Algebra 2009
Notatki do wykładów

A. Paweł Wojda
Wydział Matematyki Stosowanej AGH

28 stycznia 2010

Spis treści

Rozdział 1

Wykład 1. 7.X.2009

1.1 Wstęp

Zacznijmy od kilku informacji o historii nazwy przedmiotu.
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 *Notatek*, 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

[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.

będziecie mieli okazje do poznania niektórych zastosowań. Czasu nie wystarczyło, by przedstawić ich więcej. Poznacie je z pewnością na innych przedmiotach (kodowanie, matematyka dyskretna, teoria algorytmów...).

Jak z pewnością zauważyliście, spis literatury jest znacznie obszerniejszy niż ten, który podałem podczas wykładu. Oczywiście nie musicie wszystkiego czytać, w każdym razie nie dzisiaj :)

A. Paweł Wojda

1.2 Arytmetyka liczb całkowitych

Przypomnijmy **twierdzenie o dzieleniu liczb całkowitych**.

Twierdzenie 1.1 *Dla dowolnych liczb całkowitych a i b, $b > 0$ istnieją jednoznacznie wyznaczone liczby $q, r \in \mathbf{Z}$ takie, że $a = bq + r$, przy czym $0 \leq r < b$.*

Liczby q oraz r nazywamy, odpowiednio, **ilorazem** i **resztą** dzielenia a przez b.

Warto podkreślić, że twierdzenie 1.1 nie jest tym, które większość studentów pamięta ze szkoły[3].

Mówimy, że d jest **największym wspólnym dzielnikiem** liczb całowitych a i b jeżeli

- $d|a$ i $d|b$ oraz
- dla każdego $c \in \mathbf{Z}$: $c|a \ \wedge c|b \Rightarrow c|d$

Algorytm Euklidesa

Niech $a, b \in \mathbf{Z}$, $a, b \neq 0$.
Tworzymy rekurencyjnie ciąg (r_n):
$r_0 = a, \quad r_1 = b$
$r_{n-1} = q_n r_n + r_{n+1}$, gdzie $0 \leq r_{n+1} < r_n$.

Twierdzenie 1.2 *Niech $a, b \in \mathbf{Z}$, $a, b \neq 0$. Istnieje takie k całkowite, że $r_k \neq 0$, $r_{k+1} = 0$ (gdzie ciąg (r_n) jest wyznaczony przy pomocy algorytmu Euklidesa). Co więcej, mamy wówczas $r_k = \text{NWD}(a, b)$.*

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

Twierdzenie 1.3 *Niech $a, b \in \mathbf{Z}$, nie równe równocześnie zero.*

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

Wniosek 1.4 *Jeśli $a, b \in \mathbf{Z}$, $a \perp b$, to istnieją $\alpha, \beta \in \mathbf{Z}$:*

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

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

Twierdzenie 1.5 (Euklides) *Istnieje nieskończenie wiele liczb pierwszych.*

[3]Sprawdź, jaki jest wynik dzielenia liczby -9 przez 7?

1.3 Grupy

Definicja 1.1 (Przypomnienie) *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. Grupa S_X (permutacji zbioru X z działaniem składania funkcji).

Rozdział 2

Wykład 2. 14.X.2008

2.1 Grupy c.d.

$h : G_1 \to G_2$ 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**.

Przykład 2.1 *Przykłady grup:* $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$ $(\mathbf{Q}^{+*}, \cdot)$ $(\mathbf{Z_n}, +)$, $(\mathbf{R}, +), ...$ *– grupy przemienne (*$\mathbf{Q}^* = \mathbf{Q} - \{0\}$*),* $\mathbf{Q}^{+*} = \{a \in \mathbf{Q} | a > 0\}$. $(S(X), \circ)$ *– grupa permutacji zbioru* X*, nieprzemienna dla* $|X| \geq 3$
Z dokładnością do izomorfizmu, istnieje tylko jedna grupa o co najwyżej 3 elementach.
Istnieją dokładnie dwie grupy (z dokładnością do izomorfizmu) rzędu 4*: grupa* $(\mathbf{Z}_4, +)$ *oraz grupa Kleina (materacowa)* $(\mathbf{Z}_2 \times \mathbf{Z}_2, +)$.

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 elemwntu* 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* $\mathbf{Z}^*_{10} = \{1, 3, 7, 9\}$.

Definicja 2.1 *Niech* $n \in \mathbf{N}$*. Definiujemy*

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

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

Definicja 2.2 (Funkcja φ Eulera) *Niech $n \in \mathbf{N}$. Przez $\varphi(n)$ oznaczamy liczbę takich $a \in \mathbf{N}$, że $a \perp n = 1$ (a i n są względnie pierwsze). Funkcję $\varphi : \mathbf{N} \to \mathbf{N}$ nazywamy* **funkcją Eulera**.

Definicja 2.3 *Jeśli grupa G na skończoną liczbę elementów, wówczas mówimy, że G jest* **skończona** *a jej liczbę elementów nazywamy* **rzędem grupy** *G.*

Przykład 2.3 *Rząd $\mathbf{Z}_n$ jest równy n.*
Rząd $\mathbf{Z}^*$ jest równy 4.

Następne twierdzenie nie wymaga dowodu.

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

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

Własności funkcji Eulera: Niech P będzie liczbą pierwszą. Wówczas

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

Twierdzenie 2.4 (Formuła Sita[1] lub Zasada Włączania i Wyłączania) *Niech*
$A_1, A_2, ..., A_n$ będą zbiorami skończonymi. Wówczas zachodzi wzór

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

Formuła sita posłuży nam do wykazania następującego twierdzenia.

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

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

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

Wniosek 2.6 *Wzór na φ z twierdzenia 2.5 pozostaje identyczny jeśli położymy $n = p_1^{a_1} \cdot ... \cdot p_t^{a_t}$ gdzie $p_1 < ... < p_t$ są liczbami pierwszymi, $a_1, ..., a_t \in \mathbf{N}$.*

[1] 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). Jego innym, wielkim osiągnięciem była próba zmierzenia promienia Ziemi przez zmierzenie 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, a było to w czasach kiedy w kulistość Ziemi wierzył mało kto!

2.2 Grupy cykliczne

Definicja 2.4 (Generator grupy) *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}.*

Przykład 2.5 1 *(a także -1) jest generatorem grupy* $\mathbf{Z}$ *(addytywnej grupy liczb całkowitych).*
2 *jest generatorem (multyplikatywnej) grupy* $\mathbf{Z}_5^*$.

Rozdział 3

Wykład 3 - 21.X.2009

3.1 Grupy cykliczne - c.d.

Twierdzenie 3.1 *Jeżeli G jest multyplikatywną grupą skończoną, $g \in G$, wówczas istnieje $n \in \mathbf{N}$ takie, że $g^n = g^{-1}$*

Dow. ...

Definicja 3.1 *Jeśli grupa G na skończoną liczbę elementów, wówczas mówimy, że G jest* **skończona** *a jej liczbę elementów nazywamy* **rzędem grupy** *G.*

Definicja 3.2 *Najmniejsze $n \in \mathbf{N}$ takie, że*

$$g^n = e \tag{3.1}$$

nazywamy **rzędem** *elementu g grupy, jeśli $n \in \mathbf{N}$ spełniające (3.1) nie istnieje, wówczas mówimy, że rzędem g jest ∞.*
Jeśli grupa zawiera generator, to nazywamy ją cykliczną.

Przykład 3.1 *Grupa $(\mathbf{Z}_4, +)$ jest cykliczna, grupa Kleina nie.*

Twierdzenie 3.2 *Każda grupa cykliczna jest przemienna.*

Dowód oczywisty – tym bardziej trzeba umieć!

Twierdzenie 3.3 *Każda skończona grupa cykliczna G jest izomorficzna z $(\mathbf{Z}_n, +)$, gdzie n jest rzędem grupy G.* [1]

Bez dowodu (za to do udowodnienia samodzielnego) podałe:

Twierdzenie 3.4 *Każda nieskończona grupa cykliczna jest izomorficzna z $(\mathbf{Z}; +)$.*

Oczywiście stąd wynika, że każda grupa cykliczna jest przeliczalna (ale to w ogóle od razu *widać*.

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

3.2 Twierdzenia Cayleya i Lagrange'a

3.2.1 Podgrupy - przypomnienie

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.
Jako ćwiczenia należy udowodnić następujące 3 twierdzenia.

Twierdzenie 3.5 (Znane!) *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 $a * b^{-1} \in H$.*

Twierdzenie 3.6 (Łatwe) *Jeśli w grupie skończonej G zbiór $S \neq \emptyset$ jest zamknięty ze względu na działanie grupowe $(*)$, to S stanowi podgrupę G.*

Twierdzenie 3.7 (Trudniejsze) *Każda podgrupa grupy cyklicznej jest cykliczna.*

Dowód można znaleźć stronie 154 *Przeglądu Algebry współczesnej* Birkhofa i MacLane'a.

3.2.2 Twierdzenie Cayleya

Definicja 3.3 (Grupa transformacji) *Dowolną podgrupę grupy permutacji $S(X)$ nazywamy* **grupą transformacji**.

Twierdzenie 3.8 (Tw. Cayleya) *Dowolna grupa jest izomorficzna z pewną grupą tranformacji.*

3.2.3 Twierdzenie Lagrange'a

Twierdzenie 3.9 (Lagrange'a) *Niech H będzie podgrupą grupy skończonej G, $a = |H|, b = |G|$. Wówczas $a|b$.*

Definicja 3.4 (Przystawanie modulo półgrupa) *Niech H będzie podgrupą grupy G, $a, b \in G$. Mówimy, że a* **przystaje do** *b* **modulo** *H (piszemy $a \equiv b \ (mod\ H)$ lub aR_Hb) jeżeli $ab^{-1} \in H$.*

Lemat 3.10 *Jeżeli H jest podgrupą G wówczas relacja przystawania modulo H jest w G relacją równoważności.*

Lemat 3.11 *Niech G będzie dowolną grupą, zaś H jej podgrupą. Wówczas klasą elementu neutralnego grupy G modulo H jest zbiór H.*

Rozdział 4

Wykład 4 - 28.X.2009

Dokończenie dowodu twierdzenia Lagrange'a.

Lemat 4.1 *Niech G będzie dowolną grupą, zaś H jej podgrupą. Wówczas dowolne dwie klasy równoważności modulo H są równoliczne (bijektywne)*[1].

Oczywiście twierdzenie Lagrange'a wynika natychmiast z lematu 4.1.

4.0.4 Wnioski z twierdzenia Lagrange'a

Wniosek 4.2 *Każdy element grupy skończonej G ma rząd będący dzielnikiem rzędu grupy G.*

Wniosek 4.3 *Jeśli rząd grupy G jest liczbą pierwszą, to G jest cykliczna.*

Wniosek 4.4 (stary) *Jedynymi grupami grupami rzędu 4 są $\mathbf{Z}_4$ i grupa Kleina.*

4.0.5 Twierdzenie Eulera i Małe Twierdzenie Fermata

Twierdzenie 4.5 (Eulera) *Jeśli liczby naturalne a, n są względnie pierwsze, wówczas*

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

Twierdzenie 4.6 (Małe Twierdzenie Fermata) *Jeśli p jest liczbą pierwszą, $a \in \mathbf{Z}$, to*

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

[1] W przypadku gdy G jest grupą skończoną oznacza to, że dowolne dwie klasy równoważności modulo H mają taką samą liczbę elementów.

4.1 Ćwiczenia

1. Niech G będzie grupą. Wykaż, że podzbiór niepusty $H \subset G$ jest podgrupą G wtedy i tylko wtedy, gdy $\forall x, y \in H : xy^{-1} \in H$.
2. Wykaż że jeśli w grupie skończonej G zbiór $S \neq \emptyset$ jest zamknięty ze względu na działanie grupowe, wówczas S jest podgrupą.
3. Wykaż, że podgrupa grupy cyklicznej jest cykliczna.

4.2 Chińskie twierdzenie o resztach – równania modularne

Twierdzenie 4.7 *Równanie modularne*

$$ax \equiv 1 \ (mod \ n) \tag{4.1}$$

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).

Uwaga. 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 4.8 (Chińskie o resztach[2]) *Niech $a, b \in \mathbf{Z}$, $m, n \in \mathbf{N}$, $m \perp n$. Wówczas układ równań*

$$\begin{cases} x & \equiv & a & (\ mod\ m) \\ x & \equiv & b & (\ mod\ n) \end{cases} \tag{4.2}$$

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 (4.2) jest postaci $\{x_0 + k(mn) | k \in \mathbf{Z}\}$).

Twierdzenie 4.8 pozwala łatwo (indukcyjnie) udowodnić następujące uogólnienie chińskiego twierdzenia o resztach - o tym uogólnieniu podczas wykładu nie mówiłem!

[2]Twierdzenie to udowodnił ok. 350 roku n.e. Sun Tsu Suan-Ching.

Twierdzenie 4.9 *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*

$$\begin{cases} x & \equiv & a_1 & (\ mod\ m_1) \\ x & \equiv & a_2 & (\ mod\ m_2) \\ & & \ldots & \\ x & \equiv & a_k & (\ mod\ m_k) \end{cases} \tag{4.3}$$

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

Rozdział 5

Wykład 5 - 4.XI.2009

5.1 Kwadratowe residua modulo

Twierdzenie 5.1 *Niech p będzie liczbą pierwszą i niech $a \in \mathbf{Z}_p$. Wówczas a ma co najwyżej dwa pierwiastki kwadratowe w $\mathbf{Z}_p$.*

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 $a = b^2 \pmod{n}$.

Twierdzenie 5.2 *Niech $p \in \mathbf{N}$ będzie liczbą pierwszą, $p \equiv 3 \pmod 4$ i niech a będzie residuum kwadratowym w $\mathbf{Z}_p$. Wówczas pierwiastkami kwadratowymi a z $\mathbf{Z}_p$ są $a^{\frac{p+1}{4}} \pmod p$ oraz $-a^{\frac{p+1}{4}} \pmod p$.*

5.2 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[1]. 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[2], na dodatek

[1] *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?

[2] E od angielskiego *encoding*

wychodząc z założenia, że wszystkie przesyłane wiadomości są podsłuchiwane (przez Ewę).

By osiągnąć swój cel, Alicja i Bob będą postępowali według następującego schematu:

1	Bob znajduje funkcję kodującą (szyfrującą) E oraz dekodującą D, a więc takie by $D(E(l)) = l$
2	Bob przesyła tekstem otwartym (Ewa widzi przekaz) funkcję E Alicji
3	Alicja koduje 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[3] 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, 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[4]. 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.

5.2.1 Metoda Rabina

Metodę kodowania Rabina[5] można opisać następująco. Niech n będzie ustaloną, wystarczająco dużą (powiedzmy 300-cyfrową) liczbą. Funkcją kodującą jest

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

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

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

[5] Nazwa od twórcy metody: Michaela Rabina

Oznacza to tyle, że Bob prześle Alicji liczbę n i funkcję kodującą. 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?

Oto opis metody.

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 (a wszystko to podgląda Ewa).

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:

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

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

Układy równań modularnych mają jednoznaczne rozwiązania modulo $n = pq$ dzięki lematowi chińskiemu. 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.

5.2.2 Metoda RSA

O ile metoda Rabina wykorzystuje Małe Twierdzenie Fermata, to metoda RSA[6] opiera się na twierdzeniu Eulera.

Opis metody RSA.

1. Bob:

   (a) Znajduje 2 duże liczby pierwsze p, q, liczy $n = pq$ oraz $\varphi(n) = (p-1)(q-1)$.

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

(b) Wybiera (dowolne) $e \in \mathbf{Z}^*_{\varphi(n)}$ (a więc e jest względnie pierwsze z $\varphi(n)$).

(c) 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 $l = m^e \pmod n$

   (b) Wysyła l Bobowi.

Bob: Liczy

$$l^d = (m^e)^d \equiv m \tag{5.1}$$

Prawdziwo wzoru 5.1 wymaga uzasadnienia. Oto one.

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

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

(b) Przypadek: m i n nie są względnie pierwsze. Wtedy albo $p|m$ albo $q|m$ (gdyby $p|m$ i $q|m$ to mielibyśmy sprzeczność z (milczącym) założeniem, źe $m < n$[7]). Załóżmy, że $p|m$ oraz $q \not| m$.
Mamy teraz: $m^{ed} = m^{1+k(p-1)(q-1)} = m(m^{q-1})^{k(p-1)}$. Ale $q \perp m$ (bo q jest liczbą pierwszą i q nie dzieli m). Wiemy że, $\varphi(q) = q - 1$. A więc $m^{ed} \equiv m \cdot 1^{k(p-1)} = m \pmod q$.
Ostatecznie otrzymaliśmy

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

Mamy także

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

(bo $m \equiv 0 \pmod p$. Z chińskiego twierdzenia o resztach m jest jedynym rozwiązaniem układu równań

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

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

[7]Co to jest *milczące założenie*? Odpowiedź jest prosta. To takie o którym wykładający zapomniał! Zakładamy, że liczby szyfrowane są mniejsze od n, w przeciwnym przypadku ulegałyby obcięciu modulo n, a więc zniekształceniu. Takie szyfrowanie byłoby bez sensu!

Rozdział 6

Wykład 6. 18.XI.2009

Sesja!!! Terminy egzaminów pisemnych;

I termin 1 lutego 2010, s. 1,8, 1.9, 2.1 godz. 13.30

II termin 22 luty s. 1.8 i 1.9 godz. 9.00

III termin 26 luty s. 1.8 godz. 9.00

Egzamin ustny dla osób zwolnionych z egz. pisemnego rozpocznie się najprawdopodobniej już 1 lutego. Szczegóły zostaną podane później.

6.1 Grupy c.d.

6.1.1 Zliczanie

Przykady szachownic o 2×2 i 2×3 polach.
Problem: Ile jest różnych szachownic?

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

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).

Przykłady: grupa Kleina jako podgrupa permutacji na zbiorze $\{1, 2, 3, 4\}$. Grupa izomtrii kwadratu, szachownicy itp.

Twierdzenie 6.1 *Jeśli grupa G działa na zbiorze X, $g \in G$, to g jest bijekcją.*

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

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

Przykład ..

Twierdzenie 6.2 *Stabilizator dowolnego elementu $x \in X$ jest podgrupą grupy G.*

Przykład. Grupa obrotów sześcianu (foremnego).
Orbitą elementu $x \in X$ nazywamy zbiór

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

Relacja R określona przez

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

jest w X równoważnościowa.

Twierdzenie 6.3 *Jeśli skończona grupa G działa na zbiorze X, wówczas dla każdego $x \in X$*

$$|G| = |Stab\ x| \cdot |Orb\ x|$$

Liczne przykłady – ilustracja funkcjonowania twierdzenia 6.3.
Grupa izometrii pięciokąta.

Grupy izometrii sześciościanu:

wykonalnych: 24-elementowa

nie dających się przeprowadzić bez zniszczenia sześcianu: 48-elementowa

Rozdział 7

Wykład 7 - 25.XI.2009

7.1 Grupy - c.d.

Dowód twierdzenia 6.3 z poprzedniego wykładu.

7.1.1 Lemat Burnside'a

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

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

Twierdzenie 7.1 (Lemat Burnside'a) *Niech G będzie grupą skończoną działającą na zbiorze skończonym X. Wówczas liczba N orbit zbioru X ze względu na G wynosi*

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

Przykłady ...
Dowód (metodą podwójnego zliczania)...

Przykład. Liczba różnych naszyjników o sześciu perłach: dwóch czarnych i czterech białych.

7.1.2 Podgrupy normalne

Warstwy prawo- i lewostronne

Już wiemy (dowiedzieliśmy sie tego przy okazji dowodu twierdzenia Lagrange'a), że dla dowolnej podgrupy H grupy multyplikatywnej G relacja: $aRb \Longleftrightarrow ab^{-1}$ jest równoważnościowa. Klasą równoważności dowolnego elementu $a \in G$ dla tej relacji jest zbiór

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

zwany **warstwą prawostronną**.
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 7.2 *Jeśli grupa G jest przemienna, to dla dowolnej podgrupy H i $a \in G$*

$$aH = Ha$$

Definicja 7.1 *Mówimy, że podgrupa H grupy G jest* **normalna** *(lub* **niezmiennicza***), jeśli dla dowolnego $a \in G$ zachodzi $aH = Ha$.*

Rozdział 8

Wykład 8 - 2.XII.2009

8.1 Grupy - c.d.

8.1.1 Podgrupy normalne

Twierdzenie 8.1 *Podgrupa H grupy G jest normalna wtedy i tylko wtedy gdy dla każdego $a \in G$ i dla każdego $b \in H$*

$$aba^{-1} \in H$$

Dowód ...

Twierdzenie 8.2 *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 jako ćwiczenie! !

Twierdzenie 8.3 *Dla dowolnego morfizmu grup $f : G \to H$ zbiór $Ker\ f = f^{-1}(\{e_H\})$ jest podgrupą grupy G.*

Dowód jako ćwiczenie! !

Twierdzenie 8.4 *Jeśli H jest podgrupą normalną grupy G, to G/H z działaniem zdefiniowanym wzorem*

$$Ha \cdot Hb = Hab$$

jest grupą (zwaną **grupą ilorazową***).*

Dowód jako ćwiczenie! !

Twierdzenie 8.5 (O morfiźmie grup) *Jeśli $f : G \to H$ jest morfizmem grup, to grupa ilorazowa $G/Ker\ f$ jest izomorficzna z $Im\ f$.*
Dokładniej: jeśli oznaczymy przez $k : G \to G/Ker\ f$ **morfizm kanoniczny** *dany wzorem $k(g) = (Ker\ f)g$, zaś przez $h : G/Ker\ f \to Im\ f$ odwzorowanie zadane wzorem $h((Ker\ f)a) = f(a)$, to h jest izomorfizmem grup i zachodzi wzór $f = h \circ k$.*

Dowód jako ćwiczenie! !

8.2 Pierścienie

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**. *(Tego akurat odczas wykładu nie powiedzaiłem, ale wiecie to skąd inąd!)*

Twierdzenie 8.6 *Pierścień P jest bez dzielników zera wtedy i tylko wtedy dla dowolnych elementów spełniony jest warunek:*

$$\forall a, b, c \in P,\ c \neq 0 \begin{cases} ac = bc & \Rightarrow \quad a = b \\ ca = cb & \Rightarrow \quad a = b \end{cases} \qquad (\text{ prawa skracania}) \qquad (8.1)$$

[1] Inaczej: dla każdego $a \in P, a \neq 0$ istnieje $a' \in P$ taki, że $aa' = 1$.

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. ■

8.2.1 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 $\mathbf{Z}$. 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).

- Niech P będzie pierścieniem przemiennym[2]. Zbiór $\{\sum_{i=0}^{\infty} a_i \mathbf{x}^i | a_i \in P\}$ nazywamy zbiorem **szeregów formalnych** Łatwo można wykazać (**ćwiczenie!**), 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[3], zbiór szeregów foralnych o skończonej liczbie współczynników różnych od zera z działaniami określonymi wzorami: !

[2] O tym założeniu nie powiedziałem podczas wykładu!
[3] W domu lub podczas ćwiczeń!

- $(\sum_{i=0}^{\infty} a_i \mathbf{x}^i) + (\sum_{i=0}^{\infty} b_i \mathbf{x}^i) = \sum_{i=0}^{\infty} (a_i + b_i)\mathbf{x}^i$
- $(\sum_{i=0}^{\infty} a_i \mathbf{x}^i) \cdot (\sum_{j=0}^{\infty} b_j \mathbf{x}^j) = \sum_{l=0}^{\infty} c_l \mathbf{x}^l$, gdzie $c_l = \sum_{k=0}^{l} a_k b_{l-k}$ jest pierścieniem przemiennym (z jedynką, o ile w P jest jedynka).

8.3 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.

Twierdzenie 8.7 *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. $\forall a, b \in A \; ab \in A$.

8.4 Zadania

Zadanie 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 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 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 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)).

8.4.1 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. $a, b \in P \Rightarrow a - b \in P$
2. $\alpha \in P, a \in I \Rightarrow \alpha a \in I, a\alpha \in I$

Przykład 8.1 *W dowolnym pierścieniu P zbiory $\{0\}$ i P są ideałami.*

Przykład 8.2 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** .

