Zadanie 1 (2.1). *Pokaż, że* $(P(X), \triangle)$ *jest grupą abelową, dla* $X \neq \emptyset$.

Zauważmy wpierw, że dla wszystkich $A, B \subset X$, $A \triangle B \subset A \cup B \subset X$, zatem $P(X)$ jest zamknięte na działanie $\triangle$.
Zauważmy, że $(x \in A \triangle B) \Leftrightarrow ((x \in A) \dot{\vee} (x \in B))$, zatem wystarczy sprawdzić, że zbiór waluacji zdań z działaniem $\dot{\vee}$ jest grupą abelową:

$\dot{\vee}$	0	1
0	0	1
1	1	0

Łatwo zauważyć, że 0 jest elementem neutralnym takiej grupy.
W każdym wierszu i kolumnie tabelki mamy dokładnie jeden element neutralny. Zatem istnieje element przeciwny do każdego dla takiej grupy. W dodatku każde 0 jest na przekątnej, co oznacza, że każdy element jest sam do siebie przeciwny względem $\dot{\vee}$.
W dodatku macierz wyników jest symetryczna względem przekątnej, więc działanie to jest abelowe.
Dla wszystkich waluacji x, y zachodzi $(0 \dot{\vee} x) \dot{\vee} y = 0 \dot{\vee} (x \dot{\vee} y)$ (ten fakt zachodzi dla (symetrycznych) elementów neutralnych w dowolnej strukturze algebraicznej). Podobnie, gdy zamienimy $x, 0$ lub $y, 0$ rolami.
Ostatni przypadek do sprawdzenia łączności to $(1 \dot{\vee} 1) \dot{\vee} 1 = 0 \dot{\vee} 1 = 1 = 1 \dot{\vee} 0 = 1 \dot{\vee} (1 \dot{\vee} 1)$.
Stąd również $(P(X), \triangle)$ jest grupą abelową. Jej element neutralny e to zbiór pusty, bo dla wszystkich $x \in X$, $x \in e = 0$, bo 0 było elementem neutralnym poprzedniej grupy.
Podobnie $A^{-1} = A$, bo dla wszystkich $x \in X$, $x \in A \Rightarrow x \in A^{-1}$ oraz $x \notin A \Rightarrow x \notin A^{-1}$, bo w poprzedniej grupie element przeciwny do elementu był sobą samym.

Zadanie 2 (2.2). *Niech* $|X| = n$. *Pokazać, że* $(P(X), \triangle)$ *jest izomorficzna z* $(C_2 \times \ldots \times C_2, +_2^{(n)})$.

Niech $A \subset X = \{x_1, x_2, \ldots, x_n\}$.
Określmy funkcję charakterystyczną zbioru A: $\chi(A) = (1_A(x_1), 1_A(x_2), \ldots, 1_A(x_n))$, gdzie

$$1_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

Jasne jest, że jeśli $A \neq B$, to istnieje $x_i \in A \triangle B$, zatem $i - ta$ współrzędna $|\chi(A) - \chi(B)| = 1$, więc χ jest iniekcją. Ponieważ przyjmuje ona również 2^n różnych wartości, a $|P(X)| = 2^n$, to jest również surjekcją. Ponadto jest to (homo)morfizm, gdyż korzystając z tego, że tabelka działania $\dot{\vee}$ jest identyczna z dodawaniem w C_2, mamy:

$$\chi(A \triangle B) = (1_{A \triangle B}(x_1), 1_{A \triangle B}(x_2), \ldots, 1_{A \triangle B}(x_n)) = (1_A(x_1) +_2 1_B(x_1), \ldots, 1_A(x_n) +_2 1_B(x_n)) = \chi(A) +_2^{(n)} \chi(B)\,.$$

Uwaga $(\{0,1\}, \dot{\vee})$ jest grupą izomorficzna z $(C_2, +_2)$, skąd można również wnioskować powyższy fakt.

Q Co to jest podgrupa normalna?

