Rozwiązania egzaminu z algebry 1

Mikołaj Znamierowski

21 lutego 2025

Ostatnio pomagałem w rozwiązywaniu tych zadań, a więc, jak już rozwiązania są gotowe, to postanowiłem się nimi podzielić z innymi - może komuś pomogą w przygotowaniu się do własnego egzaminu. Potraktowałem ten plik jako swego rodzaju skrypt do rozwiązywania zadań egzaminacyjnych - postarałem się zawrzeć weń wszystkie najważniejsze schematy rozumowań, z których wynika większość zadań, jakie mogą się trafić. Jest to świetny egzamin do tych celów, gdyż pojawiło się nań większość takich pomysłów. Przy okazji, do niektórych z zadań dodałem kilka ciekawostek, które mogą się spodobać głodnym wiedzy :)

1 Część teoretyczna

Rozwiązuję tylko podpunkty (b), bo (a) to jedynie podawanie znanych definicji i faktów z wykładu/skryptu.

1. Permutacji zbioru $\{1, 2, \ldots, n\}$ jest $n!$ (na miejsce 1 wstawiamy liczbę od 1 do n na n sposobów, potem na każde następne liczbę jeszcze nieużytą na $n-1$, $n-2$, ... sposobów). Permutacji parzystych z kolei jest tyle samo, co nieparzystych (między tymi zbiorami jest bijekcja będąca mnożeniem przez transpozycję $(1,2)$), więc $|A_n| = \frac{n!}{2} = \frac{1}{2}|S_n|$. Stąd, $[S_n : A_n] = 2$, a to, jak wiadomo, implikuje normalność $A_n \trianglelefteq S_n$.

2. Mnożenie $(aH) \cdot (bH) = (ab)H$ jest sensownie określone (tzn. nie zależy od wyboru reprezentantów warstw), gdyż jeśli $aH = a'H$, $bH = b'H$, to $a^{-1}a' \in H$ oraz $b^{-1}b' \in H$, czyli

$$(ab)^{-1}a'b' = b^{-1}a^{-1}a'b' = b^{-1}(a^{-1}a')b \cdot b^{-1}b' \in H$$

   bo pierwszy człon (przed znakiem mnożenia) to sprzężenie elementu $a^{-1}a' \in H$ elementem $b \in G$, które, z normalności H, leży w H; zaś drugi człon to po prostu element H, czyli ich iloczyn leży w H. Stąd więc faktycznie $(ab)H = (a'b')H$.

3. $\mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_5$, bo $NWD(2,5) = 1$. Dokładniej: grupa po prawej stronie ma element $(1,1)$ rzędu 10, a przy tym jest 10-elmentowa, czyli jest to 10-elementowa grupa cykliczna, a więc taka sama, jak $\mathbb{Z}_{10}$. Pamiętajmy przy tym, że rozpatrując $\mathbb{Z}_n$ jako grupę (cykliczną) mamy na myśli, że operacją grupową jest dodawanie modulo n (więc elementem neutralnym jest 0). Z kolei S_3 nie jest iloczynem prostym swoich dwóch podgrup właściwych. Aby to zobaczyć, zauważmy, że $|S_3| = 3! = 6$, czyli jedyne podgrupy właściwe S_3 mają moce 2 i 3 (bo muszą to być różne od 6 i 1 liczby dzielące liczbę 6), więc są to podgrupy cykliczne. Stąd, gdyby S_3 było iloczynem prostym tych podgrup, to $S_3 \simeq \mathbb{Z}_3 \times \mathbb{Z}_2 \simeq \mathbb{Z}_6$, czyli w szczególności S_3 byłoby abelowe (nawet cykliczne), a nie jest, bo na przykład

$$(12)(23) = (312) \neq (321) = (23)(12)$$

4. Załóżmy, że element p dziedziny R jest pierwszy, a przy tym rozkładalny, czyli, że $p \neq 0$ i można go rozłożyć na iloczyn dwóch nieodwracalnych elementów, tzn. $p = ab$, gdzie $a, b \notin \mathcal{U}(R)$. Skoro $p = ab$, to $p|ab$, więc (skoro p jest pierwszy), $p|a$ lub $p|b$. Bez straty ogólności przyjmijmy, że $p|a$. Oznacza to, że $a = pr$ dla pewnego $r \in R$. Wówczas $p = ab = prb$, więc skoro R jest dziedziną, to $1 = rb$ (bo $p(1-br) = 0$, $p \neq 0$, czyli $1 - br = 0$), ale to oznacza, że b jest odwracalny - sprzeczność.

