'h = G'$ ponieważ $h \in G'$. ■

Zadanie 7.8. Gdyby istniał element $x \in G'$ taki, że $x \notin H$, mielibyśmy $H \cap Hx = \emptyset$. x jest iloczynem komutatorów $x = a_1b_1a_1^{-1}b_1^{-1} \ldots a_kb_ka_k^{-1}b_k^{-1}$. Skoro grupa G/H jest abelowa mamy:

$$Hx = Ha_1Hb_1Ha_1^{-1}Hb_1^{-1} \ldots Ha_kHb_kHa_k^{-1}Hb_k^{-1} = H$$

- sprzeczność.

Zadanie 7.9. Z zadania 7.8 i twierdzenia 7.2 wynika, że $S_4' \subset A_4$. Skoro $|A_4| = 12$, rząd podgrupy S_4' może wynosić 1, 3, 4 lub 12.

$|S_4'| \neq 1$ bowiem $S_4/\{1\} \simeq S_4$ jest grupą nieprzemienną (pamiętamy (twierdzenie 7.3), że G/G' jest grupą abelową). $|S_4'| \neq 3$. Gdyby podgrupa S_4' była rzędu 3, wówczas S_4' byłaby 3-podgrupą Sylowa. Łatwo jednak zauważyć, że A_4 ma cztery 3-podgrupy Sylowa (każda z nich generowana przez cykliczną permutację rzędu 3). S_4 nie byłoby więc podgrupą normalną A_4. $|S_4'| \neq 4$. Jest tylko jedna podgrupa rzędu 4 grupy A_4, mianowicie $K = \{(1), (12)(34), (13)(24), (14)(23)\}$ bowiem K zawiera wszystkie elementy rzędu 2 grupy A_4 i grupa A_4 nie zawiera elementu rzędu 4. Grupa S/K nie jest abelowa (na przykład $K(1234) \cdot K(1324) \neq K(1324) \cdot K(1234)$).

Zadanie 7.10. Nie. Na przykład grupa S_4 jest rozwiązalna, $S_4' = A_4$ – grupa nieprzemienna.

Zadanie 7.11. Rozpatrzymy 2 przypadki.
Przypadek 1: $p = q$.

Niech G będzie grupą rzędu p^3.
Centrum $Z(G)$ jest podgrupą normalną grupy G a więc $|Z(G)| = p^l$, $l \in \{0,1,2,3\}$.
Na mocy twierdzenia6.8 (każda nietrywialna p-podgrupa ma centrum o co najmniej 2 elementach) $l \neq 0$. Niech $x \in Z(G)$ będzie elementem rzędu p (taki element istnieje na mocy twierdzenia Cauchy'ego, pamiętamy także, że $Z(G)$ jako podgrupa p-grupy jest p-grupą). Podgrupa $< x >$ generowana przez x jest podgrupą normalną grupy G. Mamy ciąg podgrup normalnych:

$$G \rhd < x > \rhd \{1\} \tag{14.1}$$

Skoro $|G/ < x > | = p^2$ i $| < x > /\{1\}| = p$, grupy ilorazowe $G/ < x >$ i $< x > /\{1\}$ są przemienne.
Przypadek 2: $p \neq q$**.**
Przypuśćmy, że $n_p = 1$ lub $n_q = 1$. Wtedy istnieje normalna p-podgrupa lub normalna q-podgrupa H grupy G. Łatwo sprawdzić, że odpowiednim ciągiem jest

$$G \rhd H \rhd \{1\}$$

Przypuśćmy więc, że $n_p > 1$ i $n_q > 1$. Z trzeciego twierdzenia Sylowa $n_p|q$ i $n_p \equiv 1(\mod q)$, a więc $n_q > q$. Ponieważ $q > p$ otrzymujemy, że $n_q = p^2$. W grupie G istnieje więc $n_q(q-1) = p^2(q-1) = p^2q - p^2$ elementów rzędu q.
Elementów rzędu podzielnego przez p może być więc co najwyżej $p^2q-(p^2q-p^2)-1 = p^2-1$ a więc dokładnie tyle, ile w jednej podgrupie rzędu p^2, mielibyśmy więc $n_p = 1$, a to jest sprzeczne z przypuszczeniem, że $n_p > 1$.

Zadanie 7.12. Dowód przeprowadzimy przy pomocy indukcji matematycznej. Jeśli $|G| = p$, wówczas G jest przemienna, a więc rozwiązalna.
Przypuśćmy, że $n > 1$ i każda grupa rzędu p^k, gdzie $1 \leq k < n$ jest rozwiązalna. Niech $|G| = p^n$. Jeśli G jest abelowa, twierdzenie jest prawdziwe (zadanie 7.4).
Jeśli G nie jest przemienna, wówczas $|Z(G)| \geq 2$ i wobec tego $Z(G) \neq \{1\}$. Mamy także $Z(G) \lhd G$.
Z założenia indukcyjnego grupy $Z(G)$ oraz $G/Z(G)$ są rozwiązalne, a więc także G jest rozwiązalna (twierdzenie 7.9).

14.6 Rozdział 8

Zadanie 8.10. Pierścień ilorazowy $\mathbb{Z}[\mathbf{x}] :< 3+i >$ ma 10 elementów:

$$< 3+i >, 1+ < 3+i >, ..., 9+ < 3+i >$$

Uzasadnienie. $10 = (3+i)(3-i) \in < 3+i >$.
Mamy także $i+ < 3+i >= -3+ < 3+i >= 7+ < 3+i >$.
Element $1+ < 3+i >$ jest rzędu 10 w $\mathbb{Z}[i] :< 3+i >$ a każdy element w $\mathbb{Z}[i] :< 3+i >$ można zapisać w następujący sposób:
$a+ib+ < 3+i >= (a+ < 3+i >) + b(7+ < 3+i >) = (a+7b)+ < 3+i >$.

Na przykład $15+12i+ < 3+i >= (15+84)+ < 3+i >= 99+ < 3+i >= 9+ < 3+i >$.

Zadanie 8.12. Przypuśćmy, że Ker $f = \{0\}$. Jeśli $f(a) = f(b)$ to $0 = f(a) - f(b) = f(a-b)$. Wobec tego $a - b \in$ Ker f a stąd $a - b = 0$. W konsekwencji $a = b$, skąd wynika, że f jest monomorfizmem.
Z drugiej strony, dla dowolnego homomorfizmu pierścieni f mamy $f(0) = f(0+0) = f(0) + f(0)$ i wobec tego $f(0) = 0$. Jeśli f jest monomorfizmem, wówczas w jądrze nie może być, poza zerem pierścienia P, żadnego innego elementu.

14.7 Rozdział 11

Zadanie 11.13. Wskazówka (do zad. (a) i (b), inne podobnie).
(a) Udowodnimy, że $\sqrt[3]{\pi^2}$ jest elemtem przestępnym nad $\mathbb{Q}$ (czyli liczbą przestępną). Niech F będzie dowolnym ciałem. Dla każdego elementu $a \in E : F$ mamy $a^3 \in F(a)$. Stąd i na mocy twierdzenia z wykładu (chodzi tu o twierdzenie, które mówi, że jeśli a jest el. algebraicznym nad F to każdy el. $b \in F(a)$ jest także algebraiczny nad F), gdyby $\sqrt[3]{\pi^2}$ było elementem algebraicznym nad $\mathbb{Q}$ (czyli liczbą algebraiczną), wówczas $(\sqrt[3]{\pi^2})^3 = \pi^2$ byłoby liczbą algebraiczną. Wówczas istniałby wielomian $v = a_0 + ... + a_n\mathbf{x}^n \in \mathbb{Q}[\mathbf{x}]$ taki, którego pierwiastkiem jest π^2. Wtedy π byłoby pierwiastkiem wielomianu $w = \sum_{k=0}^{2n} b_k\mathbf{x}^k$, gdzie

$$b_k = \begin{cases} 0 & \text{dla } k \text{ nieparzystych,} \\ a_{k/2} & \text{dla } k \text{ parzystych.} \end{cases}$$

(b) $a = \sqrt[3]{\pi^2}$ jest elementem algebraicznym nad $\mathbb{Q}(\pi)$, bowiem jest pierwiastkiem wielomianu $\mathbf{x}^3 - \pi^2 \in \mathbb{Q}(\pi)$.

