Paweł Gładki

Algebra

http://www.math.us.edu.pl/ ~ pgladki/

Konsultacje: *Środa, 14:00-15:00*

Jeżeli chcesz spotkać się z prowadzącym podczas konsultacji, postaraj się powiadomić go o tym przed lub po zajęciach, zadzwoń do jego pokoju, lub wyślij mu emaila.

Zasady zaliczania przedmiotu:

2 kolokwia, każde warte 15 punktów, 2 sprawdziany, każdy warty 6 punktów, aktywność na zajęciach, warta 3 punkty, zadania domowe, warte 15 punktów, egzamin, warty 40 punktów.

Do egzaminu przystępują tylko te osoby, które uzyskają zaliczenie z ćwiczeń. Warunkiem zaliczenia ćwiczeń jest zdobycie co najmniej 30 punktów. Warunkiem zdania egzaminu jest zdobycie co najmniej 60 wszystkich punktów.

Sprawdziany odbędą się na zajęciach **3 marca** i **28 kwietnia**. Kolokwia odbędą się na zajęciach **31 marca** i **26 maja**. Egzamin odbędzie się **9 czerwca.**

Każde kolokwium będzie trwało 90 minut, każdy sprawdzian 20 minut, a egzamin końcowy 180 minut.

Zadania domowe:

Do każdego wykładanego tematu został opracowany zestaw zadań, który należy rozwiązać w Moodle:

`http://el2.us.edu.pl/wmfich/`
→ *Inne matematyka*
→ *Algebra dla WIiNoM (studia stacjonarne)*

Dostępnych jest 13 zadań domowych na każdy tydzień zajęć za wyjątkiem tygodni, w których odbywać się będą kolokwia. Każdy zestaw składa się z 10 zadań, które zostaną udostępnione w każdy czwartek, w który odbywać się będą zajęcia i które muszą zostać rozwiązane nie później niż do kolejnego czwartku.

Uwaga! Zadania rozwiązywać należy w Moodle Wydziału Matematyki, Fizyki i Chemii, a nie w Moodle Wydziału Informatyki i Nauk o Materiałach. Studenci, którzy jeszcze nie mają konta zobowiązani są do jak najszybszego jego założenia.

Plan wykładu:

02.17 NWD, NWW i algorytm Euklidesa.
02.24 Grupa, pierścień, ciało.
03.03 Ciało liczb zespolonych.
03.10 Pierścień wielomianów.
03.17 Pierścienie ilorazowe. Ideały pierwsze i maksymalne. Konstrukcja ciał p^n-elementowych.
03.24 Układy równań liniowych.
03.31 Działania na macierzach.
04.14 Wyznaczniki.
04.21 Przestrzenie linowe. Podprzestrzenie.
04.28 Kombinacje liniowe wektorów.
05.05 Baza i wymiar.
05.12 Struktura zbioru rozwiązań układu równań.
05.19 Przekształcenia liniowe.
05.26 Macierze przekształceń liniowych.
06.02 Podprzestrzenie niezmiennicze. Wektory i wartości własne.

Literatura:

1. G. Banaszak, W. Gajda, *Elementy algebry liniowej, cz.I,* WNT 2002.
2. G. Banaszak, W. Gajda, *Elementy algebry liniowej, cz.II,* WNT 2002.
3. A. Białynicki-Birula, *Algebra,* PWN 1971.
4. A. Białynicki-Birula, *Algebra liniowa z geometrią,* PWN 1976.
5. N. W. Jefimow, E. R. Rozendorn, *Algebra liniowa wraz z geometrią wielowymiarową,* PWN 1976.
6. A. J . Kostrykin, *Wstęp do algebry, cz.I: Podstawowe struktury algebraiczne,* PWN 2004.
7. A. J . Kostrykin, *Wstęp do algebry, cz.II: Algebra liniowa,* PWN 2004.

Zbiory zadań:

1. L. Jeśmianowicz , J. Łoś, *Zbiór zadań z algebry,* PWN 1975 oraz 1981.
2. A. I . Kostrykin (red.), *Zbiór zadań z algebry,* PWN 2005.
3. D. K. Fadiejew, I . S. Sominskij, *Sbornik zadacz po wyższej algebrie,* Moskwa 1977 (w jęz. rosyjskim).
4. S. Przybyło, A. Szlachtowski, *Algebra i wielowymiarowa geometria analityczna w zadaniach,* WNT 1992.

NWD, NWW
i algorytm Euklidesa

Twierdzenie o dzieleniu z resztą

Niech $a, b \in \mathbb{Z}$, $b \neq 0$. Wówczas istnieje dokładnie jedna para liczb całkowitych $q, r \in \mathbb{Z}$ taka, że

$$a = qb + r \text{ oraz } 0 \leq r < |b|.$$

Dowód:

Pokażemy najpierw istnienie stosownej pary.
Załóżmy, że $b > 0$ i zdefiniujmy

$$q = \left[\frac{a}{b}\right] \text{ oraz } r = a - bq.$$

Wówczas $q \leq \frac{a}{b} < q + 1$.
Zatem $bq \leq a < bq + b$.
Stąd $0 \leq r = a - bq < b = |b|$.
W przypadku, gdy $b < 0$, definiujemy

$$q = -\left[\frac{a}{|b|}\right] \text{ oraz } r = a - bq$$

i dalej rozumujemy analogicznie.

Pozostaje wykazać jednoznaczność wyboru powyższej pary.
Załóżmy, że $a = bq_1 + r_1 = bq_2 + r_2$, gdzie $0 \leq r_1, r_2 < |b|$.
Wówczas $r_2 - r_1 = b(q_1 - q_2)$.
Jeśli $r_2 - r_1 \neq 0$, to wówczas $|b| \leq |r_2 - r_1| \leq \max\{r_1, r_2\} < |b|$.
Zatem $r_2 - r_1 = 0$ i w konsekwencji $q_1 - q_2 = 0$. $\square$

Definicja:

Niech $a, b \in \mathbb{Z}$, $b \neq 0$, niech $q, r \in \mathbb{Z}$ będą jednoznacznie wyznaczonymi liczbami całkowitymi takimi, że

$$a = qb + r \text{ i } 0 \leq r < |b|.$$

Liczbę q nazywamy **niepełnym ilorazem** z dzielenia a przez b, zaś liczbę r **resztą** z dzielenia a przez b.

Przykłady:

1. Niech $a = 26$, $b = 11$. Bez trudu sprawdzamy, że wówczas $q = 2$ oraz $r = 4$.
2. Niech $a = -26$, $b = 11$. Wówczas $q = -3$, a $r = 7$; w szczególności nie możemy powiedzieć, że resztą z dzielenia -26 przez 11 jest -4, gdyż wprawdzie $-26 = -2 \cdot 11 - 4$, ale $-4 < 0$.

Definicja:

Niech $a, b \in \mathbb{Z}$. Mówimy, że b **dzieli** a (lub że a **jest podzielna przez** b), jeśli dla pewnej liczby całkowitej $q \in \mathbb{Z}$ zachodzi $a = bq$, co oznaczamy $b|a$. W przeciwnym razie piszemy $b \nmid a$. Liczbę q nazywamy **ilorazem** z dzielenia a przez b.

Przykłady:

3. Jest jasne, że $2|4$, $3|18$, $-8|16$ i $157|0$.
4. Bezpośrednio z definicji podzielności wynika też, że $0|a$ wtedy i tylko wtedy, gdy $a = 0$. Widzimy wszakże, że iloraz z dzielenia 0 przez 0 nie jest jednoznacznie określony.

Twierdzenie:

Niech $a, b, c \in \mathbb{Z}$. Wówczas:

1. $a|a$;
2. $a|b \wedge b|c \Rightarrow a|c$;
3. $a|b \wedge b|a \Rightarrow a = b \vee a = -b$;
4. $a|0$;
5. $1|a$;
6. $a|b \Rightarrow a|bc$;
7. $a|b \wedge a|c \Rightarrow a|b + c$.

Dowód:

Udowodnimy dla przykładu część (3) twierdzenia.
Jeżeli $a = 0$, to $a|b$ wtedy i tylko wtedy, gdy $b = 0$, a więc $a = b$.
Podobnie, gdy $b = 0$, to $a = b = 0$, załóżmy więc, że $a, b \neq 0$.
Niech $b = q_1 a$ i $a = q_2 b$, dla pewnych $q_1, q_2 \in \mathbb{Z}$.
W szczególności $q_1, q_2 \neq 0$.
Wówczas $b = q_1 q_2 b$.
Zatem $q_1 q_2 = 1$.
Stąd $q_1 = q_2 = 1$ lub $q_1 = q_2 = -1$. $\square$

Definicja:

Niech $a_1, \ldots, a_k \in \mathbb{Z}$, $k \geq 2$.
Liczbę $d \in \mathbb{N}$ taką, że