5. Przykładów można podawać dużo (najbardziej popularnym chyba jest $\mathbb{Z}[\sqrt{5}]$), ale wydaje mi się, że najszybszy w uzasadnieniu jest ten: Jeśli $\mathbb{K}$ jest ciałem, to $R = \mathbb{K}[x^2, x^3]$ jest dziedziną (bo, ze względu na stopnie wielomianów, zero można otrzymać jedynie mnożąc wielomiany stałe, a przy tym wielomiany stałe to elementy ciała, co już oczywiście jest dziedziną) bez jednoznaczności rozkładu (bo element x^6 ma dwa rozkłady $x^3 \cdot x^3$ i $x^2 \cdot x^2 \cdot x^2$, o różnych liczbach czynników nierozkładalnych - elementy te są nierozkładalne ze względu na stopnie, bo w R nie ma elementu x).

2 Część zadaniowa

1. Zauważmy, że $I+J = R$. Istotnie, $3 \in I$ oraz $5 \in J$, więc $2 = 5-3 \in I+J$, więc też $1 = 3-2 \in I+J$. Stąd w szczególności $I + J$, jako cały pierścień, jest ideałem pierwszym w R. Ponadto, na mocy Chińskiego Twierdzenia o Resztach (CRT) mamy $R/(I \cap J) \simeq R/I \times R/J \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$ - nie jest to dziedzina, gdyż $3 \cdot 5 = 0$ jest zerowym iloczynem niezerowych elementów. Stąd więc $I \cap J$ nie jest pierwszy (bo inaczej iloraz byłby dziedziną).

   Uwaga: Skorzystaliśmy tutaj z ogólnego faktu, że jeśli $n \in \mathbb{Z}$, to $\mathbb{Z}[x]/(n, x) \simeq \mathbb{Z}_n$. Zakładam, że jest to znane, ale jeśli nie, można to pokazać z twierdzenia o izomorfizmie: bierzemy homomorfizm $\phi : \mathbb{Z}[x] \to \mathbb{Z}_n$ zadany przez $\phi(f) = f(0) \pmod n$. Jest to homomorfizm, gdyż waluacja w pierścieniach przemiennych zawsze jest homomorfizmem. Jest ponadto epimorfizmem (tzn. "na"), gdyż biorąc wielomian stały równy $r \in \{0, 1, \ldots, n-1\}$ możemy dostać każdą wartość w $\mathbb{Z}_n$. Jądro tego homomorfizmu to $\ker(\phi) = (n, x)$, bo:

   "$\subseteq$": Jeśli $\phi(f) = 0$, to $f(0) = 0 \pmod n$, więc pisząc $f(x) = a_0 + a_1 x + \ldots + a_k x^k$ mamy $n|a_0$, czyli pisząc $a_0 = nb$, mamy $f = n \cdot b + x \cdot (a_1 + \ldots + a_k x^{k-1}) \in (n, x)$.

   "$\supseteq$": Jeśli $f \in (n, x)$, to mamy $f = n \cdot (a_0 + \ldots + a_k x^k) + x \cdot (b_0 + \ldots + b_l x^l)$ mamy $\phi(f) = 0 \cdot (\ldots) + 0 \cdot (\ldots) = 0$ (pierwsze zero, bo robimy modulo n, drugie zero, bo bierzemy $x = 0$). $\square$

2. Treść o tym nie wspomina (zapewne licząc, że studenci się domyślą, bo np. mogło być podobne zadanie na wykładzie), ale działania w tym pierścieniu wykonujemy po współrzędnych, tzn. $(f + g)(x) = f(x) + g(x)$ oraz $(fg)(x) = f(x)g(x)$. Ponadto, elementem neutralnym dodawania jest funkcja stała równa 0, zaś mnożenia: funkcja stała równa 1.

   (a) Należy sprawdzić dwie rzeczy: $\forall_{f,g \in I} f - g \in I$ oraz $\forall_{f \in I,\, g \in R} fg \in I$. Obydwa sprawdzamy biorąc waluacje w 0 oraz w 1: $(f-g)(0) = f(0) - g(0) = 0 - 0 = 0$, $(f-g)(1) = f(1) - g(1) = 0 - 0 = 0$, $(fg)(0) = f(0)g(0) = 0 \cdot g(0) = 0$ oraz $(fg)(1) = f(1)g(1) = 0 \cdot g(1) = 0$.

