Master's Comprehensive Exam—Algebra—August 1997

Notation. Let $|G|$ denote the order of the group G. If η is a homomorphism and $k \geqslant 1$, η^k means the composition $\eta \circ \cdots \circ \eta$ of k copies of η. If R is a ring, R^k means the direct sum $R \oplus \cdots \oplus R$ of k copies of R.

1. Let G be a group. Let H and K be normal subgroups of G, with $H \cap K = \{1\}$.

(a) Prove that every element of H commutes with every element of K. Hint: for all $h \in H$ and $k \in K$, prove that $hkh^{-1}k^{-1} = 1$.

(b) Prove that the map $H \times K \to G$ given by $(h, k) \mapsto hk$ is a homomorphism.

(c) Assume in addition that the groups are finite, and that $|G| = |H| \cdot |K|$. Prove that $H \times K \cong G$.

(d) The map in (b) can fail to be a homomorphism if one or both of H, K is **not** normal. Let $G = S_3$. Give examples of subgroups H, K of S_3, at least one of which is not normal, and specific elements (h_1, k_1) and $(h_2, k_2) \in H \times K$, which illustrate why the map can fail to be a homomorphism.

2. Let G be a group. Let H be a subgroup of G of index n. Prove that there is a normal subgroup N in G, with $N \subseteq H$, such that the index $[G : N]$ is a divisor of $n!$. Hint: consider the action of G on the coset space G/H.

3. Let R be a ring with identity element 1. Let I and J be ideals of R.

(a) Define the ideal $I + J$.

(b) In the ring $\mathbb{Z}$, what is $(10) + (16)$? Proof is not required, but explain briefly.

(c) Prove the following version of the Chinese Remainder Theorem. Assume I and J are relatively prime, meaning $I + J = (1)$. Let a and b be any two elements of R. Prove that there is an $x \in R$ such that $x \equiv a \pmod{I}$ and $x \equiv b \pmod{J}$.

4. Consider the free $\mathbb{Z}$-module $\mathbb{Z}^3$. Let K be the submodule generated by the 3-tuples $(2, 4, 5)$ and $(6, -4, 3)$. Let $M = \mathbb{Z}^3/K$.

(a) Express M up to isomorphism as a direct sum of cyclic $\mathbb{Z}$-modules.

(b) What is the torsion submodule of M?

(c) Does M have a submodule isomorphic to $\mathbb{Z}/(4)$? Explain.

(d) Does M have a submodule M' such that M/M' is isomorphic to $\mathbb{Z}/(3)$? Explain.

5. (a) Let n be a positive integer. Let F be a field of characteristic zero containing a primitive n-th root of unity ζ. Let $a \in F$, and let E be the splitting field of $x^n - a$ over F. Prove that the Galois group of E/F is cyclic, and that its order is a divisor of n.

(b) Give an example where the order of the Galois group is strictly between 1 and n.

6. In this problem, $\zeta = \zeta_5$ is a primitive fifth root of unity over $\mathbb{Q}$. Let $E = \mathbb{Q}(\zeta)$.

(a) Describe the Galois group G of $E/\mathbb{Q}$. What is its order? Is it cyclic? (No proof required on part (a).)

(b) Choose a generator η of G. For the η you have chosen, make a table showing ζ^i and $\eta(\zeta^i)$ for $i = 1, 2, 3, 4$.

(c) Find an expression in ζ which is invariant under η^2 but not invariant under η. Call this expression u.

(d) Let H be the subgroup of G generated by η^2. According to the Galois correspondence, there is a subfield $K = \operatorname{Inv} H \subset E$ consisting of the elements of E which are invariant under H. Prove that $K = \mathbb{Q}(u)$, showing both the $(\supseteq)$ and $(\subseteq)$ directions.

(e) Find the minimal polynomial of u over $\mathbb{Q}$.

(f) Prove that $K = \mathbb{Q}(\sqrt{5})$.

(g) Make a table showing all the subgroups of G, including G itself and $\{1\}$. List the subfield of E that corresponds to each subgroup under the Galois correspondence.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX