EXERCISES

2.10. If G is a finite group and $K \leq H \leq G$, then

$$[G:K] = [G:H][H:K].$$

2.11. Let $a \in G$ have order $n = mk$, where $m, k \geq 1$. Prove that a^k has order m.

2.12. (i) Prove that every group G of order 4 is isomorphic to either $\mathbb{Z}_4$ or the 4-group $\mathbf{V}$.
(ii) If G is a group with $|G| \leq 5$, then G is abelian.

2.13. If $a \in G$ has order n and k is an integer with $a^k = 1$, then n divides k. Indeed, $\{k \in \mathbb{Z}: a^k = 1\}$ consists of all the multiples of n.

2.14. If $a \in G$ has finite order and $f: G \to H$ is a homomorphism, then the order of $f(a)$ divides the order of a.

2.15. Prove that a group G of even order has an odd number of elements of order 2 (in particular, it has at least one such element). (*Hint.* If $a \in G$ does not have order 2, then $a \neq a^{-1}$.)

2.16. If $H \leq G$ has index 2, then $a^2 \in H$ for every $a \in G$.

2.17. (i) If $a, b \in G$ commute and if $a^m = 1 = b^n$, then $(ab)^k = 1$, where $k = \operatorname{lcm}\{m, n\}$. (The order of ab may be smaller than k; for example, take $b = a^{-1}$.) Conclude that if a and b have finite order, then ab also has finite order.
(ii) Let $G = \mathrm{GL}(2, \mathbb{Q})$ and let $A, B \in G$ be given by

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}.$$

Show that $A^4 = E = B^3$, but that AB has infinite order.

2.18. Prove that every subgroup of a cyclic group is cyclic. (*Hint.* Use the division algorithm.)

2.19. Prove that two cyclic groups are isomorphic if and only if they have the same order.

Definition. The ***Euler φ-function*** is defined as follows:

$$\varphi(1) = 1; \qquad \text{if } n > 1, \quad \text{then } \varphi(n) = |\{k: 1 \leq k < n \text{ and } (k, n) = 1\}|.$$

2.20. If $G = \langle a \rangle$ is cyclic of order n, then a^k is also a generator of G if and only if $(k, n) = 1$. Conclude that the number of generators of G is $\varphi(n)$.

2.21. (i) Let $G = \langle a \rangle$ have order rs, where $(r, s) = 1$. Show that there are unique $b, c \in G$ with b of order r, c of order s, and $a = bc$.
(ii) Use part (i) to prove that if $(r, s) = 1$, then $\varphi(rs) = \varphi(r)\varphi(s)$.

2.22. (i) If p is prime, then $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.
(ii) If the distinct prime divisors of n are $p_1, \ldots, p_t$, then

$$\varphi(n) = n(1 - 1/p_1)\ldots(1 - 1/p_t).$$

2.23 **(Euler).** If $(r, s) = 1$, then $s^{\varphi(r)} \equiv 1 \bmod r$. (*Hint.* The order of the group of units $U(\mathbb{Z}_n)$ is $\varphi(n)$.)