Dowody wstępne

Lemat 1. *Dla każdych liczb całkowitych nieujemmych* n, m *nie równych jednocześnie 0, o największym wspólnym dzielniku* d *istnieją liczby całkowite* k, l *takie, że* $nk + lm = d$

Dowód. Dokonajmy indukcji po sumie tych liczb. Dla sumy wynoszącej 1 mamy, że z dokładnością do permutacji $n = 1$, $m = 0$. Wtedy biorąc $k = 1$, $l = 0$ uzyskujemy prawdziwość tezy indukcyjnej.

Załóżmy więc, że teza jest prawdziwa dla wszystkich par (n, m) o sumie mniejszej niż pewne S. Rozpatrzmy dowolną parę (n, m) o sumie S. Bez straty ogólności załóżmy, że $n \geqslant m$ (co daje $n > 0$). Łatwo widać, że $d \mid n \wedge d \mid m \iff d \mid n - m \wedge d \mid m$, czyli największy wspólny dzielnik liczb (n, m) to największy wspólny dzielnik liczb $(n - m, m)$.

Zapiszmy więc na mocy założenia indukcyjnego, że istnieją takie $k', l' \in \mathbb{Z}$, że $k'(n - m) + l'm = d$. Wtedy jednak $k'n + (l' - k')m = d$, więc przyjmując $k = k'$, $l = l' - k'$ uzyskujemy, że teza jest prawdziwa także dla pary (n, m). □

Lemat 2. *Jeśli* p *jest liczbą pierwszą, zaś* $a, b \in \mathbb{Z}$, *to z tego, że* $p \mid ab$ *wynika, że* $p \mid a$ *lub* $p \mid b$.

Dowód. Załóżmy, że $p \mid ab$, zaś $p \nmid a$. Wtedy największy wspólny dzielnik liczb p, a musi wynosić jeden. Na mocy lematu 1 istnieją liczby $k, l \in \mathbb{Z}$, że $pk + la = 1$. Stąd $pkb + lab = b$. Jednakże $p \mid pkb$, $p \mid lab$, skąd wtedy $p \mid b$. □

Twierdzenie 1. *Każdą liczbę całkowitą dodatnią można jednoznacznie z dokładnością do permutacji zapisać jako iloczyn liczb pierwszych.*

Dowód. Najpierw udowodnimy indukcyjnie, że każdą liczbę całk. dod. da się zapisać na przynajmniej jeden sposób. Liczbę jeden można przestawić jako iloczyn pusty.

Załóżmy więc, że każdą liczbę całk. dod. mniejszą niż pewne $S > 1$ można zapisać jako iloczyn liczb pierwszych. Rozpatrzmy teraz liczbę S. Jest ona albo pierwsza, albo złożona. W każdym przypadku posiada jakiś dzielnik pierwszy p. Wtedy zauważmy, że z założenia indukcyjnego liczbę $\frac{S}{p}$ można zapisać jako iloczyn liczb pierwszych. Jednak dopisując do tego rozkładu liczbę p uzyskujemy rozkład liczby S.

Udowodnimy teraz, że taki rozkład jest jednoznaczny. Załóżmy bowiem nie wprost, że istnieje choć jedna liczba naturalna o niejednoznacznym rozkładzie na czynniki pierwsze. Na mocy zasady minimum istnieje najmniejsza taka liczba, oznaczmy ją n.

Gdyby $n = 1$, to mielibyśmy, że iloczyn niezerowej liczby liczb pierwszych jest równy jeden, co jest sprzecznością.

Załóżmy więc, że $1 < n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$, gdzie p_i, q_j są liczbami pierwszymi, zaś a_i, b_j liczbami całkowitymi dodatnimi dla $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant l$. Oczywiście $k, l > 0$.

Zauważmy jednak, że żadna z liczb q_j nie może być równa liczbie p_1, gdyż w przeciwnym wypadku także liczba $\frac{n}{p_1} < n$ posiadałaby niejednoznaczny rozkład na czynniki pierwsze powstały ze skreślenia liczby p_1 z dwóch rozkładów liczby n.