Definicja 8.3 *Pierścień P nazywamy* **pierścieniem głównym** *jeżeli każdy jego ideał jest ideałem głównym.*

Najlepiej znanym przykładem pierścienia głównego jest pierścień liczb całkowitych.

Twierdzenie 8.8 *Pierścień liczb całkowitych* $\mathbf{Z}$ *jest pierścieniem głównym.*

Dowód. Przypuśćmy, że A jest ideałem w $\mathbf{Z}$, $A \neq \{0\}$. 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 $a|b$. ■

Rozdział 9

Wykład 9 - 9.XII.2009

9.1 Pierścienie - c.d.

9.1.1 Więcej o pierścieniach wielomianów

Dla wielomianu $v = v_0 + v_1 x + \ldots \in P[x]$ największe k_0 dla którego $v_{k_0} \neq 0$ nazywamy **stopniem wielomianu** v i oznaczmy przez $\partial(v)$. Stopniem wielomianu zerowego jest $-\infty$[1]. Współczynnik v_{k_0} nazywamy wtedy **współczynnikiem dominującym** wielomianu v.

Z łatwością można sprawdzić, prawdziwość następujących dwóch twierdzeń.

Twierdzenie 9.1 *Dla dowolnego pierścienia P zbiór $P[x]$ jest pierścieniem. Jeśli P jest pierścieniem całkowitym, wówczas także $P[x]$ jest pierścieniem całkowitym.* ■

Twierdzenie 9.2 *Dla dowolnego pierścienia P i wielomianów $v, w \in P[x]$ 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 $w \in P[x]$, $w = w_0 + w_1 x + \ldots + w_n x^n$ można skojarzyć **funkcję wielomianową**:

$$w : P \ni x \to w(x) = w_0 + w_1 x + \ldots + w_n x^n \in P$$

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).

[1]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!).

9.1.2 Podzielność w pierścieniach

Definicja 9.1 *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**.

Przykłady...

Definicja 9.2 *Elementy stowarzyszone z 1 (jedynką pierścienia) nazywamy* **jednościami pierścienia**.

Twierdzenie 9.3 *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

$$a = a_1 \cdot \ldots \cdot a_n \tag{9.1}$$

nazywamy **rozkładem na czynniki**. O rozkładzie 9.1 mówimy, że jest **właściwy**, jeśli

1. $n \geq 1$,
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:

$$a|bc \Rightarrow a|b \text{ lub } a|c$$

Wbrew temu co pamiętamy ze szkoły, pojęcia elementów nierozkładalnych i pierwszych są różne, choć *całkowite liczby* nierozkładalne i pierwsze to jednak to samo. Poniższe twierdzenie podaje relację zawierania pomiędzy zbiorami elementów pierwszych i nierozkładalnych dowolnego pierścienia całkowitego.

Twierdzenie 9.4 *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

$$a = a_1 \cdot \ldots \cdot a_k \tag{9.2}$$

dla pewnego $k \geq 2$. Wówczas istnieje $i \in \{1, \ldots, k\}$ takie, że $a|a_i$. Ponieważ (na mocy (9.2)) $a_i|a$, elementy a oraz a_i są stowarzyszone.
Wykażemy teraz, że jeśli dwa elementy x, y są stowarzyszone w pierścieniu całkowitym 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 $a = a_1 \cdot \ldots \cdot a_{i-1}a_{i+1} \cdot \ldots \cdot a_k a_i = a_i z$, przy czym z jest jednością. Korzystając z przemienności i ponownie z prawa skracania otrzymujemy, że $a_1 \cdot \ldots \cdot a_{i-1}a_{i+1} \cdot \ldots \cdot a_k = z$, 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 9.4 nie jest prawdziwe, jest **pierścień Dedekinda** $\mathbf{Z}[\sqrt{5}i] = \{a+bi\sqrt{5} | a, b \in \mathbf{Z}\}$. Wykażemy wpierw, że liczba 2 jest elementem nierozkładalnym pierścienia Dedekinda. rzeczywiście,

$$2 = (a + bi\sqrt{5})(c + di\sqrt{5})$$

daje układ równań

$$\begin{array}{rcl} ac - 5bd & = & 2 \\ bcd + ad & = & 0 \end{array}$$

Traktując ten układ jako układ o niewiadomych c i d otrzymamy

$$c = \frac{2a}{a^2 + 5b^2} \qquad d = \frac{-2b}{a^2 + b^2}$$

(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.

9.1.3 Pierścienie Gaussa

Definicja 9.3 *Pierścień P nazywamy* **pierścieniem z rozkładem** *jeżeli każdy, nie będący jednością pierścienia P, element $a \in P$ da się przedstawić jako iloczyn skończonej liczby elementów nierozkładalnych w P.*
Dwa rozkłady elementu a:

$$a = a_1 \cdot ... \cdot a_m \quad a = b_1 \cdot ... \cdot b_b$$

nazywamy **jednakowymi** *jeżeli*

1. $m = n$,
2. *istnieje permutacja $\sigma : [1, m] \to [1, n]$ taka, że elementy a_i oraz $b_{\sigma(i)}$ są stowarzyszone.*

Pierścień całkowity P nazywamy **pierścieniem Gaussa** [2] *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 $\mathbf{Z}$*, $K[x]$ - 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: $6 = 3 \cdot 2 = (1 + \sqrt{-5})((1 - \sqrt{-5}))$*.*

[2] Carl Friedrich Gauss 1777-1855

Rozdział 10

Wykład 10 - 16.XII.2009

10.0.4 Pierścienie Gaussa c.d.

Twierdzenie 10.1 *Pierścień całkowity z rozkładem P jest pierścieniem Gaussa wtedy i tylko wtedy gdy każdy element nierozkładalny $a \in P$ jest w P elementem pierwszym.*

Uwaga. Pierścień Dedekinda $\mathbf{Z}[\sqrt{-5}]$ nie jest pierścieniem Gaussa. W tym pierścieniu element 6 ma dwa różna rozkłady na czynniki nierozkładalne.

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-1})$$

10.0.5 Powrót do wielomianów

Twierdzenie 10.2 *Niech P będzie pierścieniem całkowitym i niech $p \in P[x]$ będzie wielomianem którego współczynnik dominujący jest odwracalny. Dla każdego wielomianu $v \in P[x]$ istnieją wielomiany $q, r \in P[x]$ takie, że*

$$v = qp + r, \quad \partial r < \partial p \text{ lub } r = 0 \tag{10.1}$$

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 $v^* \in P[x]$ 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 $\bar{v} = v - v_k p_m^{-1} x^{k-m} p$ 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 $v - v_k p_m^{-1} x^{k-m} p = \bar{q}p + r$,

a zatem $v = (v_k p_m^{-1} x^{k-m} + \bar{q})p + r$, co kończy dowód istnienia wielomianów q i r.

Pozostaje wykazać jedyność wielomianów q i r spełniających warunki (10.1). 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 $r = \bar{r}$. ■

Wniosek 10.3 *Niech P będzie pierścieniem z jedynką. Reszta z dzielenia wielomianu $v \in P[x]$ przez wielomian $x - c$ jest równa $v(c)$.*

Dowód. Na mocy twierdzenia o dzieleniu wielomianów możemy napisać

$$v = q(x - c) + r$$

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** $v \in P[x]$ jeśli $v(c) = 0$.
Niech $v \in P[x]$, gdzie P jest pewnym pierścieniem całkowitym, $x = q(x - c) + r$, gdzie r jest wielomianem stopnia zero. Z wniosku 10.3 wynika, że c jest pierwiastkiem wielomianu v wtedy i tylko wtedy, gdy $x - c$ dzieli v. Zapiszmy to spostrzeżenie

Wniosek 10.4 *Niech P będzie pierścieniem całkowitym. Wielomian $v \in P[x]$ jest podzielny przez wielomian $x - c$ wtedy i tylko wtedy, gdy c jest pierwiastkiem wielomianu v.* ■

Z wniosku 10.4 bardzo łatwo można wykazać jeszcze jeden, bardzo ważny wniosek.