14.8 Rozdział 12

Zadanie 12.6.

Sposób 1. Wykażemy wpierw, że wielomian $v_p(\mathbf{x}+1)$ jest nierozkładalny. Rzeczywiście jeśli $v_p(\mathbf{x}+1)$ jest nierozkładalny, to i v_p także jest nierozkładalny (gdyby v_p był rozkładalny to mielibyśmy $v_p = u \cdot w$ $(u, w \in \mathbb{Q}[\mathbf{x}])$ i wtedy $v_p(\mathbf{x}+1) = u(\mathbf{x}+1) \cdot w(\mathbf{x}+1)$ - czyli $v_p(\mathbf{x}+1)$ byłby rozkładalny, sprzeczność).
Mamy teraz

$$(\mathbf{x}-1)v_p = \mathbf{x}^p - 1$$

stąd

$$\mathbf{x}v_p(\mathbf{x}+1) = (\mathbf{x}+1)^p - 1$$

i wobec tego

$$\begin{aligned} \mathbf{x}v_p(\mathbf{x}+1) &= \mathbf{x}^p + \tbinom{p}{1}\mathbf{x}^{p-1} + ... + \tbinom{p}{p-2}\mathbf{x}^2 + p\mathbf{x} \\ &= \mathbf{x}(\mathbf{x}^{p-1} + \tbinom{p}{1}\mathbf{x}^{p-2} + ... + \tbinom{p}{p-2}\mathbf{x} + p) \end{aligned}$$

Nietrudno teraz zauważyć, że $v_p(\mathbf{x}+1)$ jest nierozkładalny na mocy kryterium Eisensteina.

Sposób 2. dopisać lub powtórzyć podobne zadanie dla $v = \mathbf{x}^p - 2$ (zamiast 2 może być 3 lub cokolwiek)

Zadanie 12.8.

f **jest homomorfizmem** $E \to E$**.** Rzeczywiście,

$$f(s+t) = (s+t)^p = \sum_{l=0}^{p} \binom{p}{p-l} s^{p-l}t^l = s^p + t^p$$

pamiętamy bowiem, że w każdym z czynników $\binom{p}{p-l}$ (poza pierwszym i ostatnim, dla $l = 0$ i $l = p$) występuje p i w związku z tym czynniki te znikają.

$$f(s \cdot t) = (s\dot{t})^p = s^p t^p = f(s)f(t)$$

f **jest monomorfizmem.** Ker $f = \{0\}$ bowiem jeśli $s^p = 0$ wówczas $s = 0$ (E jest ciałem, nie ma więc dzielników zera).
Skoro f jest monomorfizmem zbioru skończonego w siebie, musi być także epimorfizmem a więc jest automorfizmem. Co więcej, dla $s \in \mathbb{Z}_p$ mamy $s^p = s$ z małego twierdzenia Fermata.