Niech r oznacza najmniejszą liczbę całkowitą dodatnią taką, że $p_1 \mid q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$. Taka liczba istnieje, gdyż w szczególności $r = l$ spełnia zapisany przed chwilą warunek podzielności. Oczywiście $r > 1$, gdyż $p_1 \mid q_1^{b_1}$ oznaczałoby, że $q_1 = p_1$.

Jednak zauważmy, że na mocy lematu 2 mamy, że $p_1 \mid \left(q_1^{b_1} \cdots q_{r-1}^{b_{r-1}}\right) q_r^{b_r}$ implikuje, że $p_1 \mid q_r^{b_r}$ lub $p_1 \mid \left(q_1^{b_1} \cdots q_{r-1}^{b_{r-1}}\right)$. Pierwszy przypadek jest sprzecznością, gdyż wtedy $p_1 = q_r$, zaś drugi jest sprzecznością z minimalnością r.

Stąd rozkład liczby n musi być jednoznaczny, co dowodzi, że rozkład każdej liczby całk. dod. jest jednoznaczny. □

Lemat 3. *Gdy* $n, m \in \mathbb{Z}_+$ *oraz* $n \perp m$, *to istnieje takie* k, *że* $nk \equiv 1 \pmod{m}$

Dowód. Na mocy lematu 1 istnieją liczby k, l, że $kn + lm = 1$. Biorąc to równanie $\mod m$ uzyskujemy, że $kn \equiv 1 \pmod{n}$. □

Zadanie 1

Dla pewnego uproszczenia zapisu w rozwiązaniu zmienię oznaczenia. Zamiast pisać $z_1, \dots, z_n$ będę pisał $z_0, \dots, z_{n-1}$, a zamiast z_0 – Z.

Szczególny przypadek

Udowodnijmy najpierw szczególny przypadek: gdy z_k dla $k = 0, 2, \dots, n-1$ to pierwiastki zespolone stopnia n-tego z jedynki (wtedy oczywiście $Z = 0$), zaś $W(z) = z^m$ dla pewnego $0 < m < n$. Niech ε będzie pierwiastkiem pierwotnym n-tego stopnia z jedynki (tzn. $z_k = \varepsilon^k$) i niech d będzie największym wspólnym dzielnikiem liczb n, m oraz niech $n = dn'$, $m = dm'$. Wtedy oczywiście $n' > 1$, gdyż $n > m \implies \frac{n}{d} > \frac{m}{d} \geqslant 1$.

Mamy wtedy, że $\left(\varepsilon^d\right)^{n/d} = 1$ oraz $\left(\varepsilon^d\right)^w = \varepsilon^{dw} \neq 1$ (dla $0 < w < n/d$), więc ε^d jest pierwiastkiem pierwotnym stopnia $\frac{n}{d}$ z jedynki.

Zapiszmy wtedy $S := \sum\limits_{k=0}^{n-1} z_k^m = \sum\limits_{k=0}^{n-1} \varepsilon^{km} = \sum\limits_{k=0}^{n-1} \left(\varepsilon^d\right)^{km'}$. Łatwo widać, że każda reszta r z dzielenia km' przez $\frac{n}{d}$ będzie w wykładnikach sumy po prawej stronie osiągana dokładnie d razy: dla $k = i\frac{n}{d} + r$ dla $i = 0, 1, \dots, d-1$. Ponadto tylko reszta $km' \pmod{\frac{n}{d}}$ jest istotna dla wartości wyrażenia $\left(\varepsilon^d\right)^{km'}$.

Oznaczmy $\delta = \varepsilon^d$. Wtedy na mocy przemienności dodawania $S = d \sum\limits_{k=0}^{n'-1} \delta^{km'}$, gdzie $n' \perp m'$. Zauważmy teraz, że $\lambda x.m'x \pmod{n'}$ jest permutacją zbioru $\{0, 1, 2, \dots, n'-1\}$ (injektywność: gdyby $m'x \equiv m'y \pmod{n'}$, to $m'(x-y) \equiv 0 \pmod{n'}$, co przemnożone przed odwrotność m' modulo n' (która istnieje na mocy lematu 3) daje $(x-y) \equiv 0 \pmod{n'}$; surjektywność: gdy w jest odwrotnością m' modulo n', to $m'(wy) \equiv (m'w)y \equiv y \pmod{n'}$, a więc każda wartość jest osiągana).