A Jest to podgrupa $H < G$, że $(\forall g \in G) gH = Hg$, gdzie $gH := \{gh : h \in H\}$ oraz $Hg := \{hg : h \in H\}$. Oznaczamy ją przez $H \triangleleft G$.

Zadanie 3 (6). *Niech* $H < G$ *i* $|G/H| = 2$. *Pokaż, że* $H \triangleleft G$.

Jeśli $h \in H$, to $hH = H$, gdyż dla dowolnego $h' \in H$ mamy: $h' = h(h^{-1}h')$, gdzie $h^{-1}h' \in H$, bo to grupa. Zatem $H \in G/H$.
Niech zatem $g \notin H$. Wtedy $gH \cap H = \emptyset$, bo inaczej $(\exists h, h' \in H) gh' = h$, czyli $g = h'^{-1}h \in H$, wbrew założeniu. W identyczny sposób dowodzimy, że $Hg \cap H = \emptyset$. Stąd $G/H = \{H, gH\}$.
Oczywiście $H \dot{\cup} gH = G$, bo inaczej istnieje g' z dopełnienia tej sumy mnogościowej, które należy do $g'H (\ni g'e)$. To oznaczałoby, że $|G/H| > 2$. Z podobnych względów $H \dot{\cup} Hg \subset G$ (nie znamy mocy warstw prawostronnych $G \backslash H$).
Mnożąc lewostronnie $H \dot{\cup} gH = G$ przez g^{-1}, a następnie prawostronnie przez g, otrzymujemy $g^{-1}Hg \dot{\cup} Hg = G$. Stąd $H \subset g^{-1}Hg$, czyli $gH \subset Hg$. Zatem $G = H \dot{\cup} gH \subset H \dot{\cup} Hg \subset G$. Stąd mamy $gH = Hg$.

Q Co należy pokazać, aby uzasadnić, że $H < G$, jeśli wiemy, że G jest grupą?

A Wystarczy udowodnić, że

$$(\forall x, y \in H)\ xy^{-1} \in H$$

oraz, że $H \subset G$, a jeśli H jest skończonym podzbiorem G, to można w zamian sprawdzić warunek

$$(\forall x, y \in H)\ xy \in H\ .$$

Zadanie 4 (7). *Niech $G = (\mathbb{R}^2, +)$ oraz $H = \{(x, 0) : x \in \mathbb{R}\}$. Pokaż, że $H \triangleleft G$. Znajdź homomorfizm $f : G \to \mathbb{R}$, że $ker(f) = H$. Wyznacz G/H.*

$H < G$, bo $(x_1, 0) + (-x_2, 0) = (x_1 - x_2, 0) \in H$. Weźmy dowolne $g := (s, t) \in G$. Wtedy $gH = \{(x + s, t) : x, s, t \in \mathbb{R}\} = \mathbb{R} \times \{t\} (= [(0, t)]_\sim)$. Oczywiście $gH = Hg$, bo $+$ w $\mathbb{R}^2$ jest działaniem przemiennym, więc wobec dowolności g, H jest podgrupą normalną.
Przykładem homomorfizmu f, spełaniającego warunki zadania, jest wartość drugiej współrzędnej: $f(x, y) = (0, y)$.
$f(x_1, y_1) + f(x_2, y_2) = (0, y_1) + (0, y_2) = (0, y_1 + y_2) = f(x_1 + x_2, y_1 + y_2)$. Wtedy $kerf$ to zbiór tych punktów płaszczyzny, których druga współrzędna to 0, czyli H. Innym przykładem takiego endomorfzimu (homomorfizmu „w siebie") może być przeskalowanie powyższej funkcji f.
Zauważyliśmy wcześniej, że $(s, t)H = \mathbb{R} \times \{t\} = [(0, t)]_\sim$, zatem $G/H = \{\mathbb{R} \times \{t\} : t \in \mathbb{R}\} \cong (\mathbb{R}, +)$.

Q Czym różnią się klasy abstrakcji g, wyznaczonych za pomocą lewostronnych warstw od wyznaczonych za pomocą prawostronnych warstw?