Wniosek 10.5 *Niech P będzie pierścieniem całkowitym. Dowolny wielomian $v \in P[x]$ stopnia k ma co najwyżej k pierwiastków.* ■

Twierdzenie 10.6 *Pierścień wielomianów $\mathbf{K}[x]$ nad dowolnym ciałem $\mathbf{K}$ jest pierścieniem głównym.*

Dowód. Niech B będzie ideałem pierścienia $\mathbf{K}[x]$. 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 $q \in \mathbf{K}[x]$ takie, że $b = qd$.

Z twierdzenia o dzieleniu wielomianów (twierdzenie 10.2) wynika, że istnieją takie wielomiany $q, r \in \mathbf{K}[x]$, 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. ■

Już niebawem okaże się, że bardzo ważną własnością pierścieni głównych jest, że dowolny wstępujący ciąg ideałów pierścienia głównego jest stacjonarny. Tę własność wykażemy w następnym twierdzeniu.

Twierdzenie 10.7 *W pierścieniu głównym P każdy wstępujący ciąg ideałów*

$$C_1 \subset C_2 \subset \ldots \subset C_k \subset \ldots$$

jest stacjonarny, tzn. istnieje $k_0 \in \mathbf{N}$ takie, że

$$C_{k_0} = C_{k_0+1} = \ldots$$

Dowód. Suma ideałów $C = \bigcup_{i=1}^{\infty} C_i$ iest ideałem (por. zad. **??**). Ponieważ P jest pierścieniem głównym, istnieje $a \in P$ takie, że $C = (a)$. Oczywiście $a \in C$, a więc istnieje $k_0 \in \mathbf{N}$ takie, że $a \in C_{k_0}$.
Z definicji C (jako mnogościowej sumy C_I, $i \in \mathbf{N}$): $C_{k_0} \subset C$. Z drugieje strony, skoro $a \in C_{k_0}$, to z definicji ideału $(a) \subset C_{k_0}$, a więc $C \subset C_{k_0}$ i ostatecznie: $C = C_{k_0}$. ■

Największym wspólnym dzielnikiem elementów a i b pierścienia całkowitego P nazywamy element $d \in P$ spełniający warunek:

$$d|a,\ d|b \quad \text{oraz dla każdego } c \in P: \quad c|a, c|b \Rightarrow c|d$$

Największy wspólny dzielnik elementów a i b oznaczamy przez NWD(a, b) lub, częściej, przez (a, b).
W pierścieniach głónych 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 10.8 *Każde dwa elementy a, b pierścienia 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

$$S = \{s_1 a + t_1 b | s_1, t_1 \in P\}$$

Łatwo sprawdzić (por. zadanie **??**), że S jest ideałem. Ponieważ z założenia P jest pierścieniem głównym, ideał S jest główny, a więc istnieje $d \in P$ takie, że

$S = (d)$. Ponieważ zarówno a jak i b należą do S, $d|a$ oraz $d|b$.
Jeśli $c|a$ i $c|b$, a więc $a = \alpha c$, $b = \beta c$ $(\alpha, \beta \in P)$, 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 $a \perp b$.

10.1 Miasta Parzyste i Nieparzyste - w prezencie na gwiazdkę!

W mieście E o 32 mieszkańcach kluby są tworzone według następujących zasad.

(i) Każdy klub ma parzystą liczbę członków.

(ii) Przecięcie dowolnych dwóch klubów ma parzystą liczbę elementów.

Natomiast w mieście O (także o 32 mieszkańcach) kluby są tworzone według tak, by

(a) Każdy klub miał nieparzystą liczbę członków.

(b) Przecięcie dowolnych dwóch klubów miało parzystą liczbę elementów.

Problem. Jaka jest maksymalna liczba klubów w E, a jaka w O?
Wykazaliśmy, że w O można utworzyć co najmniej $2^{16} \geq 65536$ klubów, podczas gdy w O co najwyżej 32.
Bardzo się zdziwiliśmy!

Uwaga konkurs! Ogłaszam konkurs na nazwy miast E i O
Wesołych Świąt!

Rozdział 11

Wykład 11 - 6.I.2010

W którym wykorzystaliśmy wiele twierdzeń z wykładów poprzednich. Można nawet pokusić się o stwierdzenie, że po ciężkiej (?) pracy w ubiegłym roku przyszedł czas żniw. Teraz dopiero możemy zobaczyć jak wiele i jak bardzo pożytecznych twierdzeń i pojęć nauczyliśmy się. A kto tego nie widzi... do okulisty!

11.1 Pierścienie euklidesowe

Definicja 11.1 *Pierścień całkowity P nazywamy* **euklidesowym** *jeśli istnieje funkcja $h : P^* \to \mathbf{N}^+$ taka, że dla wszystkich $a \in P, b \in P^*$ istnieją $q, r \in P$: $a = bq + r$, i albo $r = 0$ albo $h(r) < h(b)$.*

Przykłady.

1. $\mathbf{Z}$ z funkcją $h(n) = |n|$
2. $K[x]$ gdzie Kjest pewnym ciałem, z funkcją $h(v) = 2^{\partial(v)}$
3. $\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$ zaś $h(a + bi) = a^2 + b^2$
   Wykażemy, że funkcja h tak zdefiniowana rzeczywiście spełnia postulaty definicji pierścienia euklidesowego.
   Niech $a+bi \in \mathbf{Z}[i]$ i niech $c+di \in \mathbf{Z}[i]^*$. 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 $a + bi = (c + di)(e_0 + f_0 i) + r$. Pozostaje więc wykazać, że $h(r) < |c + di|^2$.

$$h(r)| = |r|^2 = |a + bi - (c + di)(e_0 + f_0 i)|^2 =$$

$$= |(c + di)(e + fi) - (c + di)(e_0 + f_0 i)|^2 \leq |c + di|^2 |e + fi - e_0 - f_0 i|^2 =$$

$$= |c + di|^2((e - e_0)^2 + (f - f_0)^2) \leq |c + di|^2(\frac{1}{4} + \frac{1}{4}) < |c + di|^2 = h(c + di)$$

Łatwo można wykazać , że prawdziwe jest następujące twierdzenie. Ćwiczenie!

Twierdzenie 11.1 *Każdy pierścień euklidesowy jest pierścieniem głównym.*

Bez żadnych trudności można zaobserwować, że w pierścieniach euklidesowych funkcjonuje algorytm euklidesowy znajdowania NWD dowolnych dwóch elementów (wystarczy prześledzić algorytm Euklidesa dla liczb całkowitych). Ćwiczenie!

ALGORYTM EUKLIDESOWY W PIERŚCIENIU EUKLIDESOWYM)

11.2 Zasadnicze Twierdzenie Arytmetyki

Następujące twierdzenie nazywa się Zasadniczym Twierdzeniem Arytmetyki (lub Twierdzeniem o Jednoznacznej Faktoryzacji).

Twierdzenie 11.2 *Każdy pierścień główny jest pierścieniem Gaussa.*

Dow. ...

Oczywiście, skoro każdy pierścień euklidesowy jest pierścieniem głównym, prawdziwy jest następujący wniosek.

Wniosek 11.3 *Każdy pierścień Euklidesa jest pierścieniem Gaussa.*

11.3 Ciało ułamków pierścienia całkowitego

Niech P będzie pierścieniem całkowitym, $P^* = P - \{0\}$. wzbiorze $Q = P \times P^*$ zdefiniujmy dwa działania:

$$(a, b) + (c, d) = (ad + bc, bd) \tag{11.1}$$

$$(a, b) \cdot (c, d) = (ac, bd) \tag{11.2}$$

oraz relację R:

$$(a, b)R(c, d) \Longleftrightarrow ad = bc \tag{11.3}$$

Twierdzenie 11.4 *Dla dowolnego pierścienia całkowitego P relacja R zdefiniowana przez 11.3 jest relacją równoważności zgodną z działaniami 11.1 i 11.2.*

Dzięki twierdzeniu 11.4 w zbiorze ilorazowym $P \times P^*/R$ można wprowadzić działania dodawania i mnożenia:

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)] \tag{11.4}$$

$$[(a,b)] \cdot [(c,d)] = [(ac, bd)] \tag{11.5}$$

Twierdzenie 11.5 (O ciele ułamków) *Dla dowolnego pierścienia całkowitego P zbiór $P \times P^*/R$ z działaniami zdefiniowanymi wzorami 11.4 i 11.5 jest ciałem przemiennym.*

Ciało występujące w tezie twierdzenia 11.5 nazywamy **ciałem ułamków** pierścienia P.

