ALGEBRA II

We use the following standard notation: $\mathbb{Z}$ is the ring of integers, $\mathbb{Q}$ is the field of rational numbers, $\mathbb{R}$ is the field of real numbers, $\mathbb{C}$ is the field of complex numbers, and $\mathbb{F}_q$ is the finite field with q elements (where $q = p^e$ for some prime p and $e \geq 1$).

(1) Let K be a subfield of $\mathbb{C}$ such that K is a Galois extension of $\mathbb{Q}$ with $[K : \mathbb{Q}]$ odd. Show that $K \subset \mathbb{R}$.

Solution: Let σ be complex conjugation. Then $\sigma^2 = \mathrm{Id}$, so σ must map to an element of $\mathrm{Gal}(K/\mathbb{Q})$ whose square is the identity. But, since $|\mathrm{Gal}(K/\mathbb{Q})|$ is odd, the only such element is the identity. So σ acts trivially on K, and we deduce that $K \subset \mathbb{R}$.

(2) Let p be an odd prime number. Form the semidirect product $G = \mathbb{F}_p \rtimes \mathbb{F}_p^*$ for the standard (scalar multiplication) action of $\mathbb{F}_p^*$ on $\mathbb{F}_p$. Let ℓ be a prime. Calculate the cardinality of the set of all group homomorphisms G to the cyclic group $\mathbb{Z}/\ell\mathbb{Z}$ in the following cases:

(a) ℓ is a prime number different from p.

(b) $\ell = p$.

Solution:

(a) We first consider the case that $\ell \neq p$. In this case, $\mathrm{Hom}(\mathbb{F}_p, \mathbb{Z}/\ell\mathbb{Z}) = 0$, so any homomorphism $G \to \mathbb{Z}/\ell\mathbb{Z}$ must vanish on the normal subgroup $\mathbb{F}_p$, and hence must factor through the quotient $\mathbb{F}_p^\times$. We have shown that $\mathrm{Hom}(G, \mathbb{Z}/\ell\mathbb{Z}) \cong \mathrm{Hom}(\mathbb{F}_p^\times, \mathbb{Z}/\ell\mathbb{Z})$. Now, $\mathbb{F}_p^\times$ is the cyclic group of order $p-1$, so $\mathrm{Hom}(\mathbb{F}_p^\times, \mathbb{Z}/\ell\mathbb{Z})$ is $\mathbb{Z}/\ell\mathbb{Z}$ if ℓ divides $p-1$, and trivial if ℓ does not divide $p-1$.

(b) Now, we consider $\mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$. We will show that this is trivial (using that p is odd).

Since $\mathbb{Z}/p\mathbb{Z}$ is abelian, any homomorphism from G to $\mathbb{Z}/p\mathbb{Z}$ must vanish on the commutator subgroup of G. The commutator of $(a, -1)$ and $(0, -1) \in \mathbb{F}_p \rtimes \mathbb{F}_p^*$ is $(2a, 1)$ so, if $p > 2$, every element of $\mathbb{F}_p \rtimes \{1\}$ is a commutator. Thus, any homomorphism from G to $\mathbb{Z}/p\mathbb{Z}$ must factor through the quotient $\mathbb{F}_p^\times$. But the orders of $\mathbb{F}_p^\times$ and $\mathbb{Z}/p\mathbb{Z}$ are relatively

Date: Aug 2021.

prime, so we deduce that $\mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$ is trivial. (The problem didn't ask for this but: If $p = 2$, then $G \cong \mathbb{Z}/2\mathbb{Z}$, so $\mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z})$ has two elements.)

(3) Let p be a prime number, and let $k = \mathbb{F}_p(x)$. For $f(x) \in k$, let $K_f = k[y]/(y^p - f(x))$. Show that the ring K_f is a field exactly when $f(x)$ is not a p-th power.

Solution: We know that $k[y]/g(y)k[y]$ is a field if and only if $g(y)$ is irreducible in the polynomial ring $k[y]$. If $f(x) = h(x)^p$ then $y^p - f(x) = (y - h(x))^p$ and is hence not irreducible. We will now show that, on the other hand, if $y^p - f(x)$ is reducible, then $f(x)$ is a p-th power. Indeed, in the algebraic closure of k, the polynomial $y^p - f$ factors as $(y - f^{1/p})^p$. So any nontrivial factor of $y^p - f$ in $k[y]$ would have to be of the form $(y - f^{1/p})^a$ for $1 \leq a \leq p - 1$. But then examining the coefficient of y^{a-1}, we see that $-af^{1/p}$ is in k, so $f^{1/p}$ is in k, as desired.

(4) Fix a prime number p. Describe a p-Sylow subgroup in each of the following groups:

(a) $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$

(b) $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$

Here we use the following notation: for any ring R, the group $\mathrm{GL}_2(R)$ is the group (2×2) invertible matrices over R (with group operation being matrix multiplication).

Solution:

(a) As is well known, $|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = (p^2 - 1)(p^2 - p)$, so it is divisible by p and not p^2. Thus, a p-Sylow subgroup is any subgroup of size p, such as the group of matrices of the form $\left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right]$.

(b) We first compute the order of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. We have a short exact sequence $1 \to \Gamma \to \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \to 1$, where Γ is matrices in $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ whose reduction modulo p is the identity matrix. Note that any element in $\mathbb{Z}/p^2\mathbb{Z}$ which is $1 \bmod p$ is a unit, so any matrix with entries in $\mathbb{Z}/p^2\mathbb{Z}$ which is $\mathrm{Id} \bmod p$ is invertible, so Γ is simply all matrices with entries in $\mathbb{Z}/p^2\mathbb{Z}$ which are $\mathrm{Id} \bmod p$. There are p^4 of these, so $|\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})| = p^4(p^2 - 1)(p^2 - p)$, and a p-Sylow subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ is a group with p^5 elements. The easiest example is to take a preimage, in $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ of a Sylow subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Concretely, we get the group of matrices with entries in $\mathbb{Z}/p^2\mathbb{Z}$ of the form $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with $a \equiv d \equiv 1 \bmod p$ and $c \equiv 0 \bmod p$.

(5) Let L/K be an algebraic extension of fields of characteristic 0. Assume that for every $\alpha \in L$, the extension $K(\alpha)/K$ has degree ≤ 2. Show that $[L : K] \leq 2$.

Solution: Indeed, suppose for the sake of contradiction that $[L : K] > 2$. Then we can find α in L but not in K, so $[K(\alpha) : K] = 2$, and we can then find β in L but not in $K(\alpha)$, so $[K(\alpha, \beta) : K] > 2$. But then, using the primitive element theorem, we can find γ in $K(\alpha, \beta)$ such that $K(\gamma) = K(\alpha, \beta)$, contradicting that we are supposed to have $[K(\gamma) : K] \leq 2$ for all γ in L.