CS21001 Discrete Structures, Autumn 2007

Tutorial 10: November 1 and 8, 2007

---

1 **(a)** Define an operation $*$ on $\mathbb{R}$ as $x * y = x + y + xy$. Prove or disprove: $(\mathbb{R}, *)$ is a group.

Solution [Closure] Obvious.

[Associativity] We have $(x*y)*z = (x+y+xy)*z = (x+y+xy)+z+(x+y+xy)z = x+y+z+xy+xz+yz+xyz$ and $x*(y*z) = x*(y+z+yz) = x+(y+z+yz)+x(y+z+yz) = x+y+z+xy+xz+yz+xyz$, i.e., $(x * y) * z = x * (y * z)$.

[Identity] It is easy to check that 0 is the identity with respect to $*$.

[Inverse] Let $x \in \mathbb{R}$ have the inverse $y \in \mathbb{R}$, i.e., $x * y = x + y + xy = 0$, i.e., $y = \frac{-x}{1+x}$, i.e., y exists if and only if $x \neq -1$. Since -1 does not have an inverse under $*$, $(\mathbb{R}, *)$ is not a group.

(b) Prove or disprove: $(\mathbb{R} \setminus \{-1\}, *)$ is a group.

Solution It only remains to check the closure property. Take $x, y \in \mathbb{R}$, $x, y \neq 1$. Then $(1 + x)(1 + y) \neq 0$, i.e., $x + y + xy \neq -1$, i.e., $\mathbb{R} \setminus \{-1\}$ is closed under $*$.

2 Let S be the set of all functions $\mathbb{Z} \to \mathbb{Z}$. Define addition of functions in $\mathbb{Z}$ as $(f + g)(n) = f(n) + g(n)$ for all $n \in \mathbb{Z}$. Prove that S is an Abelian group under this addition.

Solution [Closure] Obvious.

[Associativity] $((f + g) + h)(n) = (f + g)(n) + h(n) = (f(n) + g(n)) + h(n) = f(n) + (g(n) + h(n)) = f(n) + (g + h)(n) = (f + (g + h))(n)$ for all $n \in \mathbb{Z}$.

[Identity] The zero function that takes every $n \mapsto 0$.

[Inverse] $(-f)(n) = -(f(n))$ for every $f \in S$.

[Commutativity] $(f + g)(n) = f(n) + g(n) = g(n) + f(n) = (g + f)(n)$ for all $n \in \mathbb{Z}$.

3 Prove that the set $\operatorname{Aut} G$ of all automorphisms of a group G is a group under composition of functions.

Solution Let $f, g, h \in \operatorname{Aut} G$ be arbitrary.

[Closure] $(f \circ g)(mn) = f(g(mn)) = f(g(m)g(n)) = f(g(m))f(g(n)) = (f \circ g)(m)(f \circ g)(n)$ for all $n \in \mathbb{Z}$. That is, $f \circ g$ is a group homomorphism. Moreover, the composition of two bijections is again a bijection.

[Associativity] Function composition is associative.

[Identity] The identity function id_G is an automorphism of G.

[Inverse] An automorphism is invertible as a function and the inverse map is again a homomorphism and bijective.

4 Prove that $\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^*$.

Solution Define a function $\varphi : \operatorname{Aut} \mathbb{Z}_n \to \mathbb{Z}_n^*$ as $\varphi(f) = f(1)$.

[φ is well-defined] $(\mathbb{Z}_n, +)$ is a cyclic group generated by 1. In fact, a homomorphism f of $\mathbb{Z}_n$ is fully specified by $f(1)$, and for any $a \in \mathbb{Z}_n$, we have $f(a) = a \times f(1) \pmod{n}$. Now, f is a bijective if and only if $0, f(1), 2f(1), \ldots, (n-1)f(1)$ exhaust all elements of $\mathbb{Z}_n$, i.e., if and only if $\gcd(f(1), n) = 1$, i.e., if and only if $f(1) \in \mathbb{Z}_n^*$.

