Solutions to Algebra 2 QR (May 2023)

Problem 1. Let G be a finite group of order N and let X and Y be two sets on which G acts transitively. Suppose that $\mathrm{GCD}(|X|,\ |Y|) = 1$. Let G act on $X \times Y$ by $g \cdot (x, y) = (g \cdot x, g \cdot y)$. Show that the action of G on $X \times Y$ is transitive.

Solution. Let $Z \subset X \times Y$ be the orbit of some element. From the projection map $p\colon Z \to X$, we see that $|X|$ divides $|Z|$. (Precisely, suppose $z \in Z$ has stabilizer G_z. Since Z is transitive, we have $Z \cong G/G_z$. Let $x = p(z)$. Since p is G-equivariant, we have $G_z \subset G_x$. Since X is transitive, we have $X \cong G/G_x$. Thus $|Z|/|X| = |G_x|/|G_z|$, which is an integer by Lagrange's theorem.) Similarly, $|Y|$ divides $|Z|$. Since $|X|$ and $|Y|$ are coprime, it follows that $|X| \cdot |Y|$ divides $|Z|$, and so $Z = X \times Y$. Thus $X \times Y$ carries a transitive action.

Problem 2. Let G be a finite group with $|G| \equiv 2 \bmod 4$. Let s and t be two nonidentity elements of G with $s^2 = t^2 = 1$. Show that s and t are conjugate within G.

Solution. Since 2 divides $|G|$ but 4 does not, it follows that a 2-Sylow subgroup of G has order 2. Thus $\{1, s\}$ and $\{1, t\}$ are 2-Sylow subgroups. By the second Sylow theorem, they are conjugate, i.e., there is $g \in G$ such that $\{1, s\} = g\{1, t\}g^{-1}$. Since gtg^{-1} is not the identity, it must be s, and so s and t are conjugate.

Problem 3. Let K be the field of rational functions $\mathbb{C}(x_0, x_1, x_2, x_3, x_4)$. Let F be the subfield of K consisting of functions symmetric under the permutations $(x_0, x_1, x_2, x_3x_4) \mapsto (x_1, x_2, x_3, x_4, x_0)$ and $(x_0, x_1, x_2, x_3, x_4) \mapsto (x_0, x_4, x_3, x_2, x_1)$. How many fields L are there with $F \subseteq L \subseteq K$? (Prove your answer to be correct.)

Solution. Let σ be the automorphism of K that fixes $\mathbb{C}$ and acts on the variables by $\sigma(x_i) = x_{i+1}$ (with indices in $\mathbb{Z}/5$). Let τ be the automorphism that fixes $\mathbb{C}$ and acts on the variables by $\tau(x_i) = x_{-i}$. The group $G \subset \mathrm{Aut}(K)$ generated by σ and τ is isomorphic to the dihedral group D_5 of order 10. As F is the fixed field of G, we see that K/F is a Galois extension with group D_5. Hence, the number of intermediate fields is the number of subgroups of D_5. There is one subgroup of order one, five of order two, one of order five, and one of order ten. Thus D_5 has 8 subgroups, and so there are 8 intermediate fields.

Problem 4. Let K be a field, let $f(x)$ be a separable polynomial of degree $n \geq 3$ with coefficients in K and let L be a splitting field for $f(x)$ over K, in which $f(x)$ factors as $(x - \theta_1)(x - \theta_2) \cdots (x - \theta_n)$. Suppose that $\mathrm{Gal}(L/K)$ is the alternating group A_n. Show that θ_n lies in the field $K(\theta_1, \theta_2, \ldots, \theta_{n-2})$, but that θ_n does not lie in $K(\theta_1, \theta_2, \ldots, \theta_{n-3})$.

Solution. The Galois group of $L/K(\theta_1, \ldots, \theta_{n-2})$ consists of those permutations in A_n that fix $1, \ldots, n-2$. The only such permutation is the identity, and so the Galois group is trivial. By Galois theory, $K(\theta_1, \ldots, \theta_{n-2}) = L$, and thus contains θ_n.

The 3-cycle $(n-2\ \ n-1\ \ n)$ is an element of $\mathrm{Gal}(L/K)$ that fixes the field $K(\theta_1, \ldots, \theta_{n-3})$. Since it does not fix θ_n, it follows that θ_n does not belong to this field.