   (b) Dla danego $x_0 \in [0, 1]$, oznaczmy $I_{x_0} = \{f \in R : f(x_0) = 0\}$. Jest to ideał, co robimy identycznie jak w punkcie (a), biorąc waluację w x_0. Rozważmy ideały dla $x_0 = 0$ oraz $x_0 = 1$. Zauważmy, że $I_0 + I_1 = R$, bo $f + g = 1$ dla $f(x) = x \in I_0$ oraz $g(x) = 1 - x \in I_1$. Ponadto, $I = I_0 \cap I_1$ (jasne). Stąd, na mocy Chińskiego Twierdzenia o Resztach (CRT) mamy $R/I \simeq R/I_0 \times R/I_1$. Wystarczy zatem pokazać, że $R/I_{x_0} \simeq \mathbb{R}$ dla dowolnego $x_0 \in [0, 1]$ (więc w szczególności dla $x_0 = 0$ oraz $x_0 = 1$). Robimy to przez twierdzenie o izomorfizmie: bierzemy przekształcenie $\phi : R \to \mathbb{R}$ zadane przez waluację $\phi(f) = f(x_0)$. Jest to homomorfizm, gdyż waluacja w pierścieniach przemiennych zawsze jest homomorfizmem. Jest ponadto epimorfizmem (tzn. "na"), gdyż biorąc wielomian stały równy $r \in \mathbb{R}$ możemy dostać każdą wartość w $\mathbb{R}$. Jądro tego homomorfizmu to $\ker(\phi) = I_{x_0}$, co jest jasne z definicji. Łącznie więc, twierdzenie o izomorfizmie daje nam tezę. $\square$

   Uwaga: Wykazaliśmy pod koniec, że $R/I_{x_0} \simeq \mathbb{R}$, co jest ciałem, czyli I_{x_0} jest ideałem maksymalnym dla każdego $x_0 \in [0, 1]$. Istnieje ładny argument dotykający topologii, że są to jedyne ideały maksymalne w R. Załóżmy mianowicie, że M jest ideałem maksymalnym w R różnym od każdego z I_{x_0}. Oznacza to, że dla każdego $x_0 \in [0, 1]$ istnieje $f_{x_0} \in M$ taka, że $f_{x_0}(x_0) \neq 0$. Z ciągłości funkcji f_{x_0} (dla $x_0 \notin \{0, 1\}$), istnieje przedział (a_{x_0}, b_{x_0}), na którym f_{x_0} jest niezerowa. W przypadku $x_0 = 0$ lub $x_0 = 1$, jeden z końców jest domknięty - niech będą to $[0, b_0)$ oraz $(a_1, 1]$. Wyrzucamy te dwa przedziały z $[0, 1]$ otrzymując przedział $[b_0, a_1]$. Wówczas rodzina $\{(a_{x_0}, b_{x_0}) : x_0 \in [b_0, a_1]\}$ stanowi pokrycie otwarte zbioru zwartego $[b_0, a_1]$ (zwartość wynika z domkniętości, ograniczoności

i zawartości w $\mathbb{R}$). Możemy zatem wybrać skończone podpokrycie $\{(a_{x_i}, b_{x_i}) : x_i \in [b_0, a_1],\ 1 \leqslant i \leqslant n\}$. Niech f_{x_i} to odpowiadające im funkcje. Wówczas, funkcja

$$g = f_0^2 + f_1^2 + \sum_{i=1}^{n} f_{x_i}^2 \in M$$

jest funkcją niezerującą się w żadnym punkcie $[0, 1]$ (wszędzie jest dodatnia). W związku z tym, funkcja $\frac{1}{g}$ jest dobrze określoną funkcją ciągłą (nigdzie nie dzielimy przez 0), czyli $\frac{1}{g} \in R$. Skoro M jest ideałem, to $1 = g \cdot \frac{1}{g} \in M$, czyli $M = R$, co przeczy maksymalności M (z definicji, ideał maksymalny jest różny od całego pierścienia).

3. Oznaczmy pierścienie dane w treści kolejno jako R_1, R_2, R_3 oraz R_4. W pierścieniu R_3 ideał I, przez który dzielimy, upraszcza się do $(x^2, x^4 + 3) = (x^2, 3)$, bo $3 = x^4 + 3 - x^2 \cdot x^2 \in (x^2, x^4 + 3)$ oraz $x^4 + 3 = x^2 \cdot x^2 + 3 \in (x^2, 3)$. Możemy zatem uprościć postać elementów w R_3: dla dowolnego $f + I \in R_3$, gdzie $f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = a_0 + a_1 x + x^2(\ldots)$ możemy przenieść część kwadratową do I otrzymując $f + I = a_0 + a_1 x + I$. Dalej, biorąc reszty z dzielenia przez 3: $a \equiv a_0$ oraz $b \equiv a_1$, możemy napisać $f + I = a + bx + I$ (bo $3 \in I$). Wybór takich reprezentantów jest oczywiście jednoznaczny - R_3 ma zatem 9 elementów (po 3 możliwości na wybór a i b). Działania na takich elementach są też wykonywane modulo 3.

   Zauważmy teraz, że jako grupy addytywne, każdy element w R_2, R_3 i R_4 ma rząd nie większy niż 3 (jako iż działania są wykonywane modulo 3, to dodanie trzykrotnie tego samego elementu daje 0). Z kolei w R_1 istnieje element rzędu 9 (mianowicie 1) - stąd więc R_1 nie jest izomorficzny z żadnym z pozostałych.

   Zauważmy teraz, że w R_4 istnieje niezerowy element, którego kwadrat jest zerowy: jest to taka macierz, w której $a = 0$ oraz $b = 1$ (przyjmując oznaczenia z treści zadania). W pierścieniu R_2 oczywiście taki nie istnieje, więc $R_4 \not\simeq R_2$. Podobnie, w R_3 istnieje niezerowy element, którego kwadrat to 0 - mianowicie $x + (3, x^2)$. Stąd więc $R_3 \not\simeq R_2$.

   Pokażemy teraz, że $R_3 \simeq R_4$. Wskażemy bezpośrednio izomorfizm między tymi pierścieniami. Skoro w obydwu pierścieniach mamy niezerowe elementy, które w kwadracie są zerami, to chcielibyśmy przenieść te elementy na siebie. Ponadto, w homomorfizmach 1 przechodzi na 1, więc chcemy przenieść $1 + (3, x^2)$ na macierz identyczności. Rozumowanie to prowadzi nas zatem do konkretnego przykładu poprawnego izomorfizmu:

$$\phi(a + bx + I) = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

   Jest to oczywiście bijekcja, która przenosi 0 na 0 oraz 1 na 1. Łatwo też widać, że $\phi(f+g) = \phi(f)+\phi(g)$. Pozostaje zatem sprawdzić, że $\phi(fg) = \phi(f)\phi(g)$. Rozpisujemy (uwzględniając $x^2 + I = 0 + I$):

$$\begin{aligned} \phi((a + bx + I)(c + dx + I)) &= \phi(ac + (ad + bc)x + I) = \\ &= \begin{pmatrix} ac & ad + bc \\ 0 & ac \end{pmatrix} = \\ &= \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \\ &= \phi(a + bx + I) \cdot \phi(c + dx + I) \end{aligned}$$

   Ostatecznie więc, przekształcenie ϕ jest homomorfizmem bijektywnym, czyli izomorfizmem, co kończy rozwiązanie. Odpowiedź: jedyne izomorficzne są R_3 i R_4, zaś każda inna para jest nieizomorficzna.

   Uwaga: Jako iż plik ten ma za zadanie pokazać wszystkie najważniejsze motywy rozwiązań, wspomnijmy jeszcze o kilku najużyteczniejszych narzędziach w zadaniach tego typu: Jeśli $\mathbb{K}$ jest ciałem (np. $\mathbb{K} = \mathbb{Q}$, $\mathbb{K} = \mathbb{R}$ lub $\mathbb{K} = \mathbb{C}$, ale w szczególności $\mathbb{K} \neq \mathbb{Z}$), to $\mathbb{K}[x]$ jest dziedziną ideałów głównych. W DIGu R, każdy ideał I jest generowany przez pojedynczy element a - wówczas "wszytkie pojęcia się pokrywają", tzn. równoważne są następujące:

- I jest pierwszy
- I jest maksymalny
- a jest pierwszy
- a jest nierozkładalny
- R/I jest dziedziną
- R/I jest ciałem

W zadaniach tego typu, częstym schematem jest rozkładanie wielomianów, przez które dzielimy, a następnie stosowanie Chińskiego Twierdzenia o Resztach (CRT); zaś, gdy wielomian jest nierozkładalny, dostajemy ciało, co zazwyczaj implikuje jednoznacznie z czym mamy do czynienia. Przydatnymi narzędziami w tego typu rozumowaniach są:

- kryterium Eisenstein'a nad $\mathbb{Q}$
- fakt, że nad $\mathbb{R}$ nierozkładalne są jedynie wielomiany stopnia pierwszego oraz te stopnia drugiego, które nie mają pierwiastków rzeczywistych
- fakt, że nad $\mathbb{C}$ nierozkładalne są jedynie wielomiany stopnia 1 (zasadnicze twierdzenie algebry)
- fakt, że w pierścieniu przemiennym R dla dowolnego $a \in R$, mamy $R[x]/(x-a) \simeq R$
- twierdzenie o izomorfizmie (którego szczególnym przypadkiem jest poprzedni punkt)
- twierdzenie Bezout
- fakt, że jeśli R jest DJRem, to $R[x]$ też jest DJRem
- fakt, że jeśli $\phi : R_1 \to R_2$ jest homomorfizmem, to $\ker(\phi)$ jest ideałem w R_1
- znajdowanie elementów nilpotentnych (czyli takich $a \in R$, że $a^n = 0$ dla pewnego n)

Dla przykładu rozwiążmy następujące zadanie (ujmujące większość z tych motywów na raz):

Zadanie: Rozstrzygnąć, które z następujących pierścieni są izomorficzne:

$$\mathbb{R} \times \mathbb{R}, \quad \mathbb{C}, \quad \mathbb{R}[x]/(x^2-1), \quad \mathbb{R}[x]/(x^2), \quad \mathbb{R}[x]/(x^2+1)$$

Rozwiązanie: Jedynką w $\mathbb{R} \times \mathbb{R}$ jest element $(1,1)$. Nie ma w tym pierścieniu elementu, który w kwadracie daje minus jedynkę, tzn. $(-1,-1)$ (gdyż każdy element (a,b) po podniesieniu do kwadratu daje (a^2,b^2), w którym elementy na obydwu współrzędnych są nieujemne). Stąd $\mathbb{R} \times \mathbb{R} \not\simeq \mathbb{C}$.

Wielomian x^2+1 jest nierozkładalny nad $\mathbb{R}$, więc (x^2+1) jest maksymalny, czyli $\mathbb{R}[x]/(x^2+1)$ jest ciałem. Przez postać tego wielomianu, nietrudno się domyślić, że powinno wyjść $\mathbb{C}$. Wskazujemy zatem homomorfizm $\phi : \mathbb{R}[x] \to \mathbb{C}$ zadany przez waluację $\phi(f) = f(i)$. Waluacja jest homomorfizmem; ponadto jest to epimorfizm, gdyż każda liczba zespolona $a+bi$ jest obrazem wielomianu $a+bx$. Jądro $\ker(\phi)$ (będące ideałem właściwym w $\mathbb{R}[x]$) zawiera w sobie ideał generowany przez x^2+1 (gdyż x^2+1 zeruje się na i). Mamy zatem $(x^2+1) \subseteq \ker(\phi) \subseteq \mathbb{R}[x]$, ale (x^2+1) jest ideałem maksymalnym - stąd $(x^2+1) = \ker(\phi)$. Z twierdzenia o izomorfizmie dostajemy zatem $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$.

Dalej, zobaczmy, że $x^2-1 = (x-1)(x+1)$ jest rozkładem na czynniki nierozkładalne nad $\mathbb{R}$. Ponadto, oznaczając $I = (x+1)$, $J = (x-1)$, mamy $I + J = \mathbb{R}$, bo $1 = \frac{x+1}{2} - \frac{x-1}{2} \in I + J$. Dodatkowo $I \cap J = (x^2-1)$, bo:

- jeśli $f \in (x^2-1)$, to $f(x) = (x^2-1)g(x) = (x-1)(x+1)g(x) \in I \cap J$;
- jeśli $f \in I \cap J$, to $f(x) = (x-1)g(x)$ oraz $f(x) = (x+1)h(x)$, czyli $f(1) = 0 = f(-1)$. Podstawiając więc $x = -1$ w $f(x) = (x-1)g(x)$, dostajemy $0 = f(-1) = (-2)g(-1)$, czyli $g(-1) = 0$. Z twierdzenia Bezout oznacza to więc, że $g(x) = (x+1)g_1(x)$, czyli $f(x) = (x-1)g(x) = (x-1)(x+1)g_1(x) = (x^2-1)g_1(x)$ - stąd $f \in (x^2-1)$.

Na podstawie CRT widzimy zatem, że $\mathbb{R}[x]/(x^2-1) \simeq \mathbb{R}[x]/(x-1) \times \mathbb{R}/(x+1) \simeq \mathbb{R} \times \mathbb{R}$.

