Proposed algebra questions

1. Let G be a group. A proper subgroup H of G is called *maximal* if every subgroup of G containing H is equal to either H or G. Prove that a normal and maximal subgroup of G must have finite index p, where p is a prime number.

   Solution: Let H be a normal and maximal subgroup of G. By the fourth (or lattice) isomorphism theorem, the maximality of H implies that the only subgroups of $\overline{G} = G/H$ are $\{1\}$ and $\overline{G}$. Since H is a proper subgroup of G, $\overline{G} \neq \{1\}$. Let $x \in \overline{G}$ be any non-identity element. Then we must have $\langle x \rangle = \overline{G}$, and thus $\overline{G}$ is cyclic. If $\overline{G} \cong \mathbf{Z}$ then there are clearly non-identity subgroups of $\overline{G}$. So $\overline{G} \cong \mathbf{Z}/n\mathbf{Z}$ for some integer $n \geq 2$. As the subgroups of $\mathbf{Z}/n\mathbf{Z}$ correspond bijectively to divisors of n, it follows that $n = p$ is prime. So $[G : H] = |G/H| = p$ as desired.

2. Let p be a prime number. Determine all possibilities for the number of conjugacy classes in a group G of order p^3.

   Solution: Let Z be the center of G. The class equation for G reads

$$|G| = |Z| + \sum_{i=1}^{m} [G : C_G(x_i)],$$

   where $x_1, \ldots, x_m$ are representatives for the distinct non-trivial conjugacy classes of G, $[G : C_G(x_i)]$ is the number of elements in the conjugacy class of x_i, and $C_G(x_i)$ is the centralizer of x_i. Since G is a p-group, Z is a non-trivial subgroup of G. If $p^2 \mid |Z|$ then $|G/Z| \mid p$ and thus G/Z is cyclic. This implies that G is abelian, in which case G has exactly p^3 conjugacy classes. Otherwise G is non-abelian and we must have $|Z| = p$. In this case, the class equation is

$$p^3 = p + \sum_{i=1}^{m} [G : C_G(x_i)]$$

Since $\langle x_i, Z\rangle \leq C_G(x_i)$ and $x_i \notin Z$, we must have $|C_G(x_i)| = p^2$ for each i. Therefore $p^3 = p + mp$ so $m = p^2 - 1$, and thus there are $p^2 + p - 1$ conjugacy classes in this case. As there exist both abelian and non-abelian groups of order p^3, both types of class equations are realized and thus the possibilities for the number of conjugacy classes in G are p^3 and p^2+p-1.

3. Let R be a commutative ring with identity $1 \neq 0$.

   a. If R is a finite integral domain, prove that R is a field.

   b. Suppose $P \subset R$ is a prime ideal, and that there are elements $a_1, \ldots, a_n \in R$ such that for each $a \in R$, there exists $i \in \{1, \ldots n\}$ with $a - a_i \in P$. Prove that P is a maximal ideal.

   Solution: a. Fix $x \in R$ with $x \neq 0$, and consider the map $m_x : R \to R$ given by $m_x(r) = rx$. This map is injective, since $rx = sx$ implies $r = s$ in an integral domain. As R is finite, the injective map m_x is also surjective. Thus there exists $r \in R$ with $rx = 1$, which implies that x has a multiplicative inverse. As x was an arbitrary nonzero element, this implies that R is a field.

   b. By hypothesis, the image of every element of R in R/P under the natural homomorphism is equal to the image of some a_i. Thus R/P has finitely many elements. Since P is a prime ideal, R/P is an integral domain. By part (a), R/P is a field, which implies that P is a maximal ideal.

4. Let p be a prime number, and let $\mathbf{F}_p$ be the field with p elements. How many elements of $\mathbf{F}_p$ have cube roots in $\mathbf{F}_p$?