A Niech $H < G$ oraz $x \in gH$, co oznacza, że $g^{-1}x \in H$, a zatem $x \sim_L g$, gdy zachodzi ten warunek. Stąd $[g]_{\sim_L} = \{x \in G : g^{-1}x \in H\}$. Analogicznie, jeśli $x \in Hg$, to $xg^{-1} \in H$, czyli $[g]_{\sim_P} = \{x \in G : xg^{-1} \in H\}$. Z definicji powyższych klas abstrakcji widać, że, gdy G jest przemienną grupą, to $H \triangleleft G$.

Q Z istnienia pojęcia normalności podgrupy można się spodziewać, że istnieją podgrupy, których $gH \neq Hg$. Czy dla każdej podgrupy, warstwa lewostronna gH jest równa jakiejś warstwie prawostronnej Hg', gdzie g nie koniecznie jest równe g'?

A Nie. Odpowiedź poniżej.

Zadanie 5 (11.2). *Wyznacz warstwy podgrupy $H = \{Id, (2, 3)\}$ w $G = S_3$.*

Wartstwy lewostronne:
$IdH = (2, 3)H = \{Id, (2, 3)\}$;
$(1, 2, 3)H = (1, 2)H = \{(1, 2, 3), (1, 2)\}$;
$(1, 3, 2)H = (1, 3)H = \{(1, 3, 2), (1, 3)\}$.

Warstwy prawostronne:
$HId = H(2, 3) = \{Id, (2, 3)\}$;
$H(1, 2, 3) = H(1, 3) = \{(1, 2, 3), (1, 3)\}$;
$H(1, 3, 2) = H(1, 2) = \{(1, 3, 2), (1, 2)\}$. Wniosek: H nie jest podgrupą normalną G.

Zadanie 6 (15). *G jest grupą abelową, gdzie $a, b \in G$ oraz $ord(a) = 5$ oraz $ord(b) = 2$. Znaleźć postać $\langle\{a, b\}\rangle$.*

Z założeń o rzędzie elementów, wiadomo, że nasza podgrupa generowana przez a i b musi zawierać elementy e, a, a^2, a^3, a^4, b. Ponadto, wiadomo, że jest podgrupa grupy abelowej, jest przemienna, co oznacza, że każdy element można zapisać w postaci $a^\alpha b^\beta$ (np. $a^2baba^2 = a^2ba^3b = a^2b^2a^3 = a^5b^2 = e^2 = e$), przy czym sens mają tylko potęgi naturalne, mniejsze od odpowiednich rzędów, tj. $\alpha \in \{0,1,2,3,4\}$, a $b \in \{0,1\}$ (np. $a^{13} = (a^5)^2a^3 = e^2a^3 = a^3$). Stąd dostajemy, że $\langle\{a,b\}\rangle = \{e, a, a^2, a^3, a^4, b, ba, ba^2, ba^3, ba^4\}$.

Twierdzenie 1 (Euklides)**.** *Niech $a, b \in \mathbb{N}_+$ oraz $d = NWD(a,b)$. Istnieją takie $x, y \in \mathbb{Z}$, że $ax + by = d$. Ponadto nie istnieją $r \in \mathbb{Z}$, że $0 < r < d$ oraz $r = ax + by$ dla pewnych $x, y \in \mathbb{Z}$.*

Dowód. Rozważmy zbiór $D = \{c > 0 : c = ax + by,\ x, y \in \mathbb{Z}\}$. D jest niepusty, bo zawiera a oraz b. Zatem posiada element najmniejszy (z czego to wynika?). Oznaczmy go przez d'. Niech $a = qd' + r$, gdzie $0 \leqslant r < d'$. Wtedy $a = q(ax + by) + r$, czyli $r = a(1 - qx) - bqy$. Stąd albo $r \in D$ i $r < d'$, co jest sprzeczne z minimalnością d' albo $r = 0$. Wnioskujemy, że a jest wielokrotnością d'. Symetrycznie $d'|b$. Łatwo zauważyć, ze również d' jest największym dzielnikiem obu tych liczb, gdyż, jeśli $k|a$ oraz $k|b$, to z definicji d', $k|d'$. □