[φ is a group homomorphism] Take $f, g \in \operatorname{Aut} \mathbb{Z}_n^*$. Then for $a \in \mathbb{Z}_n$, we have $\varphi(f \circ g) = (f \circ g)(1) = f(g(1)) = f(1)g(1) = \varphi(f)\varphi(g)$.

[φ is injective] If $\varphi(f) = \varphi(g)$, we have $f(1) = g(1)$, i.e., $f(a) = af(1) = ag(1) = g(a)$ for all $a \in \mathbb{Z}_n$, i.e., $f = g$.

[φ is surjective] Take any $x \in \mathbb{Z}_n^*$. Then the function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ mapping a to $xa \pmod{n}$ is clearly an automorphism of $\mathbb{Z}_n$, and we have $\varphi(f) = f(1) = x$.

5 Let G be a (multiplicative) group and let H, K be subgroups of G. Prove the following assertions.

(a) $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

Solution [If] If $H \subseteq K$, then $H \cup K = K$, whereas if $K \subseteq H$, then $H \cup K = H$. In either case, $H \cup K$ is a subgroup of G.

[Only if] Suppose that $H \cup K$ is a subgroup of G, but neither $H \subseteq K$ nor $K \subseteq H$ is true. Then there exist $a \in H \setminus K$ and $b \in K \setminus H$. Since $a, b \in H \cup K$ and $H \cup K$ is a subgroup of G, we have $ab \in H \cup K$, i.e., $ab \in H$ or $ab \in K$. If $ab \in H$, then $b = a^{-1}(ab) \in H$, a contradiction. On the other hand, if $ab \in K$, then $a = (ab)b^{-1} \in H$, a contradiction again.

(b) HK is a subgroup of G if and only if $HK = KH$.

Solution [If] Take arbitrary elements $a = h_1k_1$ and $b = h_2k_2$ in HK (with $h_1, h_2 \in H$ and $k_1, k_2 \in K$). But then $ab^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_3h_2^{-1})$, where $k_3 = k_1k_2^{-1} \in K$. Since $HK = KH$, we have $h_4 \in H$ and $k_4 \in K$ such that $k_3h_2^{-1} = h_4k_4$. But then $ab^{-1} = (h_1h_4)k_4 \in HK$.

[Only if] If HK is a subgroup of G, we have $(HK)^{-1} = HK$. But $(HK)^{-1} = K^{-1}H^{-1} = KH$.

6 Let H be a subgroup of G with index $[G : H] = 2$. Prove that $H \lhd G$.

Solution There are two right cosets of H in G, namely, H itself and $G \setminus H$. Thus for $a \in G$, we have $aH = \begin{cases} H & \text{if } a \in H, \\ G \setminus H & \text{if } a \notin H. \end{cases}$ Likewise, $Ha = \begin{cases} H & \text{if } a \in H, \\ G \setminus H & \text{if } a \notin H. \end{cases}$

7 Let G be a finite multiplicative group and $h = \operatorname{ord} a$ for some $a \in G$.

(a) $a^n = e$ if and only if $h \mid n$.

Solution [if] Let $n = th$. Then $a^n = (a^h)^t = e^t = e$.

[Only if] Suppose $a^n = e$, where $n = qh + r$ with $0 \leqslant r < h$. Since $a^h = e$, it follows that $a^r = e$. Since $\operatorname{ord} a$ is the smallest positive integer h with the property $a^h = e$, we must have $r = 0$, i.e., $n = qh$ is an integral multiple of h.

(b) Prove that $\operatorname{ord}(a^k) = \frac{h}{\gcd(h,k)}$ for any $k \in \mathbb{Z}$.