Problem 5. Let $p \geq 5$ be prime. We consider the following four subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ where, in each case, x ranges over $\mathbb{F}_p^\times$ and y ranges over $\mathbb{F}_p$:

$$G_{1,2} = \{\left[\begin{smallmatrix} x & y \\ 0 & x^2 \end{smallmatrix}\right]\} \quad G_{1,3} = \{\left[\begin{smallmatrix} x & y \\ 0 & x^3 \end{smallmatrix}\right]\} \quad G_{2,3} = \{\left[\begin{smallmatrix} x^2 & y \\ 0 & x^3 \end{smallmatrix}\right]\} \quad G_{2,1} = \{\left[\begin{smallmatrix} x^2 & y \\ 0 & x \end{smallmatrix}\right]\}.$$

Which of these groups are isomorphic to each other? When you claim that groups are isomorphic, prove them to be so; when you claim that groups are not isomorphic, prove them not to be so.

Solution. For coprime integers n and m, put

$$G_{n,m} = \left[\begin{smallmatrix} x^n & y \\ 0 & x^m \end{smallmatrix}\right] \qquad T_{n,m} = \left[\begin{smallmatrix} x^n & 0 \\ 0 & x^m \end{smallmatrix}\right] \qquad U_{n,m} = \left[\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right],$$

where x varies over $\mathbb{F}_p^\times$ and y varies over $\mathbb{F}_p$. Both $T_{n,m}$ and $U_{n,m}$ are subgroups of $G_{n,m}$, with $U_{n,m}$ normal. Moreover, $G_{n,m} = T_{n,m}U_{n,m}$ and $T_{n,m} \cap U_{n,m} = 1$. Thus $G_{n,m}$ is the semi-direct product $T_{n,m} \ltimes U_{n,m}$.

Now, the map

$$\mathbb{F}_p^\times \to T_{n,m} \qquad x \mapsto \left[\begin{smallmatrix} x^n & 0 \\ 0 & x^m \end{smallmatrix}\right]$$

is an isomorphism; indeed, it is surjective by definition, and has trivial kernel since n and m are coprime. Of course, the map

$$\mathbb{F}_p \to U_{n,m} \qquad y \mapsto \left[\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right]$$

is also an isomorphism. We have

$$\left[\begin{smallmatrix} x^n & 0 \\ 0 & x^m \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} x^n & 0 \\ 0 & x^m \end{smallmatrix}\right]^{-1} = \left[\begin{smallmatrix} 1 & x^{n-m}y \\ 0 & 1 \end{smallmatrix}\right].$$

We thus see that $G_{n,m}$ is isomorphic to the semi-direct product $\mathbb{F}_p^\times \ltimes_{n-m} \mathbb{F}_p$, where the subscript indicates that $\mathbb{F}_p^\times$ acts on $\mathbb{F}_p$ by $x \bullet y = x^{n-m}y$.

In particular, the isomorphism class of $G_{n,m}$ only depends on $n - m$. Thus $G_{1,2}$ and $G_{2,3}$ are isomorphic.

Now, the matrix

$$\left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$$

belongs to $G_{1,3}$, and is central of order two. In terms of the semi-direct product computation, this corresponds to the fact that $-1 \in T_{1,3}$ acts trivially on $U_{1,3}$, since $(-1)^{3-1} = 1$. One easily sees that the other $G_{n,m}$'s have trivial center, and so $G_{1,3}$ is not isomorphic to them. (Here's how to see trivial center. Suppose x were a central element of $G_{n,m}$. Then x would conjugate $U_{n,m}$ trivially. This conjugation action only depends on the image of x in $T_{n,m} = G_{n,m}/U_{n,m}$. For the relevant (n,m)'s other than $(1,3)$, the action of $T_{n,m}$ on $U_{n,m}$ is faithful, by the above computation. Thus we see that x maps to 1 in $T_{n,m}$, meaning $x \in U_{n,m}$. But non-identity elements of $U_{n,m}$ are clearly not central since $T_{n,m}$ acts non-trivially on them.)

Finally we must decide if $G_{1,2}$ and $G_{2,1}$ are isomorphic. They are. This follows from the semi-direct product description: the map

$$\mathbb{F}_p^\times \ltimes_{1-2} \mathbb{F}_p \to \mathbb{F}_p^\times \ltimes_{2-1} \mathbb{F}_p, \qquad (x, y) \mapsto (x^{-1}, y)$$

is an isomorphism. In terms of matrices, this is the isomorphism

$$G_{1,2} \to G_{2,1} \qquad \left[\begin{smallmatrix} x & y \\ 0 & x^2 \end{smallmatrix}\right] \mapsto \left[\begin{smallmatrix} x^{-2} & x^{-3}y \\ 0 & x^{-1} \end{smallmatrix}\right].$$

Note that (x, y) in the semi-direct product description of $G_{n,m}$ corresponds to the matrix

$$\left[\begin{smallmatrix} x^n & 0 \\ 0 & x^m \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} x^n & x^n y \\ 0 & x^m \end{smallmatrix}\right].$$