Stąd mamy, że $S = d \sum\limits_{k=0}^{n'-1} \delta^{km'} = d \sum\limits_{k=0}^{n'-1} \delta^k$. Jednak ta ostatnia suma to suma pierwiastków z jedności stopnia n'-tego, czyli 0. Skąd $S = 0$.

To kończy dowód szczególnego przypadku.

Przypadek ogólniejszy

Dalej rozpatrujmy tylko przypadek: z_k dla $k = 0, 2, \dots, n-1$ to pierwiastki zespolone stopnia n-tego z jedynki.

Zauważmy, że gdy $W(z) = a_{n-1}z^{n-1} + \dots a_0 z^0$, to $\sum_k W(z_k) = a_{n-1}\sum_k z^{n-1} + a_{n-2}\sum_k z^{n-2} + \dots + a_0 \sum_k z^0$, co zaś na mocy przypadku szczególnego daje $\sum_k W(z_k) = a_{n-1} \cdot 0 + a_{n-2} \cdot 0 + \dots + a_1 \cdot 0 + na_0 = nW(0)$. Stąd wiemy, że teza zachodzi już dla dowolnego wielomianu, ale nadal dla ustalonych z_k.

Przypadek ogólny

Dla dowolnych już $z_0, \dots, z_{n-1}$ spełniających warunki zadania i dowolnego wielomianu W stopnia mniejszego od n.

Łatwo widać, że przekształcenie $\lambda z.\frac{z-Z}{z_0-Z}$ przekształca wielokąt $z_0, \dots, z_{n-1}$ na n-kąt powstały z pierwiastków n-tego stopnia z jedności. (Jest to złożenie przesunięcia przesuwającego Z do środka układu współrzędnych zespolonych, oraz obrotu i jednokładności takich aby punkt z_0 trafił na punkt 1. Przekształceniem odwrotnym jest oczywiście $\lambda x.Z + (z - Z)(z_0 - Z)$.

Określmy wielomian $P(z) = W(Z + (z - Z)(z_0 - Z))$, wtedy $W(z) = P(\frac{z-Z}{z_0-Z})$. Jednak na mocy powyższych uwag, $\frac{z_k-Z}{z_0-Z}$ są to pierwiastki n-tego stopnia z jedynki, a więc na mocy przypadku ogólniejszego $\sum_k W(z_k) = \sum_k P(\frac{z_k-Z}{z_0-Z}) = nP(0) = nW(Z)$.

Zadanie 3

Zdefiniujmy następującą funkcję (zwaną f. Möbiusa):

$$\mu(n) = \begin{cases} 1 & \text{gdy } n = 1 \\ 0 & \text{gdy } \exists_{p \in \mathbb{P}}\, p^2 \mid n \\ (-1)^r & \text{gdy } n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \end{cases}$$

gdzie wartość $\mu(n)$ jest wyznaczana przez najwyżej umieszczony przypadek, którego warunek spełnia n, zaś $p_1^{a_1} \cdots p_r^{a_r}$ jest rozkładem n na czynniki pierwsze zgodnie z twierdzeniem 1.

Lemat 4. *Dla każdego n całkowitego dodatniego, suma $\mu(d)$ po wszystkich d będących dodatnimi dzielnikami n wynosi odpowiednio:*

- *1 gdy $n = 1$*
- *0 w przeciwnym przypadku*

Dowód. Dla $n = 1$ teza jest trywialna.

Załóżmy więc, że $n > 1$ i zapiszmy na mocy twierdzenia 1: $n = p_1^{a_1} \cdots p_k^{a_k}$.

Wtedy mamy, grupując wyrazy sumy po liczbie czynników pierwszych d:

$$\begin{aligned}\sum_{d|n} \mu(d) = {} & \mu(1) + \mu(p_1) + \mu(p_2) + \ldots + \mu(p_k) + \\ & + \mu(p_1 p_1) + \mu(p_1 p_2) + \ldots + \mu(p_{k-1} p_k) + \mu(p_k p_k) + \\ & + \mu(p_1 p_1 p_1) + \mu(p_1 p_1 p_2) + \ldots + \mu(p_k p_k p_k) + \\ & + \ldots + \\ & + \mu(p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k})\end{aligned}$$