Rozdział 15

Oznaczenia

Symbol	**Nazwa**	**strona**
$\lfloor a \rfloor$	podłoga liczby $a \in \mathbb{R}$	12
$\lceil a \rceil$	sufit liczby $a \in \mathbb{R}$	12
$C(a)$	centralizator elementu a grupy	??
$C(H)$	centralzator podgrupy H (gdy $H \leq G$)	??
C_n	grupa obrotów właściwych n-kąta foremnego	??
char (P)	charakterystyka pierścienia P	114
D_n	grupa dihedralna	??
$E : F$	rozszerzenie E ciała F (czyt. także: ciało E jest rozszerzeniem ciała F)	147
$F(X)$	ciało generowane przez zbiór X (i ciało F)	147
$F(a_1, ..., a_n)$	ciało generowane przez elementy $a_1, ..., a_n$ i ciało F	147
$G^\dagger$ (lub E_G)	ciało ustalone przez grupę G	192
Gal$(E : F)$	grupa Galois rozszerzenia $E : F$	175
G$\mathbb{F}(q)$	ciało Galois rzędu q	163
G$\mathbb{F}^*(q)$	grupa elementów różnych od zera w G$\mathbb{F}(q)$	??
$H \leq G$	H jest podgrupą grupy G	23
$H \lhd G$	H jest podgrupą normalną grupy G	??
$< g >$	grupa generowana przez element a	27
$H_1 \oplus H_2 \oplus ... \oplus H_k$	iloczyn prosty grup $H_1, H_2, ..., H_k$	??
$H_1 \otimes H_2 \otimes ... \otimes H_k$	iloczyn wewnętrzny grup $H_1, H_2, ..., H_k$	69
Ker h	jądro homomorfizmu grup h	43
$\simeq$	izomorficzne	
$\mathbb{N}$	zbiór liczb naturalnych $\{0, 1, 2, ...\}$	
$\mathbb{N}^*$	zbiór liczb całkowitych dodatnich $(\mathbb{N} - \{0\})$	
$N_G(H)$	normalizator podgrupy H	39
$L : K$	rozszerzenie L ciała K	147
σv	rozszerzenie homomorfizmu pierścieni na homomorfizm pierścieni wielomianów	176, 203
$Z(G)$	centrum grupy G	??

Bibliografia

[1] M. Aigner i G.M. Ziegler, Dowody z Księgi, PWN, Warszawa 2002.

[2] A. Białynicki-Birula, Algebra, PWN, Warszawa 1980.

[3] G. Birkhoff i S. Mac Lane, Przegląd algebry współczesnej, PWN, Warszawa 1963.

[4] G. Birkhoff i S. Mac Lane, Algèbre, Gauthier-Villars, Paryż 1971.

[5] G. Birkhoff i T.C. Bartee, Współczesna algebra stosowana, PWN, Warszawa 1983.

[6] G. Bobiński, Algebra, www-users.mat.umk.pl/ gregbob/old/algebra/ lecture2003.pdf

[7] R. Courant i H. Robbins, Co to jest matematyka? Prószyński i S-ka, Warszawa 1998.

[8] D.A. Cox, Galois theory, Wiley 2004.

[9] É. Galois, Écrits et mémoires d'Évariste Galois, wyd. R. Bourgne i J.-P. Azra, Gauthier-Vilars, Paryż 1962.

[10] W.J Gilbert, W.K. Nicholson, Algebra współczesna z zastosowaniami, WNT, Warszawa 2008.

[11] D.W. Hardy i C.L. Walker, Applied Algebra: Codes, Ciphers and Discrete Algorithms, Prentice Hall 2003.

[12] N. Koblitz, Algebraiczne aspekty kryptografii, WNT, Warszawa 2000.

[13] M. Kordos, Wykłady z historii matematyki, SCRIPT, Warszawa 2005.

[14] A.I. Kostrykin, Wstęp do algebry, cz. 1 Podstawy algebry, PWN Warszawa 2004.

[15] A.I. Kostrykin, Wstęp do algebry, cz. 3 Podstawowe struktury algebraiczne, PWN Warszawa 2005

[16] W.K. Nicholson, Introduction to Abstract Algebra, Third Edition, Wiley 2007.

[17] Z. Opial, Algebra wyższa, PWN, Warszawa 1975.

[18] J. Rutkowski, Algebra abstrakcyjna w zadaniach, PWN Warszawa 2006.

[19] E.R. Scheinerman, Mathematics - Discrete Introduction, Brooks/Cole 2000.

