CS21001 Discrete Structures, Autumn 2005

Exercise set 4

---

1. Which of the following are semigroups? Monoids? Groups?

(a) $\mathbb{C}$ under addition of complex numbers.
(b) $\mathbb{C}$ under multiplication of complex numbers.
(c) $\mathbb{C}^*$ under addition of complex numbers, where $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
(d) $\mathbb{C}^*$ under multiplication of complex numbers.
(e) The set of all (univariate) polynomials with integer coefficients under polynomial addition.
(f) The set of all polynomials with rational coefficients under polynomial addition.
(g) The set of all non-zero polynomials with integer coefficients under polynomial multiplication.
(h) The set of all non-zero polynomials with rational coefficients under polynomial multiplication.
(i) The set of all non-constant polynomials with integer coefficients under polynomial addition.
(j) The set of all non-constant polynomials with rational coefficients under polynomial multiplication.
(k) The set $\{1, -1, \mathrm{i}, -\mathrm{i}\}$ under multiplication, where i is a complex square root of unity.
(l) $\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ under addition. The same set under multiplication.
(m) $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ under addition. The same set under multiplication.
(n) $\{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$ under addition. The same set under multiplication.
(o) $\{a + b\mathrm{i} \mid a, b \in \mathbb{Q}\}$ under addition. The same set under multiplication.
(p) $\mathbb{R}$ under the operation $*$ defined as $x * y = xy + x + y$.

2. Let G be a multiplicative group and $a, b \in G$. Prove that:

(a) $(ab)^{-1} = b^{-1}a^{-1}$.
(b) $(a^{-1})^{-1} = a$.

3. 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.

4. Let G be a group, $a, b \in G$, $m = \operatorname{ord} a$, $n = \operatorname{ord} b$, and $k \in \mathbb{Z}$. 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) Prove that $\operatorname{ord}(a^k) = m/\gcd(m, k)$.
(e) Conclude that if G is a finite cyclic group, then G has exactly $\phi(r)$ generators, where r is the order of G and ϕ is Euler's totient function.

5. 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 $\operatorname{ord} a = \operatorname{ord} b$.

6. 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 $G_1 \times G_2$.

7. Let G be a multiplicative group and H, K subgroups of G. Prove that:

(a) $H \cap K$ is a subgroup of G.
(b) $H \cup K$ need not be a subgroup of G.
(c) $HK = \{hk \mid h \in H, k \in K\}$ need not be a subgroup of G.
(d) HK is a subgroup of G if and only if $HK = KH$.
(e) If G is finite and $\gcd(|H|, |K|) = 1$, then $H \cap K = \{e\}$.

8. Let G be a multiplicative group and X a subset of G.

(a) Prove that $\langle X \rangle = \{x_1 x_2 \ldots x_n \mid n \in \mathbb{N}_0 \text{ and either } x_i \in X \text{ or } x_i^{-1} \in X \text{ for each } i = 1, 2, \ldots, n\}$ is a subgroup of G.

(b) Prove that $\langle X \rangle$ is the smallest subgroup of G that contains X.

* **(c)** We say that G is *generated* by X and that X is a generator of G, if $G = \langle X \rangle$. In that case, X is called a *minimal* generating set of G, if $X \setminus \{x\}$ does not generate G for all $x \in X$. Prove that for all $n \in \mathbb{N}$ there exists a minimal generating set of $(\mathbb{Z}, +)$ with exactly n elements.

9. Let $n \in \mathbb{N}$ and $n\mathbb{Z}$ denote the set of all integer multiples of n. Prove that $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$. What is the index $[\mathbb{Z} : n\mathbb{Z}]$?

10. Let H a subgroup of index 2 of a multiplicative group G. Prove that $aH = Ha$ for all $a \in G$.

11. Let G be a multiplicative group.

(a) Define a relation $\sim$ on G as $a \sim b$ if and only if $a^{-1}b \in H$. Prove that $\sim$ is an equivalence relation on G and that the equivalence classes of G with respect to $\sim$ are the left cosets of G.

(b) Define a relation $\sim'$ on G as $a \sim' b$ if and only if $ab^{-1} \in H$. Prove that $\sim'$ is an equivalence relation on G and that the equivalence classes of G with respect to $\sim'$ are the right cosets of G.

12. Let G be a finite cyclic group of order n and let s, t be divisors of n. Let H and K be subgroups of G of respective orders s, t. What is the order of $H \cap K$?

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

14. Let G be a group and $\operatorname{Aut} G$ denote the set of automorphisms of G.

(a) Prove that $\operatorname{Aut} G$ is a group under composition of functions.
** **(b)** Prove that the automorphism group of $(\mathbb{Z}_n, +)$ is isomorphic to $(\mathbb{Z}_n^*, \times)$.

15. 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.

16. Let $G_1, G_2, \ldots, G_n$ be groups and $G = G_1 \times G_2 \times \cdots \times G_n$.

(a) Prove that G is a group under componentwise group operations.

* **(b)** 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 $i \neq j$.