Korzystając z tego, że $\mu(x) = 0$ dla liczby x podzielnej przez kwadrat liczby pierwszej widzimy, że:

$$\begin{aligned}\sum_{d|n} \mu(d) = {} & \mu(1) + \mu(p_1) + \mu(p_2) + \ldots + \mu(p_k) + \\ & + \mu(p_1 p_2) + \ldots + \mu(p_{k-1} p_k) + \\ & + \ldots + \\ & + \mu(p_1 p_2 \ldots p_k)\end{aligned}$$

Tzn. suma przebiega *de facto* po podzbiorach zbioru $\{p_1, p_2, \ldots, p_k\}$, gdyż jeśli jakaś liczba pierwsza wystąpi dwukrotnie, to μ przybiera wartość 0.

Możliwych podzbiorów f-elementowych jest $\binom{k}{f}$, zaś wartość funkcji μ dla iloczynu każdego takiego podzbioru to $(-1)^f$. Tak więc mamy:

$$\sum_{d|n} \mu(d) = \binom{k}{0}(-1)^0 + \binom{k}{1}(-1)^1 + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k}(-1)^k = (1 + (-1))^k = 0$$

Na mocy wzoru dwumianowego Newtona i faktu, że $k > 0$. □

Oznaczmy teraz R_n – zbiór wszystkich pierwiastków zespolonych n-tego stopnia z jedynki, P_n – zbiór wszystkich pierwiastków pierwotnych n-tego stopnia z jedynki.

Dla każdego z – pierwiastka z jedynki określmy jego rząd ($o(z)$) jako najmniejsze całkowite dodatnie k takie, że $z^k = 1$.

Lemat 5. *Jeśli z jest pierwiastkiem n-tego stopnia z jedynki, to $o(z) \mid n$. Także odwrotnie, jeśli $o(z)$ jest określone i $o(z) \mid n$, to $z^n = 1$.*

Dowód. Załóżmy przeciwnie, że $o(z) \nmid n$. Wtedy oznaczmy przez r resztę z dzielenia n przez $o(z)$ (tzn. zapiszmy $n = ko(z) + r$). Oczywiście $1 \leqslant r < o(z)$. Mamy jednak $1 = z^n = z^{ko(z)+r} = z^{ko(z)} z^r = \left(z^{o(z)}\right)^k z^r = 1^k z^r = z^r$, co jest sprzeczne z definicją rzędu.

Dla dowodu drugiej części zapiszmy $n = ko(z)$, wtedy $z^n = z^{ko(z)} = \left(z^{o(z)}\right)^k = 1^k = 1$. □

Zauważmy teraz, że z jest pierwiastkiem pierwotnym stopnia k-tego z jedynki wtedy i tylko wtedy, gdy $o(z) = k$, co wynika wprost z definicji.

Mamy więc na mocy lematu 5, że $R_n = \bigcup_{d|n} P_d$, a ponieważ zbiory P_d są rozłączne dla różnych d mamy, że $\sum R_n = \sum_{d|n} \sum P_d$.

Udowodnimy teraz indukcyjnie, że $\sum P_n = \mu(n)$. Dla $n = 1$ teza jest trywialnie prawdziwa. Załóżmy więc, że jest prawdziwa dla n mniejszych od ustalonego $N > 0$ i rozpatrzmy $n = N$.

Suma pierwiastków zespolonych N-tego stopnia z jedynki wynosi 0 (ze wzorów Viete'y dla wielomianu $z^N - 1 = 0$), a więc mamy, że $0 = \sum R_N = \sum_{d|N} \sum P_d$, co jednak na mocy założenia indukcyjnego daje $0 = \sum P_N + \sum_{d|N \wedge d<N} \sum P_d = \sum P_N + \sum_{d|N \wedge d<N} \mu(d)$, jednak na mocy lematu 4 $\sum_{d|N \wedge d<N} \mu(d) = -\mu(N)$, a więc $\sum P_N = \mu(N)$, *quod erat demonstrandum.*

Zadanie 4

Dowód. Załóżmy nie wprost, że teza nie jest prawdziwa. Zaprzeczając tezę mamy, że istnieje pewne skończenie wiele liczb $a_1, a_2, \ldots, a_n$ takich, że układ funkcji $\lambda x.e^{a_1 x}, \lambda x.e^{a_2 x}, \ldots, \lambda x.e^{a_n x}$ jest liniowo zależny. Weźmy więc taki układ liczb o najmniejszej mocy, tzn. najmniejsze takie n.