Solution Let $r = \operatorname{ord}(a^k)$. We have $(a^k)^{\frac{h}{\gcd(h,k)}} = (a^h)^{\frac{k}{\gcd(h,k)}} = e$ (since $a^h = e$ and $\frac{k}{\gcd(h,k)}$ is an integer), so $r \leqslant \frac{h}{\gcd(h,k)}$. Also $(a^k)^r = e$, so by Part (a), $h \mid kr$, i.e., $\frac{h}{\gcd(h,k)} \mid \frac{k}{\gcd(h,k)} r$. Since $\frac{h}{\gcd(h,k)}$ and $\frac{k}{\gcd(h,k)}$ are coprime, we have $\frac{h}{\gcd(h,k)} \mid r$, i.e., $\frac{h}{\gcd(h,k)} \leqslant r$.

8 Let $n \in \mathbb{N}$, $n \neq 0$. Prove that the only homomorphism $\mathbb{Z}_n \to \mathbb{Z}$ is the zero map.

Solution Let $f \in \operatorname{Hom}(\mathbb{Z}_n, \mathbb{Z})$ and $a = f(1)$. Since $1 + 1 + \cdots + 1$ (n times) $= 0$ in $\mathbb{Z}_n$, we have $0 = f(0) = nf(1) = na$. Since $n \neq 0$, we have $a = 0$, i.e., $f(1) = 0$. Since 1 generates Z_n, it follows that f is the zero map.

Additional exercises

9 Which of the following are semigroups? Monoids? Groups?

(a) The set of all (univariate) polynomials with integer coefficients under polynomial addition.
(b) The set of all polynomials with rational coefficients under polynomial addition.
(c) The set of all non-zero polynomials with integer coefficients under polynomial multiplication.
(d) The set of all non-zero polynomials with rational coefficients under polynomial multiplication.
(e) The set of all non-constant polynomials with integer coefficients under polynomial addition.
(f) The set of all non-constant polynomials with rational coefficients under polynomial multiplication.
(g) The set $\{1, -1, \mathrm{i}, -\mathrm{i}\}$ under multiplication, where i is a complex square root of unity.
(h) $\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ under addition. The same set under multiplication.
(i) $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ under addition. The same set under multiplication.

(j) $\{a+bi \mid a,b \in \mathbb{Z}\}$ under addition. The same set under multiplication.
(k) $\{a+bi \mid a,b \in \mathbb{Q}\}$ under addition. The same set under multiplication.

10 Prove that:

(a) Any group of order 4 is Abelian.
(b) Any cyclic group is Abelian.
(c) Any group of prime order is cyclic.
(d) Any Abelian group of square-free order is cyclic.

11 Let G be a group, $a,b \in G$, $m = \operatorname{ord} a$, and $n = \operatorname{ord} b$. Assume that $m,n < \infty$.

(a) Prove or disprove: $\operatorname{ord}(ab) = mn$.
(b) Prove or disprove: If $\gcd(m,n) = 1$, then $\operatorname{ord}(ab) = mn$.
(c) Prove or disprove: If G is Abelian and $\gcd(m,n) = 1$, then $\operatorname{ord}(ab) = mn$.
(d) If G is a finite cyclic group, prove that G has exactly $\phi(r)$ generators, where r is the order of G and ϕ is Euler's totient function.

12 Let G be a multiplicative group and $a \in G$.

(a) Define the *centralizer* of a as $C(a) = \{b \in G \mid ab = ba\}$. Prove that $C(a)$ is a subgroup of G. What is $C(a)$ if G is Abelian?

(b) Two elements $a,b \in G$ are said to be *conjugate* (to one another), denoted $a \sim b$, if $b = xax^{-1}$ for some $x \in G$. Prove that conjugacy is an equivalence relation on G.

(c) Prove that if $a \sim b$, then $\operatorname{ord} a = \operatorname{ord} b$.

13 **(a)** Let G be the set of all invertible (i.e., non-singular) 2×2 matrices with real entries. Prove that G is a group under matrix multiplication.