Na koniec, zauważmy jeszcze, że w pierścieniu $\mathbb{R}[x]/(x^2)$ istnieje element nilpotentny, stopnia 2, mianowicie $x+(x^2)$. Takie elementy nie istnieją jednak ani w $\mathbb{R}\times\mathbb{R}$, ani w $\mathbb{C}$. Podsumowując więc, formalnie mówiąc, dostaliśmy trzy rozłączne klasy abstrakcji w relacji równoważności izomorfizmu:

$$\mathbb{R} \times \mathbb{R} \simeq \mathbb{R}[x]/(x^2-1), \quad \mathbb{C} \simeq \mathbb{R}[x]/(x^2+1) \quad \text{oraz} \quad \mathbb{R}[x]/(x^2)$$

4. (a) $\mathbb{Z}[i]$ jest dziedziną euklidesową, więc w szczególności dziedziną ideałów głównych. W DIGu natomiast ideał generowany przez element a jest maksymalny wtedy i tylko wtedy, gdy sam element jest nierozkładalny. Należy zatem sprawdzić rozkładalność elementów 5, 7 oraz $5+i$. Przypomnijmy, że w dziedzinie euklidesowej, element jest odwracalny wtedy i tylko wtedy, gdy jego norma wynosi 1. Jeśli więc znajdziemy rozkład elementu na dwa elementy o normie różnej od 1, będzie to istotnie nietrywialny rozkład. Mamy $5 = (2+i)(2-i)$, przy czym $N(2\pm i) = 2^2+1^2 = 5 \neq 1$, czyli I_1 nie jest maksymalny. Dalej, $5+i = (1+i)(3-2i)$, przy czym $N(1+i) = 2$ oraz $N(3-2i) = 13$, więc I_3 nie jest maksymalny. Pokażemy teraz, że 7 jest nierozkładalny (tzn. I_2 jest maksymalny). Załóżmy, że $7 = (a+bi)(c+di)$, przy czym $N(a+bi) \neq 1 \neq N(c+di)$. Przykładając normę do tej równości dostajemy $49 = (a^2+b^2)(c^2+d^2)$. Skoro normy są różne od 1, a przy tym $N(x+iy) = x^2+y^2 \geqslant 0$ dla dowolnych $x, y \in \mathbb{Z}$, to $(a^2+b^2) = (c^2+d^2) = 7$. Zauważmy jednak, że 7 nie da się przedstawić w postaci sumy dwóch kwadratów liczb całkowitych (bo np. patrząc modulo 4, kwadraty liczb całkowitych mogą dawać jedynie reszty 0 lub 1, więc suma dwóch takich nie da reszty 3) - sprzeczność.

   (b) Niech $I = (3-6i, 6+2i)$. Pokażemy, że $I = R$, czyli, że generatorem tego ideału jest 1. Mamy $I \ni (6+2i)i + (3-6i) = -2+6i+3-6i = 1$, więc faktycznie $1 \in I$.

Uwaga: Zauważmy, że dokładnie tym samym argumentem, co w punkcie (a), można pokazać, że liczba pierwsza p (pierwsza w sensie $\mathbb{Z}$) jest nierozkładalna w $\mathbb{Z}[i]$, gdy $p \equiv 3 \pmod 4$. Okazuje się, że wynikanie jest również w drugą stronę: jeśli $p \in \mathbb{Z}$ jest liczbą pierwszą, to jest nierozkładalna w $\mathbb{Z}[i]$ wtedy i tylko wtedy, gdy $p \equiv 3 \pmod 4$. Co bezpośrednio z tym związane: Liczba pierwsza $p \in \mathbb{Z}$ jest przedstawialna w postaci sumy dwóch kwadratów liczb całkowitych wtedy i tylko wtedy, gdy $p \not\equiv 3 \pmod 4$ - fakt ten nazywa się czasami Średnim lub Świątecznym Twierdzeniem Fermata (lub Fermata-Eulera) i jest klasycznym rezultatem pokazującym, że algebra abstrakcyjna potrafi dać bardzo rzeczywiste rezultaty.