Wtedy uzyskujemy z minimalności n, że układ funkcji $\lambda x.e^{a_1 x}, \lambda x.e^{a_2 x}, \ldots, \lambda x.e^{a_{n-1} x}$ jest liniowo niezależny.

Z tego uzyskujemy, że $\lambda x.e^{a_n x}$ jest kombinacją liniową funkcji $\lambda x.e^{a_1 x}, \lambda x.e^{a_2 x}, \ldots, \lambda x.e^{a_{n-1} x}$, stąd mamy, że $\lambda x.e^{a_n x} = \sum\limits_{k=1}^{n-1} t_k \lambda x.e^{a_k x}$ dla pewnych $t_k \in \mathbb{R}$. Stąd

$$\lambda x.e^{a_n x} = \lambda x. \left(\sum_{k=1}^{n-1} t_k e^{a_k x} \right) \tag{1}$$

Różniczkując mamy, że $\frac{d}{dx} \lambda x.e^{a_n x} = \frac{d}{dx} \lambda x. \left(\sum\limits_{k=1}^{n-1} t_k e^{a_k x} \right)$, skąd

$$\lambda x.a_n e^{a_n x} = \lambda x. \left(\sum_{k=1}^{n-1} (t_k a_k e^{a_k x}) \right). \tag{2}$$

Gdyby $a_n = 0$, to mielibyśmy, że funkcja $\lambda x.0$ jest kombinacją liniową funkcji $\lambda x.e^{a_k x}$, czyli wszystkie współczynniki kombinacji musiałby być zerowe, skąd $\forall_k\ t_k a_k = 0$. Jednak ponieważ liczby a_i są parami różne, to w szczególności $a_k \neq a_n = 0$, skąd $\forall_k\ t_k = 0$, ale wtedy mamy, że równość 1 przybiera postać: $\lambda x.e^0 = \lambda x.0$, co jest sprzecznością.

Stąd $a_n \neq 0$ i możemy zapisać równanie 2 jako:

$$\lambda x.e^{a_n x} = \lambda x. \left(\sum_{k=1}^{n-1} \frac{t_k a_k}{a_n} e^{a_k x} \right). \tag{3}$$

Jednak $\lambda x.e^{a_1 x}, \lambda x.e^{a_2 x}, \ldots, \lambda x.e^{a_{n-1} x}$ jest liniowo niezależny, a więc jest bazą przestrzeni (nad $\mathbb{R}$) $V = \text{lin}\{\lambda x.e^{a_1 x}, \lambda x.e^{a_2 x}, \ldots, \lambda x.e^{a_{n-1} x}\}$, do której należy $\lambda x.e^{a_n x}$, a więc posiada on jednoznaczny rozkład jako kombinację liniową elementów bazy, skąd porównując równości funkcyjne 1 i 3 mamy, że $\forall_k\ t_k = \frac{t_k a_k}{a_n}$, skąd $\forall_k\ (t_k = 0 \vee a_k = a_n)$. Ponieważ dla żadnego k (z $\{1, 2, \ldots, n-1\}$) nie może zajść $a_k = a_n$, to mamy, że $\forall_k\ t_k = 0$, co jak udowodniliśmy wyżej jest sprzecznością. $\square$

Zadanie 5

Załóżmy, że teza jest fałszywa, a więc istnieje skończony liniowo zależny podzbiór zbioru pierwiastków liczb pierwszych.

Rozszerzeniem ciała K o elementy $x_1, x_2, \ldots, x_n$ nazwiemy najmniejsze ciało $K[x_1, \ldots, x_n]$ zawierające jako podzbiór ciało K oraz jako elementy $x_1, \ldots, x_n$.

Zauwazmy, że $K[\sqrt{r}] = \{a + b\sqrt{r} \mid a, b \in K\}$.