Dla wielomianu $v \in P[x]$ (gdzie P jest pewnym pierścieniem całkowitym) można zastanawiać się, kiedy element $\frac{a}{b}$ z ciała ułamków pierścienia P może być pierwiastkiem v (w niemal oczywisty sposób możemy przrecież traktować wielomian v jako wielomian nad ciałem ułamków pierścienia P). Rozwiązanie tego problemu przypomina znane ze szkoły twierdzenie o pierwiastkach wymiernych wielomianów o współczynnikach całkowitych.

Twierdzenie 11.6 *Niech P będzie pierścieniem całkowitym, F ciałem ułamków pierścienia P, zaś a i b względnie pierwszymi elementami P. Jeżeli element $\frac{a}{b} \in F$ jest pierwiastkiem wielomianu*

$$P[x] \ni v = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

wówczas $a|a_0$ oraz $b|a_n$.

Dow. ...

Rozdział 12

Wykład 12 - 13.I.2010

12.1 Kryterium Eisensteina

Bardzo często zamiast mówić, że wielomian jest nierozkładalny mówimy, że jest **nieprzywiedlny**. Kryterium Eisensteina[1] bardzo ważnym, często stosowanym warunkiem wystarczającym nieprzywiedlności wielomianów nad pierścieniem Gaussa.

Twierdzenie 12.1 *Niech P będzie pierścieniem Gaussa, $p \in P[x]$, $p = a_0 + a_1x + \cdots + a_nx^n$. 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 p jest nierozkładalny w P (a co za tym idzie, także w F - ciele ułamków pierścienia P).

Dow. ...

Zauważmy, że dla dowolnego $n \geq 1$ wielomian $x^n + 2$ jest nierozkładalny na mocy kryterium Eisensteina.[2] Mamy więc przykład nieskończonego zbioru wielomianów nierozkładalnych.

[1] 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 pźniej otrzymał honorowy doktorat Uniwersytetu we Wrocławiu (jeszcze przed tem nim uzyskał habilitacje, w wieku lat 24 w Berlinie). Był członkiem Akademii Getyndze i w Berlinie. Gauss miał o nim powiedzieć, że *było tylko trzech matematyków o epokowym znaczeniu: Archimedes, Newton i Eisenstein.* No cóż, w końcu jednak wyszło na to, że to jednak wyniki Gaussa przetrwały i wpłynęły na rozwój nauki, przede wszystkim zaś matematyki w znacznie większym stopniu. Choć porównywanie tu nie bardzo ma jakikolwiek sens.

[2] Zauważmy także, że 2 można tu zastąpić dowolną liczbą pierwszą $\neq \pm 1$ i otrzymać także wielomian nierozkładalny w $\mathbf{Z}[x]$.

12.2 Pierścienie ilorazowe

Twierdzenie 12.2 *Niech P będzie pierścieniem, a $D \subset P$ jego podpierścieniem. Relacja R_D zdefiniowana w D wzorem*

$$aR_Db \iff a - b \in D$$

jest relacją równoważności w D.

Dow. ... Ćwiczenie!

Zbiór klas równoważności P/R_D nazywamy **ilorazem pierścienia P przez podpierścień D i oznaczamy przez P/D.**

Twierdzenie 12.3 *W dowolnym pierścieniu P i dla dowolnego podpierścienia $D \subset P$ relacja R_D jest zgodna z działaniami pierścienia wtedy i tylko wtedy, gdy D jest ideałem pierścienia P.*

Dow. ... Ćwiczenie!

Twierdzenie 12.4 (O ilorazie pierścienia przez ideał) *Jeśli I jest ideałem pierścienia P, to P/I jest pierścieniem (przemiennym, jeśli P jest przemienny, z jedynką, jeśli P jest z jedynką).*

Dow. ... Ćwiczenie

Zauważmy, że zerem pierścienia P/I jest I. Jeśli P jest pierścieniem, zaś I jego ideałem, wówczas pierścień P/I nazywamy **pierścieniem ilorazowym**.

12.3 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 12.5
1. *Obraz homomorfizmu pierścieni $h : P \to Q$ jest podpierścieniem pierścienia Q.*
2. *Jądro homomorfizmu pierścieni $h : P \to Q$ jest ideałem pierścienia P.*

Twierdzenie 12.6 *Dla dowolnych pierścieni P, Q homomorfizm pierścieni $h : P \to Q$ jest monomorfizmem wtedy i tylko wtedy, gdy $Ker\ h = \{0\}$.*

Dow. Ćwiczenie!

Twierdzenie 12.7 (Podstawowe o izomorfiźmie 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 homomorfiźmie k.

Dow. ...

12.4 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).
Wielomian n zmiennych $\mathbf{x_1}, ..., \mathbf{x_n}$ definiujemy rekurencyjnie poprzez (rekurencyjną) definicję 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).

12.4.1 Wielomiany symetryczne

Twierdzenie 12.8 (Wzory Viety) *Niech K będzie ciałem. Jeśli $K[x] \ni v = a_0 + a_1 x + \ldots + a_n x^n$ jest wielomianem stopnia n o n pierwiastkach $\alpha_1, \ldots, \alpha_n$ (niekoniecznie różnych) należących do pewnego ciała $L \supset K$, wówczas*

$$v = k(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$$

i zachodzą wzory (zwane **wzorami Viety***):*

$$a_n = k$$

$$a_{n-1} = -k(\alpha_1 + \ldots + \alpha_n)$$

$$a_{n-2} = k(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n)$$

$$\ldots$$

$$a_0 = k(-1)^n \alpha_1 \cdot \ldots \cdot \alpha_n$$

Dowód - praktycznie oczywisty: wystarczy porównać współczynniki wielomianu we wzorze

$$a_0 + a_1x + \ldots + a_nx^n = k(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$$

***r*-tym podstawowym wielomianem symetrycznym** $S_r(x_1, \ldots, x_n)$ nazywamy wielomian n zmiennych $x_1, \ldots, x_n$ który jest sumą wszystkich różnych iloczynów r różnych zmiennych.

Przykład.
$n = 4, r = 1$: $S_1(x_1, \ldots, x_5) = x_1 + x_2 + x_3 + x_4 + x_5$
$n = 5, r = 3$: $S_3(x_1, \ldots, x_5) = x_1x_2x_3 + x_1x_2x_4 + \ldots + x_3x_4x_5$

Wniosek 12.9 (Inna postać tw.Viety) *Jeżeli* $\alpha_1, \ldots, \alpha_n \in L$ *są pierwiastkami wielomianu* $v \in K[x]$ *(gdzie ciało* K *jest podciałem ciała* L*),* $v = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ *to*

$$a_r = (-1)^r S_r(\alpha_1, \ldots, \alpha_n)$$

Stąd ważny (zobaczycie!) wniosek.

Wniosek 12.10 *Jeśli* $\alpha_1, \ldots, \alpha_n \in L$ *są pierwiastkami wielomianu* $v \in K[x]$ *(gdzie* K *jest podciałem ciała* L*), to*

$$S_r(\alpha_1, \ldots, \alpha_n) \in K$$

dla każdego $r, 1 \leq r \leq n$.

Wielomian $v \in P[\mathbf{x_1}, ..., \mathbf{x_n}]$ nazywamy **symetrycznym** jeżeli dla dowolnej permutacji $\sigma \in S_n$ zachodzi wzór

$$v(\mathbf{x_{\sigma 1}}, ..., \mathbf{x_{\sigma n}}) = \mathbf{v}(\mathbf{x_1}, ..., \mathbf{x_n})$$

Twierdzenie 12.11 (Podstawowe o wielomianach symetrycznych) *W dowolnym opierścieniu z jedynką* D *dla każdego wielomianu symetrycznego* $v \in D[x_1, \ldots, x_n]$ *istnieje dokładnie jeden wielomian* $w \in D[x_1, \ldots, x_n]$ *taki, że*

$$v(x_1, \ldots, x_n) = w(S_1(x_1, \ldots, x_n), \ldots, S_n(x_1, \ldots, x_n))$$

Twierdzenie to udowodnię na następnym wykładzie.

