General Examination: Algebra

Solve at least three items from each problem.
(Items are labeled by (a), (b), (c) and (d).)

Problem 1.

(a) Let a be an arbitrary real number such that $a \neq 1, a \neq -1$. Put $C(a) = \{a^n \mid n \in \mathbb{Z}\} \subset \mathbb{R}$.

- Prove that $C(a)$ is an infinite cyclic group with respect to multiplication of real numbers.
- Let $\mathbb{R}^+$ be the group of reals with respect to addition. On the set $G = C(a) \times \mathbb{R}^+$ define a binary operation $\circ$ by

$$(a^m, r) \circ (a^n, s) = (a^{m+n}, ra^n + s).$$

Show that G is a group under this operation.

(b) Let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ and $U(n)$ the group of units of $\mathbb{Z}_n$.

- List all elements of $U(9)$.
- Show that $U(9)$ is a cyclic subgroup of order 6.

(c) Find an element of largest possible order in the group of permutations S_{12}.

(d) Denote by D_n the nth dihedral group (the group of rigid motions of a regular n-gon). Find the center of the group D_7. (Recall that the center $Z(G)$ of a group G consists of all elements $g \in G$ such that $gx = xg$ for any element $x \in G$.)

Problem 2.

(a) Prove that A_4 has no subgroups of order 6.

(b) Prove that for relatively prime integers m and n the group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$.

(c) Let J be an ideal in a ring R. Prove that

$$Ann_r(J) = \{x \in R \mid tx = 0 \ for\ every\ t \in J\}$$

is also an ideal in R.

(d) Show (using Fermat's Little Theorem) that if $p = 4n+3$ is prime then there is no solution to the equation $x^2 + 1 = 0(mod\ p)$.

Problem 3.

(a) Let $F = \mathbb{Z}_3[x]/(x^3 + x^2 + 2)$. Show that F is a field and find $(x^2 + x + 1)^{-1}$ in F.

(b) Show that $\alpha = \sqrt[2]{2 + \sqrt[2]{3}}$ is algebraic over $\mathbb{Q}$ and find its minimal plynomial.

(c) Find the Galois group of the polynomial $x^4 + 2x^2 - 8$ in $\mathbb{Q}[x]$.

(d) Let $GF(p^n)$ be the finite field of p^n elements. Prove that the Frobenius map $GF(p^n) \to GF(p^n)$ defined by $x \to x^p$ is an automorphism of $GF(p^n)$ of order n.