Zadanie 7 (16)**.** *Niech $G = \langle g\rangle$ będzie n-elementową grupą cykliczną. Pokaż, że $\langle g^k\rangle = \langle g^{NWD(n,k)}\rangle$ dla każdego $k \geqslant 1$. Wywnioskuj, że jeśli $d|m$ w m-elementowej grupie cyklicznej, to istnieje dokładnie jedna podgrupa mocy d.*

Niech $d = NWD(n,k)$. Wtedy $d = nx+ky$ dla pewnych $x, y \in ZZ$. Zatem $g^d = g^{nx+ky} = (g^n)^x(g^k)^y = (g^k)^y \ni \langle g^k\rangle$. Podobnie, jeśli d jest dzielnikiem k, to istnieje s, że $ds = k$, czyli $g^k = (g^d)^s \ni \langle g^{NWD(n,k)}\rangle$. Stąd mamy pierwszą własność.
Łatwo zauważyć, że $NWD(\frac{m}{d}, m) = \frac{m}{d}$. Ponadto $|\langle g^{\frac{m}{d}}\rangle| = d$. Korzystając z pierwszej własności, można pokazać, że $\langle\{g^k, g^l\}\rangle = \langle g^{NWD(k,l,m)}\rangle$, a dalej indukcyjnie dla większych generatorów. Zatem każda podgrupa jest generowana przez jeden element. Rozważmy zatem $\langle g^{NWD(m,k)}\rangle$. Ponieważ $NWD(m,k)$ dzieli m, więc istnieje liczba s, że $NWD(m,k)s = m$. Zatem powyższa podgrupa ma s elementów, a z założenia musi to być d. Stąd $NWD(m,k) = \frac{m}{d}$. Zatem istnieje tylko jedna podgrupa rzędu d.

Zadanie 8 (20)**.** *Oblicz $2^{2017} \bmod 11$ oraz $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 7$.*

Z Małego Twierdzenia Fermata wynika, że $a^{p-1} = 1 \bmod p$. Zatem $2^{10} = 1 \bmod 11$.
Zastanówmy się zatem ile wynosi 2^5 (5 jest „dużym" dzielnikiem 10).
$2^5 = 32 = -1 \bmod 11$. Stąd $2^{2017} = (2^5)^{403}2^2 = (-1)^{403}4 = -4 = 7 \bmod 11$.
Podobnie $a^6 = 1 \bmod 7$. Zatem można rozważać a^3.
$2^3 = 8 = 1 \bmod 7$. $5 = -2 \bmod 7$, a 3 jest nieparzyste, więc $5^3 = -2^3 = -1 \bmod 7$.
$3^3 = 27 = -1 \bmod 7$, a więc $4^3 = 1 \bmod 7$. Osobno można rozpatrzyć przypadek $6 = -1 \bmod 7$.
Stąd

$$2^{20}+3^{30}+4^{40}+5^{50}+6^{60} = (2^3)^62^2+(3^3)^{10}+(4^3)^{13}4^1+(5^3)^{16}5^2+(-1)^{60} = 4+1+4+25+1 = 35 = 0 \bmod 7\ .$$

Zadanie 9 (22)**.** *Oblicz $\varphi(81000)$.*

Niech $\prod_{i=1} p_i^{a_i}$ będzie rozkładem n na czynniki pierwsze. Zachodzi wtedy wzór

$$\varphi(n) = \prod_{i=1} p_i^{a_i-1}(p_i - 1)\ .$$

$81000 = 2^3 \cdot 3^4 \cdot 5^3$, zatem $\varphi(81000) = 2^2(2-1) \cdot 3^3(3-1) \cdot 5^2(5-1) = 4 \cdot 54 \cdot 100 = 21600$.

Uwaga Aby udowodnic powyższy wzór, należy najpierw wyznaczyć $\varphi(1)$ oraz $\varphi(p^\alpha)$, a następnie skorzystać z własności multiplikatywności tocjentu Eulera (w sensie funkcji arytmetycznych (funkcji z $\mathbb{C}^{\mathbb{N}}$), tj. $f(n)f(m) = f(nm)$, gdy tylko $NWD(n,m) = 1$).