[20] W. Sierpiński, Zasady algebry wyższej, Monografie Matematyczne, Warszawa-Wrocław 1946.

[21] I. Stewart, Galois Theory, Chapman and Hall Mathematics, Londyn, Nowy York 1989.

[22] K. Szymiczek, Algebra, UŚ 2010:
http://www.math.us.edu.pl/zatl/szymiczek/referaty/AlgebraSD.pdf

[23] K. Szymiczek, Zbiór zadań z teorii grup, PWN 1989.

[24] H. Weil, Symetria, PWN, Warszawa 1960.

Indeks

p-podgrupa, 81
p-podgrupa Sylowa, 81

addytywny rząad elementu pierścienia, 114
algorytm, 16
algorytm Euklidesa, 16
antymorfizm grafu, 89
automorfizm ciala, 175
automorfizm Frobeniusa, 203
automorfizm ustalający ciało, 175

bryła platońska, 60
bryły foremne, 60
Burnside W., 63

Cauchy, 70
centralizator elementu grupy, 40, 44
centrum grupy, 40
charaktery, 190
charaktery niezależne, 190
charakterystyka pierścienia, 114
cialo, 105
cialo stabilne, 198
cialo ulamkow, 130
ciało skończone, 188
ciało, 129
ciało algebraicznie zamkniete, 152
ciało domknięte, 195
ciało Galois, 163
ciało pośrednie, 190, 193
ciało skończone, 163
ciało ustalone prez grupę, 192
ciało ustalone przez grupę, 192

Dedekind, 163, 190
Dirichlet, 163
drugie twierdzenie Sylowa, 84
dzailanie addytywne, 105
dzialanie grupy na zbiorze, 59
dzialanie multyplikatywne, 105
dzielnik zera, 42
dzielniki zera, 105

element algebraiczny, 155
element neutralny, 19
element nierozkladalny, 112
element odwrotny, 19
element pierwszy, 112
element prymitywny rozszerzenia, 148
epimorfizm grup, 24
epimorfizm pierścieni, 110
Eratostenes, 21
Euklides, 11, 16
Euler, 12, 21
Eulera funkcja, 21

Fermat, 45
formula sita, 21
Frobenius, 81
Frobenius F.G., 63

Galois E., 205
Gauss, Carl Friedrich, 119
generator grupy, 27
graf, 88
grupa, 19
grupa abelowa, 19
grupa addytywna, 19
grupa alternujaca, 41
grupa automorfizmów grafu, 89
grupa cykliczna, 26, 27
grupa dihedralna, 33
grupa dzialajaca na zbiorze, 59
grupa Galois, 175

grupa ilorazowa, 36
grupa Kleina, 25
grupa multiplikatywna, 19
grupa obrotow szescianu, 67
grupa obrotow wlasciwych, 24
grupa permutacji, 19
grupa pochodna, 97
grupa przemienna, 19
grupa rozwiązalna, 95
grupa skonczona, 21
grupa transformacji, 29
grupy izomorficzne, 25
grupy rozwiazalne, 95

homomorfizm grup, 24
homomorfizm kanoniczny, 37
homomorfizm pierścieni, 109

ideal, 107
ideal glowny, 109
ideał, 107
identyfikacjia grup izomorficznych, 25
iloczyn prosty wewnetrzny grup, 69
iloczyn prosty zewnetrzny grup, 69
iloraz, 15
izomorfizm grup, 24
izomorfizm pierścieni, 110

jądro homomorfizmu grup, 37
jądro homomorfizmu pierścieni, 110

komutant, 97
komutator, 97
krawedz grafu, 88
Kronecker, L., 70
krotność pierwiastka wielomianu, 164
krotnosc, 26
kryterium Eisensteina, 135
kwaterniony, 76

lemat Burnside'a, 63
lemat Dedekinda, 190
lemat-gaussa, 132
liczba algebraiczna, 155
liczby pierwsze, 11
liczby wzglednie pierwsze, 17

