Zadanie 1

Określmy operacje tak, aby odpowiadały one dodawaniu i mnożeniu modulo 3, przy przyjęciu, że $a = 2$.
Operacja dodawania:

$+$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

Operacja mnożenia:

$\cdot$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Zauważmy teraz, że oba te działania są przemienne, istnieje element neutralny dodawania i element neutralny odejmowania, a także dla każdego elementu istnieje element przeciwny, a dla niezerowego elementu – element odwrotny.

Pozostaje sprawdzić łączność i rozdzielność, lecz jednak łatwo widać, że skoro zachodzą one w $\mathbb{Z}$, a branie reszty modulo 3 zachowuje te własności, to także w podanym wyżej zbiorze działania spełniają te własności.

Zadanie 2

Rozpatrzmy najpierw zbiór K wielomianów nad $\mathbb{Q}$, branych modulo wielomian $P(x) = x^3 - 7$. Twierdzę, że wraz z kanonicznymi operacjami mnożenia i dodawania wielomianów modulo wielomian tworzy on ciało. Oczywiście tworzy on pierścień przemienny z jedynką, gdyż dodawanie jest łączne i przemienne, istnieje zero oraz dla każdego elementu – element przeciwny. Tak samo mnożenie jest łączne i przemienne, a także rozdzielne względem dodawania oraz istnieje jedynka.

Wystarczy więc pokazać istnienie elementów odwrotnych. Najpierw zauważmy, że wielomian P jest nierozkładalny nad $\mathbb{Q}$, co wynika np. z kryterium Eisensteina dla $p = 7$ albo faktu, że nie ma on pierwiastków wymiernych i jest stopnia trzeciego.

Weźmy więc jakiś niezerowy wielomian $Q(x) \in \mathbb{Q}[X]$ o stopniu mniejszym niż 3. Wtedy łatwo widać, że $\mathrm{NWD}(Q(x), P(x)) = 1$, a zatem rozszerzony algorytm Euklidesa ($\mathbb{Q}[X]$ jest pierścieniem euklidesowym) da nam wielomiany $K(x), L(x) \in \mathbb{Q}[X]$ takie, że $K(x) \cdot Q(x) + L(x) \cdot P(x) = 1$. Biorąc to modulo wielomian $P(x)$ otrzymujemy równość w pierścieniu K: $K(x) \cdot Q(x) = 1$, a zatem $K(x)$ jest odwrotnością wielomianu $Q(x)$.

Stąd K jest ciałem. Pokażemy teraz, że zbiór V z zadania jest izomorficzny z K. Izomorfizm $\phi : K \to V$ zdefiniujemy jako: $\phi(Q) = Q(\sqrt[3]{7})$. Zauważmy, że istotnie jest on zgodny ze wszystkimi działaniami, trzeba jednak udowodnić, że jest bijekcją.

Dla każdego $x \in V$ z definicji V mamy, że $x = a + \sqrt[3]{7}b + (\sqrt[3]{7})^2 c$, a więc istotnie $x = \phi(a + bx + cx^2)$, a więc jest to surjekcja.

Aby pokazać injektywność, załóżmy, że pewne $x = \phi(a + bx + cx^2) = \phi(t + ux + vx^2)$. Wtedy z liniowości ϕ, $0 = \phi((a - t) + (b - u)x + (c - v)x^2)$. To zaś oznacza, że $x = \sqrt[3]{7}$ jest nad $\mathbb{Q}$ pierwiastkiem wielomianu $Z(x) = (a - t) + (b - u)x + (c - v)x^2 + kP(x)$. Jest on jednak także pierwiastkiem wielomianu $P(x)$, a więc jest pierwiastkiem największego wspólnego dzielnika tych wielomianów, który jednak z nierozkładalności $P(x)$ jest równy albo $P(x)$ albo 1. W tym drugim przypadku mamy sprzeczność, w pierwszym zaś mamy, że $P(x)|Z(x)$, a więc tak naprawdę, to w K mamy $Z(x) = 0$.

To zaś oznacza, że jednak ϕ jest injektywna, a więc jest izomorfizmem, a więc V jest ciałem.

Zadanie 3

Dowód. Możemy operacje dwuargumentowe na zbiorze $\{0, 1\}$ utożsamiać z operacjami logicznymi.

Zauważmy, że za pomocą działania $|$ (które będę dalej nazywał NAND), można zdefiniować negację: istotnie $a|a \iff \neg a$. Za pomocą zaś negacji oraz NAND można zdefiniować koniunkcję: istotnie $\neg(a|b) \iff a \wedge b$. Za pomocą zaś negacji oraz koniunkcji można zdefiniować alternatywę korzystając z prawa De Morgana: $\neg(\neg a \wedge \neg b) \iff a \vee b$.