1. $d|a_1, \ldots, d|a_k$,
2. $e|a_1, \ldots, e|a_k \Rightarrow e|d$,

nazywamy **największym wspólnym dzielnikiem** liczb $a_1, \ldots, a_k$ i oznaczamy $NWD(a_1, \ldots, a_k)$.
Liczbę $m \in \mathbb{N}$ taką, że

1. $a_1|m, \ldots, a_k|m$,
2. $a_1|n, \ldots, a_k|n \Rightarrow m|n$,

nazywamy **najmniejszą wspólną wielokrotnością** liczb $a_1, \ldots, a_k$ i oznaczamy $NWW(a_1, \ldots, a_k)$.

Przykład:

5. Sprawdzamy, że $NWD(24, 36) = 12$. Zauważmy, że, na przykład, $6|24$ i $6|36$, ale oczywiście $6 \neq NWD(24, 36)$. Ponadto $NWW(24, 26) = 72$. Podobnie zauważmy, że $24|144$ i $36|144$, ale $144 \neq NWW(24, 36)$.

Twierdzenie:

Niech $a, b \in \mathbb{N}$. Wówczas $NWD(a, b) \cdot NWW(a, b) = a \cdot b$.

Dowód:

Rozważmy $\frac{ab}{NWD(a,b)}$.
Ponieważ $a, b, NWD(a,b) \in \mathbb{N}$, widzimy, że $\frac{ab}{NWD(a,b)} \geq 0$.
Ponadto $\frac{ab}{NWD(a,b)} \in \mathbb{Z}$.
Niech $NWD(a,b)q_1 = a$, dla pewnej liczby $q_1 \in \mathbb{N}$.
Wówczas $\frac{ab}{NWD(a,b)} = \frac{NWD(a,b)q_1 b}{NWD(a,b)} = q_1 b$, a więc $b|\frac{ab}{NWD(a,b)}$.
Analogicznie $a|\frac{ab}{NWD(a,b)}$.
Wobec tego $NWW(a,b)|\frac{ab}{NWD(a,b)}$, czyli
$NWW(a,b)NWD(a,b)|ab$.

Rozważmy $\frac{ab}{NWW(a,b)}$.
Zauważmy, że $\frac{ab}{NWW(a,b)} \in \mathbb{N}$.
Niech $NWW(a,b) = s_1 a$, dla pewnej liczby $s_1 \in \mathbb{N}$.
Wówczas $\frac{ab}{NWW(a,b)} = \frac{ab}{s_1 a} = \frac{b}{s_1}$.
Wobec tego $\frac{ab}{NWW(a,b)} | b$.
Analogicznie $\frac{ab}{NWW(a,b)} | a$.
Wobec tego $\frac{ab}{NWW(a,b)} | NWD(a,b)$, czyli
$ab | NWW(a,b)NWD(a,b)$. $\square$

Przykład:

6. Odwołując się do poprzedniego przykładu sprawdzamy, że $NWD(24, 36)NWW(24, 36) = 12 \cdot 72 = 864 = 24 \cdot 36$.

Twierdzenie (algorytm Euklidesa):

Niech $a, b \in \mathbb{Z}$ i niech

$$\begin{aligned}
a &= q_1 b + r_1, \text{ dla } 0 < r_1 < |b|, q_1, r_1 \in \mathbb{Z}, \\
b &= q_2 r_1 + r_2, \text{ dla } 0 < r_2 < r_1, q_2, r_2 \in \mathbb{Z}, \\
r_1 &= q_3 r_2 + r_3, \text{ dla } 0 < r_3 < r_2, q_3, r_3 \in \mathbb{Z}, \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, \text{ dla } 0 < r_n < r_{n-1}, q_n, r_n \in \mathbb{Z}, \\
r_{n-1} &= q_{n+1} r_n, \text{ dla } q_{n+1} \in \mathbb{Z}.
\end{aligned}$$

Wówczas $r_n = NWD(a, b)$.