   Solution: Since $\mathbf{F}_p^*$ is abelian, the map $\phi : \mathbf{F}_p^* \to \mathbf{F}_p^*$ given by $\phi(x) = x^3$ is a group homomorphism. Since every element of the kernel of ϕ has order dividing 3, if $3 \nmid p-1$ then ϕ is injective and hence surjective. Thus every element of $\mathbf{F}_p$ has a cube root if $p \not\equiv 1 \pmod 3$. If $3 \mid p - 1$, then the cyclic group $\mathbf{F}_p^*$ has a unique subgroup of order 3, and thus $\mathrm{Ker}(\phi)$ has order 3. By the first isomorphism theorem, $\mathbf{F}_p^*/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi)$, so $\mathrm{Im}(\phi)$ has $(p-1)/3$ elements. It follows that if $p \equiv 1 \pmod 3$, then (counting zero) there are $1 + (p-1)/3 = (p+2)/3$ elements of $\mathbf{F}_p$ with cube roots in $\mathbf{F}_p$. In summary, the answer to the question is $(p+2)/3$ if $p \equiv 1 \pmod 3$, and p if $p \not\equiv 1 \pmod 3$.

5. Let p be an odd prime, let $\mathbf{F}$ be a finite field of order p^2, and let $\mathbf{F}_p$ denote the prime subfield of $\mathbf{F}$.

a. Show that there exists $\omega \in \mathbf{F}$ such that $\omega^2 \in \mathbf{F}_p$ but $\omega \notin \mathbf{F}_p$.

b. With ω as in part (a), show that $(x + y\omega)^p = x - y\omega$ for all $x, y \in \mathbf{F}_p$.

Solution: a. Let g be a generator of the cyclic group $\mathbf{F}_p^*$ of order $p - 1$. Then there does not exist an element $x \in \mathbf{F}_p^*$ such that $x^2 = g$, for otherwise writing $x = g^k$ we would have $g^{2k} = g$ and thus $g^{2k-1} = 1$, which is impossible since g has even order. Since $\mathbf{F}$ is the unique quadratic extension of $\mathbf{F}_p$, g has a square root ω in $\mathbf{F}$, which by the preceding discussion cannot lie in $\mathbf{F}_p$.

b. By the binomial theorem and Fermat's little theorem, $(x + y\omega)^p = x^p + y^p\omega^p = x + y\omega^p$, so it suffices to show that $\omega^p = -\omega$, or equivalently, that $\omega^{p-1} = -1$. Since $\omega^2 \in \mathbf{F}_p^*$, we have $(\omega^{p-1})^2 = (\omega^2)^{p-1} = 1$. Since a polynomial of degree $d \geq 1$ over $\mathbf{F}$ can have at most d roots in $\mathbf{F}$, and since $1^2 = (-1)^2 = 1$ in $\mathbf{F}$, it follows that $\omega^{p-1} \in \{\pm 1\}$. But an element $\alpha \in \mathbf{F}$ is in $\mathbf{F}_p$ if and only if $\alpha^p = \alpha$. It follows that $\omega^{p-1} \neq 1$ and thus $\omega^{p-1} = -1$ as desired.

6. Let A be a square matrix with real entries such that $A^2 = -I$, where I denotes the identity matrix. Prove $\det(A) = 1$.

   Solution: Let λ be an arbitrary eigenvalue of A. Then λ^2 is an eigenvalue of A^2, and hence, of $-I$. Therefore, $\lambda^2 = -1$. This implies that no eigenvalue of A is real, which means that eigenvalues of A come in conjugate pairs. Hence, $\det(A) > 0$ and $\det(A^2) = 1$ (because I must have even number of rows). So $\det(A) = 1$.

7. Let V be the set consisting of all convergent sequences of real numbers. Then V is a vector space under the following operations: for any $\{x_n\}, \{y_n\} \in V$ and for any real number c, $\{x_n\} + \{y_n\} = \{x_n + y_n\}$ and $c\{x_n\} = \{cx_n\}$. Let $T : V \to V$ be the linear transformation defined as $T(\{x_n\}) = \{(\lim_{n\to\infty} x_n) - x_n\}$. Find all eigenvalues of T and describe their eigenvectors.

   Solution: Let λ be an eigenvalue of T. Then there exists a nonzero sequence $\{x_n\}$ such that $T(\{x_n\}) = \lambda\{x_n\}$. Hence, we have $\lambda x_n = (\lim x_n) - x_n$ for all n. This implies that $(\lambda + 1)x_n = \lim x_n$. Hence, either $\lambda = -1$ and $\lim x_n = 0$, or $\lambda = 0$ and $\{x_n\}$ is a constant sequence. Therefore, T has two distinct eigenvalues -1 and 0. The eigenvectors of -1 are the nonzero sequences which converge to 0, and the eigenvectors of 0 are the nonzero constant sequences.