Male Twierdzenie Fermata, 45
monomorfizm grup, 24
monomorfizm pierścieni, 110
Muzychuk M., 88

najwiekszy wspolny dzielnik, 15
normalizator podgrupy, 39

odwzorowanie addytywne pierścieni, 109
orbita, 61

pierścień ilorazowy, 108
pierscien, 105
pierscien bez dzielnikow zera, 105
pierscien clkowity, 105
pierscien Dedekinda, 113
pierscien Gaussa, 119
pierscien przemienny, 105
pierscien z jedynka, 105
pierscien z rozkladem, 119
pierwsze twierdzenie o izomorfizmie grup, 37
pierwsze twierdzenie Sylowa, 79
pochodna wielomianu, 164
podciało, 129
podgrupa, 23
podgrupa niezmiennicza, 35
podgrupa normalna, 35
podloga liczby rzeczywistej, 12
podpierścień, 107
podpierscień, 107
podstawowe twierdzenie o homomorfizmie grup, 37
Podstawowe Twierdzenie o Izomorfizmie Grup, 37
podstawowe twierdzenie o izomorfizmie grup, 36, 37
podstawowe twierdzenie o wielomianach symetrycznych, 142
potega elementu, 26
prawa skracania, 106
prawostronna warstwa modulo podgrupa, 31
przystawanie modulo ideal, 108
przystawanie modulo polgrupa, 30

relacja przystawania modulo, 106
reszta, 15
rozklad na czynniki, 112
rozklad wasciwy, 112
rozklady jednakowe, 119
rozszerzenie cial, 147
rozszerzenie Galois, 194
rozszerzenie nieskończone, 155
rozszerzenie proste, 148
rozszerzenie rozdzielcze ciała, 184
rozszerzenie skoncone, 155
rząd elementu pierścienia, 114
rzad elementu grupy, 27
rzad grupy, 21

sprzerenie podgrupy, 38
sprzerenie podzbioru grupy, 38
sprzezenie elementu grupy, 38
stabilizator, 60
stopien wielomianu, 121
sufit liczby rzeczywistej, 12
Sylow, 79

tabela Cayleya, 25
Trzecie Twierdzenie o izomorfizmie Grup, 100
twierdzenia o izomorfizmie grup, 99
twierdzenie Cantora, 163
twierdzenie Cauchy'ego, 81
Twierdzenie Cauchyego dla skonczonych grup abelowych, 70
twierdzenie Cayleya, 29
twierdzenie Dedekinda-Artina, 192
twierdzenie Kroneckera, 150
twierdzenie Lagrange'a, 30
twierdzenie Muzychuka, 88
twierdzenie o ciele rozkładu, 150
twierdzenie o dzileniu liczb calkowitych, 14
twierdzenie o elemencie prymitywnym, 187
twierdzenie o grupie Galois rozszerzenia skończonego, 179
twierdzenie o iloczynie wymiarów, 159
twierdzenie o izomorfizmie pierścieni, 110
twierdzenie o orbicie i stabilizatorze, 61
twierdzenie o rozkladzie na orbity, 82
twierdzenie o rozszerzeniach skończonych, 178
twierdzenie o rozszerzeniach skonczonych, 158
twierdzenie o wieży, 159
twierdzenie o wielomianie minimalnym, 156
twierdzenie Sylowa, 79, 84
twierdzenie Wilsona, 141

wielomian rozdzielczy, 184
wielomian unormowany, 156
wierzcholek grafu, 88
współczynnik dominujący, 156
wymiar rozszerzenia ciala, 155
wzór o rozkładzie dla p-podgrupy, 83
wzor o rozkladzie na orbity, 83

zasada sita, 21
zasada wlaczania i wylaczania, 21
Zasadnicze twierdenie o skonczonych grupach abelowych, 71
Zasadnicze twierdzenie o skonczonych grupach abelowych, 69
zasadnicze twierdzenie teorii Galois, 199
zero pierscienia, 105
znak permutacji, 41