Mając zaś koniunkcję oraz alternatywę możemy zdefiniować każdą funkcję wyrażoną w koniunktywnej postaci normalnej, w tym przypadku oznacza to, że: każdą funkcję $f : \{0,1\}^2 \to \{0,1\}$ możemy zapisać jako alternatywę koniunkcji. Dla każdej pary (A, B) dla której $f(A, B) = 1$ piszemy odpowiednią koniunkcję warunków (np. jeśli $f(0, 1) = 1$, to piszemy $\neg a \wedge b$), a następnie łączymy wszystkie takie warunki alternatywą – takie wyrażenie będzie równoważne funkcji f.

Jest to istotnie funkcja f zapisana wyłącznie z użyciem koniunkcji, alternatywy i negacji, zaś wszystkie je można wyrazić za pomocą operacji NAND, stąd i funkcję f można tak wyrazić. Co więcej: ograniczenie f do tylko dwóch argumentów jest zbędne, takie samo rozumowanie (korzystając nadal z dwuargumentowego NAND) można przeprowadzić także dla funkcji o większej liczbie argumentów. □

Zadanie 5

Dowód. Załóżmy, że dla działania $\circ$ elementem neutralnym jest ϵ, a dla $*$ jest to δ.

Wtedy mamy $\delta = \delta * \delta = (\epsilon \circ \delta) * (\delta \circ \epsilon) = (\epsilon * \delta) \circ (\delta * \epsilon) = \epsilon \circ \epsilon = \epsilon$, skąd możemy od tej pory pisać ϵ na wspólny obustronny element neutralny obu tych działań.

Mamy wtedy $a * b = (a \circ \epsilon) * (\epsilon \circ b) = (a * \epsilon) \circ (\epsilon * b) = a \circ b$, skąd istotnie są to takie same działania, będziemy więc na nie oba pisać $*$.

Mamy jednak: $a * b = (\epsilon * a) * (b * \epsilon) = (\epsilon * b) * (a * \epsilon) = b * a$, jest to więc działanie przemienne.

Ponadto: $(a * b) * c = (a * b) * (\epsilon * c) = (a * \epsilon) * (b * c) = a * (b * c)$, jest to więc działanie łączne. □

Zadanie 6

Część a

Dowód. Zauważmy, że $b*a = (a*b)*(a*b) = ((b*a)*(b*a))*((b*a)*(b*a))$. Jednak mamy także, że $x*x = (x*x)*(x*x)$. Podstawiając $x = b*a$, otrzymujemy $(b*a)*(b*a) = ((b*a)*(b*a))*((b*a)*(b*a))$, ale jak już udowodniliśmy wyżej, jest to równe $b*a$. Stąd $(b*a)*(b*a) = b*a$, natomiast z założenia $(b*a)*(b*a) = a*b$, skąd $a*b = b*a$. □

Część b

Dowód. Zauważmy, że skoro $b \in T$, to $b = q*q$ dla pewnego $q \in S$. Z założenia mamy $(q*q)*(q*q) = (q*q)$, co daje $b*b = b$. □

Część c

Dowód. Skoro $a, b \in T$, to z części b mamy $a*a = a$. Gwiazdkując prawostronnie to równanie przez b mamy $(a*a)*b = a*b$, ale z łączności działania mamy $a*(a*b) = a*b$. □

Część d

Dowód. Skoro T jest skończony, to można zapisać jego elementy w ciągu: $x_1, x_2, \ldots, x_n$. Wtedy oznaczmy $a = x_1 * x_2 * \ldots * x_n$ (z powodu łączności działania $*$ jest to dobrze określone). Zauważmy teraz, że dla $b = x_k \in T$ mamy $a * b = (x_1 * \ldots x_n) * x_k = x_1 * \ldots * x_{k-1} * x_{k+1} * \ldots * x_n * x_k * x_k$, jednak ponieważ $x_k * x_k = x_k$, to jest to równe $x_1 * \ldots * x_{k-1} * x_{k+1} * \ldots * x_n * x_k = a$.

Łatwo też widzimy, że jeśli $x, y \in T$, to $x = t*t$, $y = u*u$, a więc $x*y = (t*t)*(u*u) = (t*u)*(t*u)$, skąd $x*y$ też należy do T. Stąd, przez indukcję, mamy, że $a \in T$. □

Część e

Dowód. Twierdzę, że szukane a jest równe temu a, które znaleźliśmy w części d. Zauważmy bowiem najpierw, że dla dowolnych $x, y \in S$: $(x*y)*(x*y) = y*x = x*y$, a więc $x*y \in T$.

Weźmy teraz $a \in T$ zdefiniowane jak wyżej oraz dowolne $b \in S$. Mamy wtedy $a*(a*b) = a$, gdyż $a*b \in T$. Z łączności mamy $(a*a)*b = a$, jednak z części drugiej $a*a = a$, skąd $a*b = a$. □