(b) Define the *center* $Z(G)$ of G as:

$$Z(G) = \{A \in G \mid AP = PA \text{ for all } P \in G\}.$$

Prove that $Z(G)$ is a normal subgroup of G.

(c) Derive that $Z(G) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R}, a \neq 0 \right\}$.

(d) A matrix $A \in G$ is said to be *similar* to a matrix $B \in G$ if $B = PAP^{-1}$ for some $P \in G$. Prove that similarity is an equivalence relation on G.

(e) For any fixed $P \in G$, define the map $f_P : G \to G$ as $f_P(A) = PAP^{-1}$. Prove that f_P is a group isomorphism.

(f) Prove that f_P is the identity map on G if and only if $P \in Z(G)$.

14 Let $f : G_1 \to G_2$ be a group homomorphism, where G_1, G_2 are multiplicative groups with identity elements e_1, e_2. Further let H_1 be a subgroup of G_1, and H_2 a subgroup of G_2. Prove the following assertions:

(a) $f(e_1) = e_2$.
(b) $f(a^{-1}) = f(a)^{-1}$ for all $a \in G_1$.
(c) $f(H_1) = \{a_2 \mid a_2 = f(a_1) \text{ for some } a_1 \in H_1\}$ is a subgroup of G_2.
(d) $f^{-1}(H_2) = \{a_1 \mid f(a_1) \in H_2\}$ is a subgroup of G_1.
(e) Let $a_2 = f(a_1)$ for some $a_1 \in G_1$. Prove or disprove: $\operatorname{ord} a_1 = \operatorname{ord} a_2$.
(f) Repeat Part (e) assuming that f is an isomorphism.
(g) $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$.

15 Let G be a finite group, and H, K subgroups of G with relatively prime orders. Prove that $H \cap K = \{e\}$.

16 Let G be a (multiplicative) group, H a subgroup of G, and $a, b \in G$. Prove that the following conditions are equivalent.

(i) $Ha = Hb$.
(ii) $b \in Ha$.
(iii) $ab^{-1} \in H$.

17 Let G be a finite cyclic group.

(a) Prove that every subgroup of G is cyclic.
(b) Let H, K be subgroups of G of respective orders s, t. What is the order of $H \cap K$?

18 Compute the multiplicative inverse of 17 modulo 71.

19 Compute the order of 19 in the multiplicative group $\mathbb{Z}_{32}^*$.

20 Let G be an Abelian group. An element $a \in G$ is called a *torsion element* of G if $\operatorname{ord} a$ is finite. Prove that the set of all torsion elements of G is a subgroup of G.

21 Prove that for any integer $n \geqslant 3$ the multiplicative group $\mathbb{Z}_{2^n}^*$ is *not* cyclic. (**Hint:** You may look at the elements $2^{n-1} \pm 1$.)

22 Prove that the only automorphisms of $(\mathbb{Z}, +)$ are the identity map and the map that sends $a \mapsto -a$.

23 Let G be a group with identity e and $H \neq \{e\}$ a subgroup of G. Prove or disprove: The only homomorphism $G/H \to G$ is the map $aH \mapsto e$ for all $a \in G$.

24 Let G be a finite cyclic group of order m, r a divisor of m, H a subgroup of G of order r, and $a \in G$. Prove that $a \in H$ if and only if $a^r = e$, where e is the identity element of G. Demonstrate by an example that this result need not hold if G is not cyclic.

25 Let $G_1, G_2, \ldots, G_n$ be groups and $G = G_1 \times G_2 \times \cdots \times G_n$. Let each G_i be finite of order m_i. Establish that G is cyclic if and only if each G_i is cyclic and $\gcd(m_i, m_j) = 1$ for $i \neq j$.

26 Let G be a finite Abelian group (with identity e) in which the number of elements x satisfying $x^n = e$ is at most n for every $n \in \mathbb{N}$. Prove that G is cyclic.