Zadanie 10 (24). *Wyznacz wszystkie n, że $\varphi(n) = 6$.*

Wypiszmy wszystkie dzielniki 6: $1, 2, 3, 6$. 1 nie jest pierwsze, ale jest poprzednikiem 2, które jest pierwsze. Ponadto $p^{1-1} = 1$, dla wszystkich p. 2 jest zarówno pierwsze, jak i poprzednikiem liczby pierwszej. 3 jest pierwsze, ale nie jest poprzednikiem liczby pierwszej. 6 nie jest pierwsze, ale jest poprzednikiem liczby pierwszej 7.
Przypuśćmy, że 7 jest w rozkładzie na czynniki (jak we wzorze z poprz. zadania) liczby n. Wtedy $7|n$, ale $7^2 \not| n$, bo inaczej $7|\varphi(n)$. Wtedy ewentualnym dodatkowym czynnikiem jest 1, co oznacza, że $\underline{n = 7}$ lub $\underline{n = 14}$, bo można pozwolić jedynie, żeby $p - 1 = 1$, czyli $p = 2$, ale ponieważ $2^{a-1} = 1$, więc $a = 1$.
Załóżmy teraz, że 7 nie ma w rozkładzie n na czynniki pierwsze. Wtedy rozkład ten musi zawierać 3, gdyż nie jest to poprzednik liczby pierwszej, a któraś z wielokrotności 3 musi sie pojawić w rozkładzie $\varphi(n)$, a wiemy, że nie może pojawić się w tym przypadku ($7 \not| n$) żadna inna. Dlatego może pojawić się tylko w 2 potędze, bo 3^{a-1} musi dzielić 3, ale nie może dzielić 3^2. Zatem wśród czynników $\varphi(n)$ pojawia się $3^1(3-1) = 6$. Analogiczny argument jak w pierwszym przypadku ($(p-1) = 1$ i $p^{a-1} = 1$) daje, że $\underline{n = 9}$ lub $\underline{n = 18}$.
Innych przypadków nie ma, bo wśród czynników rozkładu $\varphi(n)$ musi być wielokrotność 3.

Zadanie 11 (27). *Niech p, q będą róznymi liczbami pierwszymi względnie pierwszymi z a. Pokaż, że*

$$a^{(p-1)(q-1)} = 1 \, mod \, pq \ .$$

Zadanie polega na wykorzystaniu Małego Twierdzenia Fermata, ale wynika bezpośrednio z ogólniejszej wersji twierdzenia (Twierdzenia Eulera), które mówi, że

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

jeśli $NWD(a, n) = 1$.

Zadanie 12 (29). *Skorzystaj z Chińskiego twierdzenia o resztach do znalezienia rozwiązania równania*

$$x^3 - x + 1 = \ 0 \, mod \, 35 \ .$$

$35 = 5 \cdot 7$, więc można rozważyć układ równań modulo 5 i 7.
Z innej strony, równanie można przekształcic do postaci $x(x-1)(x+1) = -1$, co oznacza, że $x \notin \{-1, 0, 1\}$. Lewą strone powyższego równania oznaczmy przez $w(x)$. Przy rozważaniu $\mathbb{Z}_5$ dostajemy, że $x \in \{2, 3\}$. $w(2) = 6 = 1$. Ponieważ w ma 3 czynniki, zatem $w(-2) = w(3) = -1$. Zatem $x^3 - x + 1 = \ 0 \, mod \, 5$ dla $x = 3$.
Podobnie, w $\mathbb{Z}_7$, $w(2) = 6 = -1$. Wiadomo wtedy, że $w(-2) = w(5) = 1$. Ponadto $w(3) = 24 = 3$ oraz $w(4) = -3 = 4$. Zatem jedyne rozwiązanie $x^3 - x + 1 = \ 0 \, mod \, 7$ to $x = 2$.
Wracamy teraz do $\mathbb{Z}_{35}$. Rozwiązanie jest postaci $x = 5k + 3 = 7l + 2$, gdzie $k, l \in \mathbb{Z}$.
Gdy $k = l = 0$, to z jednej strony mamy 3, a z drugiej 2, Zatem równica to 1. Ale przy jednoczenym zwiększeniu k i l o 1, różnica maleje o 2, więc po 3 takich krokach wyniesie -5 (wielokrotność 5 lub 7). Zatem po dodaniu 5, otrzymamy 0. Zatem jednym z rozwiązań jest $k = 3 + 1 = 4$ oraz $l = 3$, czyli $x = 23$.
Chińskie twierdzenie o resztach mówi, że każde rozwiązanie otrzymujemy z warunku $x = 23 \, mod \, 35$ (każde rozwiązanie tego równania jest też rozwiązaniem także równania wyjściowego i vice versa).