5. (a) Niech s oznacza liczbę 11-podgrup Sylowa w G. Z twierdzenia Sylowa wiemy, że $s \equiv 1 \pmod{11}$ oraz $s \mid |G|$. Skoro $165 = 3 \cdot 5 \cdot 11$, to jedynymi dzielnikami 165 są 1, 3, 5, 11, 15, 33, 55, 165, więc możliwe jest jedynie $s = 1$ (żadna inna liczba nie daje reszty 1 z dzielenia przez 11). Jeśli H jest tą podgrupą, to dla dowolnego $g \in G$ podgrupa $g^{-1}Hg$ również ma 11 elementów, więc jest 11-podgrupą Sylowa - z jedyności więc mamy $g^{-1}Hg = H$, co pokazuje normalność H. Wówczas $|G/H| = [G:H] = \frac{|G|}{|H|} = \frac{165}{11} = 15$. $\square$

   (b) Z powyższego mamy $H \trianglelefteq G$ takie, że grupa G/H ma rząd 15. Przeprowadzając identyczny argument, jak wyżej, pokazujemy, że grupa G/H posiada jedyną (więc normalną) 5-podgrupę Sylowa F/H (w grupie ilorazowej G/H każda podgrupa normalna jest postaci F/H dla pewnej podgrupy normalnej $F \trianglelefteq G$). Z trzeciego twierdzenia o izomorfizmie mamy zatem $(G/H)/(F/H) \simeq G/F$, a więc dostaliśmy normalną podgrupę F w G, dla której $|G/F| = \frac{|G/H|}{|F/H|} = \frac{15}{5} = 3$, czyli w szczególności jest to grupa cykliczna (gdy rząd grupy jest pierwszy, to jest ona cykliczna). $\square$

Uwaga: W obydwu podpunktach użyliśmy podobnego argumentu. W (b) pokazał on jedynie, że w grupie rzędu 15 istnieje normalna 5-podgrupa Sylowa. Można to jednak pociągnąć znacznie dalej i pokazać, że grupa rzędu 15 musi w ogóle być cykliczna. Da się to nawet uogólnić do następującego faktu (z którego wynika większość zadań na egzaminach z grup Sylowa, więc warto pamiętać ten schemat dowodowy):

Twierdzenie: Jeśli G jest grupą skończoną o mocy pq, gdzie p i q są liczbami pierwszymi, spełniającymi $p < q$ i $p \nmid q-1$, to G jest cykliczna.

Dowód: Niech s_p i s_q oznaczają odpowiednio liczby p- i q-podgrup Sylowa w G. Wartości s_p i s_q dzielą $|G|$, więc należą one do zbioru $\{1, p, q, pq\}$. Ponownie $s_p \equiv 1 \pmod p$ oraz $s_q \equiv 1 \pmod q$, co na mocy warunków $p < q$, $p \nmid q-1$ daje jedyną możliwość $s_p = 1 = s_q$. Pokazuje to zatem, że jeśli P jest p-podgrupą Sylowa w G, zaś Q jest q-podgrupą Sylowa w G, to są one jedyne. Naszym celem jest pokazanie, że w G istnieje element rzędu pq (bo wtedy G jest generowana przez ten element). Przypuśćmy zatem przeciwnie, że nie ma takiego elementu. Rząd dowolnego elementu w G jest

dzielnikiem $|G|$, więc możliwe (pozostałe) rzędy to 1, p i q. Wówczas

$$G = \{e\} \cup A \cup B, \text{ gdzie } A = \{a \in G : o(a) = p\} \text{ oraz } B = \{b \in G : o(b) = q\}$$

jest sumą parami rozłącznych zbiorów. Zauważmy, że jeżeli $a \in A$, to $|(a)| = p$, czyli (a) jest p-podgrupą Sylowa w G, co z jedyności oznacza, że $(a) = P$. W szczególności $a \in P \setminus \{e\}$. W związku z tym, w G istnieje jedynie $p-1$ elementów rzędu p, czyli $|A| = p-1$. Analogicznie $|B| = q-1$. Łącznie zatem dostaliśmy $pq = |G| = |\{e\}| + |A| + |B| = 1 + (p-1) + (q-1) = p + q - 1$, czyli $0 = pq - p - q + 1 = (1-p)(1-q)$. Daje to jednak $p = 1$ lub $q = 1$, ale 1 nie jest liczbą pierwszą. Sprzeczność ta dowodzi zatem tezy. $\square$

Na zakończenie tego (przydługiego) pliku wspomnę jeszcze o jednym ważnym aspekcie, który nie był poruszony w żadnym z zadań: Badanie kiedy pierścień postaci $\mathbb{Z}[\sqrt{d}]$ jest dziedziną z jednoznacznością rozkładu / dziedziną ideałów głównych / dziedziną euklidesową. Przede wszystkim, w dowolnym pierścieniu przemiennym, bycie dziedziną euklidesową implikuje bycie DIGiem, zaś bycie DIGiem implikuje bycie DJRem. Często zatem w zadaniach typu "Pokazać, że $\mathbb{Z}[\sqrt{d}]$ nie jest DJRem dla $d = \ldots$", rozwiązania polegają na tym, że wskazujemy palcem taki element p, że

