CS21001 Discrete Structures
Tutorial 11

[Unless otherwise stated, all groups in the exercise set are multiplicative with identity e.]

1. Let G be a group. Suppose that there exists some $n \in \mathbb{N}$ such that for all $a, b \in G$, we have $(ab)^n = a^n b^n$ and $(ab)^{n+1} = a^{n+1} b^{n+1}$. Prove that G is abelian.

2. Let G be a finite group of even order. Prove that the number of elements of order two in G is odd.

3. Let p be a prime. Prove that any group of order p^2 has a subgroup of order p.

4. Let G be a non-abelian group, and $a, b \in G$. Prove that $\mathrm{ord}(ab) = \mathrm{ord}(ba)$.

5. Let G be a finite group, and $h = \mathrm{ord}(a)$ for some $a \in G$. Prove that $\mathrm{ord}(a^k) = \dfrac{h}{\gcd(h,k)}$ for all $k \in \mathbb{Z}$.

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

7. Prove that any finite group of square-free order is cyclic.

8. Let G be a group, $a, b \in G$, $m = \mathrm{ord}(a)$, and $n = \mathrm{ord}(b)$. Assume that $m, n < \infty$.

(a) Prove or disprove: $\mathrm{ord}(ab) = mn$.
(b) Prove or disprove: If $\gcd(m,n) = 1$, then $\mathrm{ord}(ab) = mn$.
(c) Prove or disprove: If G is Abelian and $\gcd(m,n) = 1$, then $\mathrm{ord}(ab) = mn$.
(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.

9. Let G be a finite cyclic group, and H, K subgroups of G of orders s, t, respectively. What is the order of $H \cap K$?

10. Let G be a finite cyclic group of order m, and r a divisor of m. Prove that:

(a) G contains a unique subgroup H of order r.
(b) Let $a \in G$. Prove that $a \in H$ if and only if $a^r = e$. Demonstrate by an example that this result need not hold if G is not cyclic.

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

12. Let G be as in the last exercise. Prove/Disprove: $\mathrm{Tor}(G)$ must be finite.

13. 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 $2^{n-1} \pm 1$.)

14. Let p be an odd prime, and $e \in \mathbb{N}$. Prove that the group $\mathbb{Z}^*_{p^e}$ is cyclic. (**Hint:** For $e = 1$, the result follows from Fermat's little theorem. So suppose that $e \geqslant 2$. First show that the order of $p+1$ in $\mathbb{Z}^*_{p^e}$ is p^{e-1}. Then, take a generator a of $\mathbb{Z}^*_p$. The order of a in $\mathbb{Z}^*_{p^e}$ is $k(p-1)$ for some $k \in \mathbb{N}$.)

15. 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 $i \neq j$.

16. Prove that $\mathbb{Z}^*_n$ is cyclic if and only if $n = 1, 2, 4, p^e, 2p^e$, where $p \in \mathbb{P}$ and $e \in \mathbb{N}$.(**Hint:** Use the last three exercises, and the Chinese remainder theorem.)

17. 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.

18. Let G be a 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) $ab^{-1} \in H$.

19. Give an example of a group G, a subgroup H, and an element $a \in G$ such that $aH \neq Ha$.

20. Let G be a group, H a subgroup, and $a \in G$. Prove that:

(a) aHa^{-1} is a subgroup of G, and $|aHa^{-1}| = |H|$.
(b) Prove/Disprove: If aHa^{-1} is a normal subgroup of G, then so also is H.

21. Let H be a subgroup of a group G. For every $a, b \in G$, there exists $c \in G$ such that $(aH)(bH) = cH$. Prove that H is a normal subgroup of H.

22. Prove that the intersection of two normal subgroups of a group G is again normal subgroup of G.

23. Let G be a group, and H a subgroup of index $[G : H] = 2$. Prove that H is a normal subgroup of G.

24. Let H_1 and H_2 be two normal subgroups of G with $H_1 \cap H_2 = \{e\}$. Prove that for all $a_1 \in H_1$ and for all $a_2 \in H_2$, we have $a_1a_2 = a_2a_1$.

25. Prove/Disprove: If H is a normal subgroup of G, and K is a normal subgroup of H, then K is a normal subgroup of G.

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

27. Let G be a finite group. The smallest positive integer n such that $a^n = e$ for all $a \in G$ is called the *exponent* of G, denoted $\exp(G)$. Prove that:

(a) $\exp(G) = \operatorname{lcm}(\operatorname{ord}(a) \mid a \in G)$.
(b) $\exp(G) | \operatorname{ord}(G)$.
(c) If G is abelian, then there exists an element of G of order equal to $\exp(G)$.
(d) If G is abelian, and $\exp(G) = \operatorname{ord}(G)$, then G is cyclic.
(e) Parts (c) and (d) do not necessarily hold if G is not abelian.

28. Find the exponents of the symmetry groups S_3, S_4, and S_5.

29. Let I be a non-empty index set (not necessarily finite), and let a_i, $i \in I$, be symbols. Define G to be the set of all symbolic sums of the form $\sum\limits_{i \in I} n_i a_i$, where all $n_i \in \mathbb{Z}$, and only finitely many n_i are non-zero. Define addition on G as $\sum\limits_{i \in I} m_i a_i + \sum\limits_{i \in I} n_i a_i = \sum\limits_{i \in I} (m_i + n_i) a_i$. Prove that G is an abelian group under this addition. G is called the *free abelian group* generated by the symbols a_i, $i \in I$.

30. Let G be as in the last exercise. Denote by H the subset of all elements $\sum\limits_{i \in I} n_i a_i$ of G satisfying $\sum\limits_{i \in I} n_i = 0$. Prove that:

(a) H is a subgroup of G. (H is called the *degree-zero part* of G.)
(b) $G/H \cong \mathbb{Z}$.

31. Let G be a multiplicative group (not necessarily abelian), and $A \subseteq G$. Let $\langle A \rangle$ consist of all finite products of the form $b_1 b_2 \ldots b_t$ for some $t \in \mathbb{N}_0$ and with each $b_i \in A \cup A^{-1}$. Prove that $\langle A \rangle$ is a subgroup of G (called the subgroup of G generated by A).

32. If $G = \langle A \rangle$ for some finite subset A of G, then G is called *finitely generated*. Prove that:

(a) Every finitely generated group is countable.
(b) Every countable group need not be finitely generated.

33. Let $n = pq$, e, d be as in the RSA cryptosystem. Prove that the encryption map $m \mapsto m^e \pmod{n}$ is a bijection $\mathbb{Z}_n \to \mathbb{Z}_n$.

34. Let $n \in \mathbb{N}$ be a square-free modulus, and let $e \in \mathbb{N}$. Prove that the exponentiation map $m \mapsto m^e \pmod{n}$ is a bijection $\mathbb{Z}_n \to \mathbb{Z}_n$ if and only if $\gcd(e, \phi(n)) = 1$.

35. If $n \in \mathbb{N}$ is not square-free, prove that for no $e \in \mathbb{N}$, $e \geqslant 2$, the exponentiation map $m \mapsto m^e \pmod{n}$ is a bijection $\mathbb{Z}_n \to \mathbb{Z}_n$.