Zadanie 13 (32). *Wyznacz generatory grupy $\mathbb{Z}_{11}^*$.*

Rozważmy kolejne potęgi 2 modulo 11: $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$. Otrzymaliśmy $10 = 11 - 1$ różnych, zatem 2 jest szukanym generatorem. Niech $2 = g$. Z zadania 16.[7] wiemy, że $\langle g^k \rangle = \langle g^{NWD(n,k)} \rangle$ w n-elementowej grupie cyklicznej. Chcemy, aby $\mathbb{Z}_{11}^*$ była 10-elementową grupą cykliczną. Zatem aby 2^k było generatorem, potrzeba i wystarcza (z tego samego zadania), aby $NWD(k, 10) = 1$. Czyli generatorami będą potęgi 2 o wykładnikach $1, 3, 7$ i 9, czyli odpowiednio $2, 8, 7$ i 6.
Jeśli na początku rozważalibyśmy 3, a nie 2, to otrzymalibyśmy potęgi: $3, 9, 5, 4, 1$. Nie ma ich 10, co oznacza, że to nie względnie pierwsze z 10 potęgi generatorów $\mathbb{Z}_{11}^*$, czyli żadna z wymienionych liczb nie może być generatorem. 10 odpada z podobnych (bardziej oczywistych) powodów. Natomiast $\varphi(10) = 4$, a wyrzuciliśmy już 6 liczb, zatem pozostałe 4 są generatorami.

Zadanie 14 (36.4)**.** *Załóżmy, że $(G, \cdot)$ i $(H, \star)$ są skończonymi grupami i $NWD(|G|, |H|) = 1$. Pokaż, że $Aut(G \times H)$ oraz $Aut(G) \times Aut(H)$ są izomorficzne.*

Niech $\chi \in Aut(G \times H)$. Oznaczmy działanie na $G \times H$ przez $\otimes$. Niech $e_G \neq g \in G$ i $e_H \neq h \in H$, gdzie e_G i e_H, to odpowiednio elementy neutralne grup G i H. Niech dodatkowo $\chi(g, h) = (g', h')$, a f będzie homomorfizmem między $Aut(G \times H)$ oraz $Aut(G) \times Aut(H)$. Wtedy $\chi(g, h) = \chi(e_G \cdot g, h \star e_H) = \chi(e_G, h) \otimes \chi(g, e_H)$. Przypuśćmy, że $\chi(e_G, h) = (g', h')$, gdzie $g' \neq e_G$. Wtedy $(e_G, e_H) = \chi(e_G, e_H) = \chi((e_G, h)^{ord(h)}) = (\chi(e_G, h))^{ord(h)} = (g', h')^{ord(h)} = (g'^{ord(h)}, h'^{ord(h)})$, skąd $g'^{ord(h)} = e_G$, co oznacza, że $ord(g')|ord(h)$ ale z tw. Lagrange'a, $ord(h)||H|$ i $ord(g')||G|$, więc $ord(g')|NWD(|G|, |H|)$, czyli $g' = e_G$. Sprzeczność z założeniem.
Zatem $\chi[\{e_G\} \times H] \subset \{e_G\} \times H$. Analogicznie dla $\chi[G \times \{e_H\}]$. Ale χ jest bijekcją, więc zachodzą równości. Oznacza to, że $\chi(g, h) = (\varphi(g), \psi(h))$, gdzie φ to pewien izomorfizm na G, a ψ – pewien izomorfizm na H. Wtedy, gdy zdefiniujemy $f(\chi) = (\varphi, \psi)$, to