Dowód:

Algorytm zawsze się zatrzymuje, bo jest tylko skończenie wiele liczb naturalnych w przedziale $[0, |b|]$.
Niech $d = NWD(a, b)$.
Sprawdzamy, że kolejno

$$r_n | r_{n-1}, r_n | r_{n-2}, \ldots, r_n | r_1, r_n | b, r_n | a,$$

a więc w szczególności $r_n | d$.
Podobnie, $d | a$ i $d | b$, a więc kolejno

$$d | r_1, d | r_2, \ldots, d | r_{n-1}, d | r_n.$$

Ponieważ zarówno d jak i r_n są liczbami dodatnimi, oraz równocześnie $d | r_n$ i $r_n | d$, więc $d = r_n$. $\square$

Przykład:

7. Zastosujemy algorytm Euklidesa, aby obliczyć $NWD(66, 48)$. Wykonując kolejne kroki algorytmu otrzymujemy:

$$\begin{aligned} 66 &= 1 \cdot 48 + 18 \\ 48 &= 2 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6, \end{aligned}$$

a więc $NWD(66, 48) = 6$.

Przykład:

8. Dane wygenerowane przez algorytm Euklidesa pozwalają wyznaczyć liczby całkowite x i y takie, że

$$66x + 48y = NWD(66, 48).$$

Istotnie, zaczynając od przedostatniego kroku i kolejno podstawiając otrzymujemy:

$$\begin{aligned} 6 &= 18 - 12 \\ &= 18 - (48 - 2 \cdot 18) = 3 \cdot 18 - 48 \\ &= 3(66 - 48) - 48 = 3 \cdot 66 - 4 \cdot 48, \end{aligned}$$

a więc $x = 3$ i $y = -4$.

Uwaga:

Niech $a, b, c \in \mathbb{Z}$. Algorytm Euklidesa dostarcza metody rozwiązywania równań

$$ax + by = c$$

w liczbach całkowitych.

Twierdzenie:

Niech $a, b, c \in \mathbb{Z}$. Równanie

$$ax + by = c$$

ma rozwiązanie w liczbach całkowitych wtedy i tylko wtedy, gdy $d = NWD(a, b)|c$.

Dowód:

$(\Rightarrow)$: Załóżmy, że $ax_0 + by_0 = c$, dla pewnych liczb $x_0, y_0 \in \mathbb{Z}$. Wówczas, skoro $d|a$ i $d|b$, więc $d|ax_0$ i $d|by_0$, a zatem również $d|ax_0 + by_0 = c$.

($\Leftarrow$) : Załóżmy, że $d|c$ i niech $q \in \mathbb{Z}$ będzie taką liczbą, że $dq = c$.
Stosując algorytm Euklidesa znajdujemy liczby całkowite $x_1, y_1 \in \mathbb{Z}$ takie, że $ax_1 + by_1 = d$.
Wówczas $aqx_1 + bqy_1 = c$. $\square$

Przykład:

9. Rozwiążemy równanie $66x + 48y = 18$. Na podstawie poprzedniego przykładu wiemy już, że $66 \cdot 3 + 48 \cdot (-3) = 6$, a więc $66 \cdot 9 + 48 \cdot (-12) = 18$.

Twierdzenie:

Niech $a, b, c \in \mathbb{Z}$ i niech $d = NWD(a, b)|c$. Niech $x_0, y_0 \in \mathbb{Z}$ będą rozwiązaniami równania $ax + by = c$. Wówczas wszystkie całkowite rozwiązania tego równania dane są przez

$$x = x_0 + \frac{bt}{d} \text{ oraz } y = y_0 - \frac{at}{d}, t \in \mathbb{Z}.$$

Dowód:

Sprawdzamy, że

$$a\left(x_0 + \frac{bt}{d}\right) + b\left(y_0 - \frac{at}{d}\right) = ax_0 + by_0 = c.$$

Dalej, niech $x, y \in \mathbb{Z}$ będzie rozwiązaniem równania $ax + by = c$.
Wtedy $ax + by = c = ax_0 + by_0$.
Stąd $a(x - x_0) = b(y_0 - y)$.
Jeżeli $a = a_1 d$ i $b = b_1 d$, dla pewnych $a_1, b_1 \in \mathbb{Z}$, to wówczas też $a_1(x - x_0) = b_1(y_0 - y)$.
Ponieważ $NWD(a_1, b_1) = 1$, więc $b_1 | x - x_0$.
Niech $x - x_0 = b_1 t$, dla pewnego $t \in \mathbb{Z}$.
Stąd $x = x_0 + b_1 t = x_0 + \frac{bt}{d}$.
Ponadto $a_1 b_1 t = b_1(y_0 - y)$, skąd $y = y_0 - \frac{at}{d}$. $\square$

Przykład:

10. Wszystkie rozwiązania równania

$$66x + 48y = 18$$

wyrażą się wzorami

$$x = 9 + 8t, y = -12 - 11t, t \in \mathbb{Z}.$$