Rozdział 13

Wykład 13 - 20.I.2010

Wykład rozpoczęliśmy od bardzo pożytecznego i ważnego ze względu na zastosowania aktualne i w przeszłości, twierdzenia Wilsona (1741-1793)[1]

13.1 Twierdzenie Wilsona

Twierdzenie 13.1 (Twierdzenie Wilsona) *Liczba $p \in \mathbf{N}$ jest pierwsza wtedy i tylko wtedy, gdy*

$$(p-1)! + 1 \equiv 0(\ mod\ p)$$

Dow. ...

Po twierdzeniu Wilsona przeszliśmy i dowodzie Podstawowego Twierdzenia o Wielomianach Symetrycznych (Gauss), przeszliśmy do jednego z ważniejszych twierdzeń wykładu, mianowicie do Zasadniczego Twierdzenia Algebry (Gauss, jakżeby inaczej!). W dowodzie tego twierdzenia byłem zmuszony korzystać z pojęcia **ciała rozkładu** i Twierdzenia o Ciele Rozkładu. Pewno Twierdzenia o Ciele Rozkładu nie zdąże już przedstawić, lecz samo pojęcie takiego ciała jest proste, a twierdzenie *intuicyjnie akceptowalne*. Zainteresowanych odsyłam do [13, 12].

13.2 Ciało rozkładu

Ciałem rozkładu wielomianu $v \in K[x]$ nazywamy najmniejsze ciało, w którym v rozkłada się na iloczyn czynników liniowych

$$v = a(x - b_1) \dots (x - b_n)$$

Ciało to oznaczamy $K(b_1, \dots, b_n)$

[1] Jak widać, poodczas wykładu podałem błędną informację mówiąc, że Sir John Wilson, autor twierdzenia o którym mowa, był matematykiem żyjącym w XIX wieku. Ciekawostką jest także, że Wilson tego twierdzenia nie udowodnił, a jedynie stwierdził, odkrył (a więc, jak należy sądzić, raczej podejrzewał), że jest prawdziwe. Przypisanie więc twierdzenia Wilsona Wilsonowi jest nie do końca słuszne. Pierwszy dowód podał Lagrange w 1773 roku.

Twierdzenie 13.2 (O Ciele Rozkładu) *Dla dowolnego ciała K i wielomianu $v \in K[x]$ istnieje rozszerzenie $L : K$ w którym v rozkłada się na iloczyn czynników liniowych.*

Przykłady: $\mathbf{Q}(\sqrt{2})$ (ciało rozkładu wielomianu $\mathbf{x}^2 - 2$ (nad $\mathbf{Q}$), $\mathbf{C}$ (ciało rozkładu $\mathbf{x} + 1$ nad $\mathbf{R}$).

13.3 Zasadnicze Twierdzenie Algebry

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 $d = \partial v$, $u_1, ..., u_d, a \in K$.

Twierdzenie 13.3 *Ciało liczb zespolonych jest algebraicznie zamknięte.*

Dowód (niedokończony, c.d. będzie na wykładzie następnym).
Podzielić go można na kilka części.
1. Wykażemy, że twierdzenie wystarczy wykazać dla wielomianach o współczynnikach rzeczywistych.
Niech $v \in \mathbf{C}[\mathbf{x}]$. Oznaczmy przez $\bar{v}$ wielomian powstały przez sastąpienie 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, $w(\mathbf{x}) = \sum_{l=0}^{d}(\sum_{i=0}^{l} \bar{a_i}a_{l-i})\mathbf{x}^l$. Łatwo sprawdzić, że

$$\bar{b_l} = \sum_{i=0}^{l} a_i\bar{a}_{l-i} = b_l$$

Czyli $b_l \in \mathbf{R}$ dla wszystkich l.
Jeśli, dla pewnego $u \in \mathbf{C}$ $w(u) = 0$, wówczas $v(u)\underline{\bar{v}(u)} = 0$, 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.
A więc, wielomian v (dowolny wielomian o współczynnikach rzespolonych) 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 $v \in \mathbf{R}$, $\partial v = d = 2^n m$, 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 $n = 0$, wówczs v jest stopnia nieparzystego - wiemy (także jeszcze ze szkoły!), że każdy wielomian o współczynnikach rzeczywistych i stopnia nieparzystego ma pierwiastek (i to rzeczywisty).

Przypuśćmy więc, że $n \geq 1$ i niech $u_1, ..., u_d$ będą pierwiastkami wielomianu v w jego ciele rozkładu[2]. Wówczas $v(\mathbf{x}) = a(\mathbf{x} - u_1) \cdot ... \cdot (\mathbf{x} - u_d)$ gdzie $a \in \mathbf{R}$. Oczywiście

$$v(\mathbf{x}) = a\mathbf{x}^d + aS_1(u_1, ..., u_d)\mathbf{x}^{d-1} + ...(-1)^d aS_d(u_1, ..., u_d)\mathbf{x}^d$$

i dla każdego $k = 1, ..., d$ $S_k(u_1, ..., u_d) \in \mathbf{R}[\mathbf{x}]$.

Dla dowolnego $h \in \mathbf{Z}$ 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 $v_h \in \mathbf{R}[\mathbf{x}, \mathbf{x}_1, ..., \mathbf{x}_d] = \mathbf{R}[\mathbf{x}][\mathbf{x}_1, ..., \mathbf{x}_d]$. Co więcej, dla ustalonego $h \in \mathbf{Z}$ 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 $S_1(\mathbf{x}_1, ..., x_d), ..., S_d(x_1, ..., x_d)$ o współczynnikach w $\mathbf{R}[\mathbf{x}]$. Skoro $S_1(u_1, ..., u_d), ..., S_d(u_1, ..., u_d) \in \mathbf{R}$ także wielomian $v_h(\mathbf{x}, u_1, ..., u_d)$ (a więc wielomian zmiennej $\mathbf{x}$) ma współczynniki w $\mathbf{R}$ (dla każdego całkowitego h). Stopień tych wielomianów (bo dla każdego $h \in \mathbf{Z}$ mamy jeden) wielomianu **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 $\mathbf{C}$ (to, że te wielomiany mają pierwiastki, to nic ciekawego, wiadomo z Twierdzenia o Ciele Rozkładu - ważne jest to, że te pierwiastki są w $\mathbf{C}$!).

Wobec tego każdy wielomian (dla każdego $h \in \mathbf{Z}$) ma pierwiastek w $\mathbf{C}$, a stąd relacja

$$u_i + u + j + hu_i u_j \in \mathbf{C}$$

jest spełniona dla nieskończonej liczby parametrów h. Muszą więc istnieć i oraz j (ustalone) oraz takie h i h', oba całkowite, $h \neq h'$, że

$$u_i + u_j + hu_i u_j \in \mathbf{C}$$

$$u_i + u_j + h'u_i u_j \in \mathbf{C}$$

Stąd łatwo wywnioskować, że

$$u_i + u_j \in \mathbf{C}$$

oraz

$$u_i u_j \in \mathbf{C}$$

A więc $(\mathbf{x} - u_i)(\mathbf{x} - u_j) \in \mathbf{C}[\mathbf{x}]$. Równanie zaś kwadratowe o współczynnikach zespolonych ma rozwiązania zespolone (a więc $u_i, u_j \in \mathbf{C}$). ■

[2]Tu właśnie korzystamy z Twierdzenia o Ciele Rozkładu.

Rozdział 14

Wykład 14 - 27.I.2010

14.1 Rozszerzenia ciał

Rozszerzeniem ciała K nazywamy ciało L takie, że istnieje monomorfizm $T : K \to L$. Piszemy wtedy $L : K$ (taki napis czytamy *ciało L jest rozszerzeniem ciała K*).
Oczywiście, jeśli ciało K jest podciałem ciała L, wówczas $L : K$. Co więcej, z taką sytuacją będziemy mieli do czynienia najczęściej (choć nie zawsze). Czasami ciało K nazywamy *małym* zaś L *dużym*.

Ciałem generowanym przez $X \subset K$ nazywamy najmniejsze ciało zawierające K.

Ciało generowane przez $X \subset K$ jest równe[1]:

- przecięciu wszystkich podciał ciała K zawierających X,
- zbiorowi elementów które można otrzymać w ciągu skończonym operacji (działań w ciele) na elementach z X (o ile $X \neq \emptyset$).

Niech $L : K$, $X \subset L$. Ciałem powstałym z K przez **dołączenie** X nazywamy ciało generowane w L przez $K \cup X$.

Przykład 14.1 $\mathbf{Q}(i, \sqrt{2})$

Rozszerzenie ciała K o element $a \in L$ nazywamy **rozszerzeniem prostym** i oznaczamy przez $K(a)$ (zamiast $K(\{a\})$). Rozszerzenia o zbiór skończony $\{a_1, \ldots, a_n\}$ oznaczamy przez $K(a_1, \ldots, a_n)$.

Ćwiczenie 14.1 *Sprawdź, że* $\mathbf{Q}(i, -i, \sqrt{3}, -\sqrt{3})$ *jest rozszerzeniem prostym.*

[1] O tym podczas wykładu nie powiedziałem - a więc dowód nie obowiązuje.

14.1.1 Rozszerzenia skończone, algebraiczne i przestępne

Jeśli L i K są ciałami i $L : K$ i wymiar przestrzeni wektorowej L nad ciałem K wynosi n to mówimy, że $n = [L : K]$ jest wymiarem ciała L nad K. Rozszerzenie L nazywamy wówczas **skończonym**. **Bazą** ciała L nad K nazywamy bazę L (traktowanego jako przestrzeń wektorowa nad K). L jest **rozszerzenienm nieskończonym** L, jeśli nie jest rozszerzeniem skończonym.

Element $a \in L$ nazywamy **algebraicznym** nad K jeśli a jest pierwiastkiem pewnego, niezerowego wielomianu $v \in K[\mathbf{x}]$. **Liczbą algebraiczną** nazywamy dowolny element algebraiczny nad ciałem $\mathbf{Q}$.

Przykład 14.2 *Sprawdź, że* $i, \sqrt{3}, \sqrt{2+\sqrt{2}}$ *oraz* $i+\sqrt{3}$ *są liczbami algebraicznymi. Wskaż ich wielomiany minimalne.*

Twierdzenie 14.1 (Cantora) *Zbiór liczb algebraicznych jest przeliczalny.*

Element $a \in L$ nazywamy **elementem przestępnym** nad K (gdzie $L : K$), jeżeli a nie jest algebraiczny nad K. Elementy przestępne nad $\mathbf{Q}$ nazywamy **liczbami przestępnymi**.

Wniosek 14.2 (O liczbach przestępnych) *Zbiór liczb przestępnych jest nieprzeliczalny.*

Rozszerzenie L ciała K nazywamy **algebraicznym** jeżeli każdy element $a \in L$ jest algebraiczny nad K.

Przykład 14.3 *Wszystkie dotychczasowe przykłady.*
$\mathbf{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$
Podaj inne, nietrywialne przykłady.

Twierdzenie 14.3 (O rozszerzeniach skończonych) *Każde rozszerzenie skończone jest rozszerzeniem algebraicznym.* Co więcej, jeśli $[L : K] = k$ i $a_1, \ldots, a_k$ jest bazą L nad K, to $L = K(a_1, \ldots, a_k)$ i każdy element $b \in L$ jest elementem algebraicznym stopnia co najwyżej k nad K[2].

Twierdzenie 14.4 (O wielomianie minimalnym) *Dla każdego elementu $a \in L$ algebraicznego nad K istnieje dokładnie jeden wielomian unormowany*[3] *$v \in K[\mathbf{x}]$ taki, że*

- *v jest nierozkładalny na K,*
- *$v(a) = 0$,*
- *v dzieli każdy wielomian $w \in K[\mathbf{x}]$ którego a jest pierwiastkiem*[4]*.*

[2] Części twierdzenia wypisanej tu "prostońa wykładzie nie sformułowałem, choć de facto udowodniłem. Jednak nie obowiązuje na egzaminie.

[3] To znaczy taki, którego współczynnik dominujący (przy najwyższej potędze) jest równy jedynce.

[4] O tym twierdzeniu na wykładzie nie mówiłem. Pozostaje dla ciekawych, ale na egzaminie nie będę z niego pytał. Ani z tego co jest tuż po tym twierdzeniu (3 linijki).

Wielomian v o którym mówi twierdzenie 14.4 nazywamy **wielomianem minimalnym elementu algebraicznego** a, zaś stopień tego wielomianu **stopniem elementu** a.

14.2 Ciało rozkładu

Przypomnijmy znane 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

$$I + a$$

gdzie $a \in P$. Działania w pierścieniu są wtedy określona wzorami:

$$(I + a) + (I + b) = I + (a + b)$$

$$(I + a)(I + b) = I + ab$$

Przypomnijmy także, że jeśli K jest ciałem, to $K[\mathbf{x}]$ jest pierścieniem głównym. łatwo jest udowodnić następujące twierdzenie. Ćwiczenie!

Twierdzenie 14.5 *Jeśli K jest ciałem, $v \in K[\mathbf{x}]$, $\partial v = n$, wówczas*

$$K[\mathbf{x}]/(v) = \{(v) + w : \ w \in K[\mathbf{x}], \partial w \leq n - 1\}$$

Przykład. Ułóż tabelkę działań dla $\mathbf{Z}_2[\mathbf{x}]/(\mathbf{x}^2 + 1)$, $\mathbf{Z}_5[\mathbf{x}]/(x^2 + x + 3)$, ... może jeszcze coś?

Twierdzenie 14.6 *Jeśli K jest ciałem a $v \in K[\mathbf{x}]$ wielomianem nierozkładalnym nad K, wówczas $K[\mathbf{x}]/(v)$ jest ciałem.*

Dow. ...

Ćwiczenie. Dla jakich wartości $a \in \mathbf{Z}_3$ pierścień ilorazowy $\mathbf{Z}_3[\mathbf{x}]/(x^2 + a)$! jest ciałem?

Zauważmy, że ciało $K[\mathbf{x}]/(v)$ (gdzie v jest wielomianem nieprzywiedlnym nad K) zawiera podciało izomorficzne z K. Tym podciałem jest zbiór

$$\{[a] : a \in K\} = \{(v) + a : a \in K\}$$

Izomorfizmem jest $T : K \ni a \to (v)+a$. Dlatego też $K[\mathbf{x}]/(v)$ jest rozszerzeniem K $(K[\mathbf{x}]/(v) : K)$.

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, jest to ciało $K(b_1, \dots, b_n)$

Twierdzenie 14.7 (O ciele rozkładu) *Dla dowolnego ciała K i wielomianu $v \in K[\mathbf{x}]$ istnieje rozszerzenie $L : K$ w którym v rozkłada się na iloczyn czynników liniowych.*

Dow. ...
Dowodu w *Notatkach ...* nie podaję. Zwracam tylko uwagę na 2 fakty:

- Dowód jest indukcyjny ze względu na $n = \partial v$.
- Chyba najbardziej istotną częścią dowodu jest dowód przypadku, gdy v nad K jest nierozkładalny. Wtedy jako rozszerzenie bierze się ciało[5] $K[\mathbf{x}]/(v)$ w którym pierwiastkiem wielomianu v jest $(v) + x$.

[5]To po to właśnie dowodziliśmy twierdzenie 14.6 $K[x]/(v)$, w którym pierwiastkiem v okazuje się być $(v) + x$.

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] D.A. Cox, Galois theory, Wiley 2004.

[7] W.J Gilbert, W.K. Nicholson, Algebra współczesna z zastosowaniami, WNT, Warszawa 2008.

[8] D.W. Hardy i C.L. Walker, Applied Algebra: Codes, Ciphers and Discrete Algorithms, Prentice Hall 2003.

[9] N. Koblitz, Algebraiczne aspekty kryptografii, WNT, Warszawa 200

[10] A.I. Kostrykin, Wstęp do algebry, cz. 1 Podstawy algebry, PWN Warszawa 2004.

[11] A.I. Kostrykin, Wstęp do algebry, cz. 3 Podstawowe struktury algebraiczne, PWN Warszawa 2005

[12] W.K. Nicholson, Introduction to Abstract Algebra, Third Edition, Wiley 2007.

[13] Z. Opial, Algebra wyższa, PWN, Warszawa 1975.

[14] E.R. Scheinerman, Mathematics - Discrete Introduction, Brooks/Cole 2000.

[15] I. Stewart, Galois Theory, Chapman and Hall Mathematics, Londyn, Nowy York 1989.