- p ma dwa różne rozkłady (różnej długości lub składające się z odpowiednio niestowarzyszonych elementów) - wtedy pierścień nie może być DJRem, a więc też w szczególności DIGiem
- p jest nierozkładalny, a przy tym nie pierwszy - w DJRze (więc tym bardziej w DIGu) bycie elementem nierozkładalnym jest równoważne byciu elementem pierwszym, więc prowadziłoby to do sprzeczności

Ogólne określenie kiedy $\mathbb{Z}[\sqrt{d}]$ (dla $d \notin \{0, 1\}$) nie jest DJRem jest trudne - na czas pisania tego skryptu, problem ten pozostaje otwarty. Całkiem łatwo można jednak udowodnić, że:

- Dla $d \in \{-2, -1, 2, 3\}$, $\mathbb{Z}[\sqrt{d}]$ jest dziedziną euklidesową (względem normy $N(a + b\sqrt{d}) = |a^2 - db^2|$), więc w szczególności DJRem
- Jeśli $d < -2$ i $4 \nmid d$, to $\mathbb{Z}[\sqrt{d}]$ nie jest DJRem
- Jeśli d jest bezkwadratowa (tzn. jest niepodzielna przez kwadrat żadnej liczby pierwszej) oraz $d \equiv 1 \pmod 4$, to $\mathbb{Z}[\sqrt{d}]$ nie jest DJRem

Naszkicuję dowody i zachęcam do samodzielnego uzupełnienia braków: Pierwszy z tych rezultatów sprawdzamy wprost z definicji dziedziny euklidesowej. Pozostałe dwa rezultaty bazują na tym samym pomyśle: dowodzimy, że element 2 nie jest pierwszy, bo albo dzieli $d = (\sqrt{d})^2$, nie dzieląc $\sqrt{d}$ (bo $4 \nmid d$), albo dzieli $d - 1 = (\sqrt{d} - 1)(\sqrt{d} + 1)$, nie dzieląc żadnego z tych czynników (przez obecność członu ± 1). Z kolei element ten jest nierozkładalny, bo inaczej, pisząc $2 = (k + l\sqrt{d})(m + n\sqrt{d})$ dla nieodwracalnych elementów i przykładając normę, mielibyśmy $4 = |k^2 - dl^2| \cdot |m^2 - dn^2|$. Dla $d \leqslant -3$ mamy jednak $x^2 - dy^2 \geqslant 3$, więc taki rozkład nie byłby możliwy. Z kolei dla bezkwadratowej $d \equiv 1 \pmod 4$ kongruencja $x^2 - dy^2 \equiv 2 \pmod 4$ nie ma rozwiązań. Do wykończenia tego argumentu, trzeba teraz posłużyć się następującym (ogólniejszym) faktem dla $p = 2$ (którego dowód zostawiam jako ćwiczenie korzystające z podobnych motywów):

Twierdzenie: Dana jest taka liczba bezkwadratowa $d \in \mathbb{Z} \setminus \{0, 1\}$, że $\mathbb{Z}[\sqrt{d}]$ jest DJRem. Wówczas dla dowolnej liczby pierwszej p niedzielącej d równoważne są:

1. d jest resztą kwadratową modulo p
2. $p = |x^2 - dy^2|$ dla pewnych całkowitych x, y

Zwróćmy jeszcze uwagę na jedną kwestię: bardzo użytecznym narzędziem w rozumowaniach tego typu jest norma (multiplikatywna!) $N(a + b\sqrt{d}) = |a^2 - db^2|$. Warto sobie jednak uświadomić, że samo istnienie normy multiplikatywnej nie implikuje, że jesteśmy w dziedzinie euklidesowej (dlatego rozważania te w ogóle mają sens). Do tego potrzeba by jeszcze była możliwość wykonywania dzielenia z resztą: dla dowolnych $a \in R$, $0 \neq b \in R$ istnieją takie $k \in R$, $r \in R$, że $a = bk + r$, gdzie $N(r) < N(b)$. Na ogół zatem, norma, którą się posługujemy, nie spełnia tego warunku. Co warto też podkreślić to to, że fakt "$N(a) = 1 \iff a$ jest odwracalny" zachodzi jedynie w dziedzinie euklidesowej - tym bardziej więc, na ogół (w szczególności w nie-DIGu czy nie-DJRze), nie można z tego korzystać.