$$(\varphi_1 \circ \varphi_2, \psi_1 \circ \psi_2) = f(\chi_1 \otimes \chi_2) = f(\chi_1) \circ f(\chi_2) = (\varphi_1, \psi_1) \circ (\varphi_2, \psi_2) = (\varphi_1 \circ \varphi_2, \psi_1 \circ \psi_2)$$

pokazuje w istocie homomorficzność f. Natomiast bijektywność wynika wprost z bijektywności φ oraz ψ.

Uwaga Teza zadania 36.5 jest potrzebna do wyprowdzenia wzoru dla tocjentu Eulera, podanego w rozwiązaniu zadania 22.[9]. (patrz: jedna ze wcześniejszych uwag).

Twierdzenie 2 (O Izomorfizmie)**.** *Niech G, H będą grupami, a $f : G \to H$ homomorfizmem.*
Wtedy $G\big|_{Ker(f)}$ jest izomorficzne z $Im(f)$.

Zadanie 15 (38.3)**.** *$\theta_a(w) = w(a)$, dla $w \in \mathbb{R}[x]$.*
Znajdź pierścień $\mathbb{R}[x]\big|_{Ker(\theta_a)}$.

Łatwo zauważyć, że $Im(\theta_a(w)) = \mathbb{R}$. Z tw. o izomorfizmie $\mathbb{R}[x]\big|_{Ker(\theta_a)} \simeq Im(\theta_a) = \mathbb{R}$.

Zadanie 16 (44)**.** *Pokaż, że $\mathbb{Z}[x]\big|_{(x)} \simeq \mathbb{Z}$.*

Niech $f = \theta_0$. Wtedy $(x) = Ker(\theta_0)$, zatem analogicznie do zadania 38.3 otrzymujemy tezę.

Zadanie 17 (46)**.** *Zbadaj pierścień $\mathbb{R}[x]\big|_{(x^2-1)}$.*

Zerem powyższego pierścienia jest $(x^2 - 1)$. $x^2 - 1 = (x - 1)(x + 1)$. Zobaczmy, że przekrój ideałów $(x - 1) \cap (x + 1) = (x^2 - 1)$. Niech $f = (\theta_{-1}, \theta_1)$. Wtedy $Ker(f) = (x^2 - 1)$, natomiast $Im(f)\mathbb{R}^2$. Zatem $\mathbb{R}[x]\big|_{(x^2-1)} \simeq \mathbb{R}^2$

Zadanie 18 (47.1)**.** *Pokaż, że $R[x, y] \simeq (R[x])[y]$.*

Niech $w(x,y) = \sum_{k=0}^{n} \sum_{l=0}^{m} a_{k,l} x^l y^k$ będzie dowolnym wielomianem z $R[x,y]$. Piszemy $a_{k,l} = [x^l y^k]w$. Niech $f : R[x,y] \to (R[x])[y]$ będzie zadana wzorem:

$$f\left(\sum_{k=0}^{n}\sum_{l=0}^{m} a_{k,l}x^l y^k\right) = \sum_{k=0}^{n}\left(\sum_{l=0}^{m} a_{k,l}x^l\right) y^k \ ,$$

gdzie $(\forall k)\sum_{l=0}^{m} a_{k,l}x^l \in R[x]$.
W przestrzeni wielomianów obowiązuje metryka formalna, zatem dwa wielomiany są równe, jeśli wszystkie współczynniki są równe. Jeśli $w, q \in R[x,y]$ są równymi wielomianami, to istnieje k, l, że $[x^l y^k]w \neq [x^l y^k]q$. Ale wtedy $[y^k]f(w) \neq [y^k]f(q)$. Stąd mamy różnowartościowość f. Proste spostrzeżenie, że f^{-1} jest funkcją, daje surjektywność. Morfizm jest oczywisty.