Niech $K = \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n}]$ będzie ciałem o następujących własnościach:

- $p_1, \ldots, p_n$ są parami różnymi liczbami pierwszymi;
- Jest to rozszerzenie nietrywialne, tzn. dla każdego $i \in \{1, 2, \ldots, n\}$ zachodzi warunek $\sqrt{p_i} \notin \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{i-1}}, \sqrt{p_i}$
- Istnieje liczba całkowita $S > 1$ niepodzielna przez żadną z liczb $p_1, \ldots, p_n$ ani przez kwadrat żadnej liczby pierwszej, taka, że $\sqrt{S} \in K$;
- Spośród wszystkich ciał spełniających powyższe warunki wybieramy to o najmniejszym możliwym n;
- Spośród wszystkich ciał spełniających powyższe warunki wybieramy dowolne.

Zauważmy, że gdy jakiś skończony układ $\sqrt{q_1}, \ldots, \sqrt{q_k}$ pierwiastków liczb pierwszych jest liniowo zależny, to któryś z pierwiastków jest kombinacją liniową pozostałych, a więc w szczególności należy do ciała powstałego z rozszerzenia $\mathbb{Q}$ o pozostałe pierwiastki. Stąd mamy, że warunek trzeci w powyższym wykazie warunków dla ciała K jest spełnialny (biorąc S równe temu pierwiastkowi), a więc istnieje takie ciało K.

Zauważmy, że $n > 1$, gdyż $\mathbb{Q}$ nie spełnia warunku trzeciego, na mocy znanego faktu, że pierwiastek liczby naturalnej jest naturalny lub niewymierny. Istotnie, gdyby $\sqrt{u} = \frac{p}{q}$, to $p^2 = uq^2$ i porównując parzystości wykładników w rozkładzie obu stron na czynniki pierwsze, mielibyśmy, że u jest kwadratem liczby całkowitej.

Rozpatrzmy ciało $L = \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{n-1}}]$ i oznaczmy $q = p_n$, zaś S niech będzie liczbą z warunku trzeciego na ciało K. Wiemy, że $\sqrt{S} \in K = L[\sqrt{q}]$. Wtedy jednak $\sqrt{S} = a + b\sqrt{q}$, dla pewnych $a, b \in L$, skąd mamy, że $S = a^2 + 2ab\sqrt{q} + b^2 q$.

Gdyby $ab \neq 0$, to mielibyśmy $L \not\ni \sqrt{q} = (S - a^2 - b^2 q) \cdot (2ab)^{-1} \in L$ – sprzeczność.

Gdyby $b = 0$, to mielibyśmy $\sqrt{S} = a \in L$, co znów jest sprzecznością z minimalnością K.

Gdyby $a = 0 \neq b$, to mielibyśmy, że $\sqrt{S} = b\sqrt{q}$, skąd $\sqrt{Sq} = bq \in L$. Jednak $q \nmid S$ oraz S jest bezkwadratowe, a więc Sq jest bezkwadratowe, skąd mamy, że ciało L spełnia warunek trzeci dla ciała K, co jest sprzeczne z minimalnością (warunkiem czwartym).

Zadanie 6

Udowodnię, że obie części są fałszywe. Weźmy nad $GF(2)$ przestrzeń $V = GF(2)^3$ z podprzestrzeniami: $U = \{(0,0,0), (1,0,0), (0,1,0), (1,1,0)\}$, $W_1 = \{(0,0,0), (0,1,1)\}$, $W_2 = \{(0,0,0), (1,0,1)\}$.

Część a

Dowód. Wtedy mamy, że wektor $(1,1,0) \in U$, oraz $(1,1,0) = (0,1,1) + (1,0,1) \in W_1 + W_2$, skąd $(1,1,0) \in U \cap (W_1 + W_2)$.

Z drugiej strony $U \cap W_1 = U \cap W_2 = \{(0,0,0)\}$, czyli $(U \cap W_1) + (U \cap W_2) = \{(0,0,0)\} \not\ni (1,1,0)$. □

Część b

Dowód. Wtedy mamy, że wektor $(1,1,1)$ należy do $U + W_1$ (gdyż $(1,1,1) = (1,0,0) + (0,1,1)$) oraz do $U + W_2$ (gdyż $(1,1,1) = (0,1,0) + (1,0,1)$), czyli należy do $(U + W_1) \cap (U + W_2)$.

Z drugiej strony zauważmy, że $W_1 \cap W_2 = \{(0,0,0)\}$, a więc $U + (W_1 \cap W_2) = U$, zaś $(1,1,1) \notin U$. □