Algebra II QR — January 2025

Problem 1. Let G be a finite group of order mn, where m and n are relatively prime integers, and assume that there exists a subgroup $M \subset G$ of order m and a subgroup $N \subset G$ of order n. Prove that G is isomorphic to a subgroup of the symmetric group S_{m+n} on $m+n$ elements.

Solution. The action of G on the set G/M of left cosets defines a homomorphism $\phi\colon G \to S_n$, since $n = |G/M|$, and the kernel satisfies $\ker(\phi) \subset M$. Similarly, the action of G on G/N defines a homomorphism $\psi\colon G \to S_m$ with $\ker(\psi) \subset N$. Consider the homomorphism $f = (\phi, \psi)\colon G \to S_n \times S_m$. Its kernel $\ker(f) = \ker(\phi) \cap \ker(\psi)$ is contained in $M \cap N$, but this group is trivial since its order divides the relatively prime numbers m and n. Thus f is injective. Composing with the natural injective homomorphism $S_n \times S_m \hookrightarrow S_{n+m}$ (sending (σ, τ) to the permutation of $n+m$ elements given by σ on the first n and τ on the last m), we obtain an injective homomorphism $G \to S_{n+m}$.

Problem 2. Let D_8 be the dihedral group of order 8, i.e. the group of symmetries of a square. Prove that there is an isomorphism $\mathrm{Aut}(D_8) \cong D_8$, where $\mathrm{Aut}(D_8)$ is the group of automorphisms of D_8.

Hint: It may be useful to consider an embedding $D_8 \hookrightarrow D_{16}$.

Solution. First we claim $|\mathrm{Aut}(D_8)| \leq 8$. To see this, let r and s denote the standard "rotation" and "reflection" generators of D_8. Then any $f \in \mathrm{Aut}(D_8)$ is determined by $f(r)$ and $f(s)$. Moreover, $f(r)$ must have order 4, and hence is contained in $\{r, r^3\}$. Similarly, $f(s)$ must have order 2, and hence is contained in $\{r^4, s, sr, sr^2, sr^3\}$; but $f(s) = r^4$ is not possible, since otherwise f would not be surjective. This means there are at most $2 \cdot 4 = 8$ possible elements $f \in \mathrm{Aut}(D_8)$.

Now consider a square embedded in an octagon so that its four vertices are alternating vertices of the octagon. This determines an embedding $D_8 \hookrightarrow D_{16}$, which sends $r \mapsto r^2$ and $s \mapsto s$ (where we use r and s to also denote the standard generators of D_{16}). The image is normal, as it has index 2. Thus conjugation determines an action of D_{16} on D_8. Let $\phi\colon D_{16} \to \mathrm{Aut}(D_8)$ be the corresponding homomorphism. The kernel is given by $\ker(\phi) = \{g \in D_{16} \mid gr^2 = r^2 g, gs = sg\}$. Using the presentation of a dihedral group in terms of generators and relations, $D_{16} = \langle r, s \mid r^8 = s^2 = 1, rs = sr^{-1}\rangle$, it is straightforward to compute that $\ker(\phi) = \{1, r^4\}$. Altogether, this gives an injection $D_{16}/\langle r^4\rangle \hookrightarrow \mathrm{Aut}(D_8)$, which must be an isomorphism since the source has size 8 and as shown above the target has size at most 8. It remains to note that there is an isomorphism $D_{16}/\langle r^4\rangle \cong D_8$, as is clear from the presentation in terms of generators and relations.

Problem 3. Let p be a prime. Compute the number of Sylow p-subgroups of $\mathrm{GL}_2(\mathbf{F}_p)$.

Solution. By Sylow's theorem, the number of Sylow p-subgroups is given by the index in $\mathrm{GL}_2(\mathbf{F}_p)$ of the normalizer N of any given Sylow p-subgroup P. The order of $\mathrm{GL}_2(\mathbf{F}_p)$

is

$$|\mathrm{GL}_2(\mathbf{F}_p)| = (p^2-1)(p^2-p) = p(p^2-1)(p-1)$$

because for an element $A \in \mathrm{GL}_2(\mathbf{F}_p)$, the first column can be any nonzero element of $\mathbf{F}_p^2$, and the second column can be any element of $\mathbf{F}_p^2$ not in the span of the first column. Thus a Sylow p-subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$ is a subgroup of order p. An example of such is the subgroup $P \subset \mathrm{GL}_2(\mathbf{F}_p)$ of upper triangular matrices with all diagonal entries equal to 1.

For the above P, a direct computation shows that the normalizer N consists of all upper triangular matrices in $\mathrm{GL}_2(\mathbf{F}_p)$. Thus we have $|N| = (p-1)(p^2-p)$, since the first column of any $A \in N$ can be any nonzero element of $\mathbf{F}_p^2$ of the form $(a, 0)$ and the second column can be any element of $\mathbf{F}_p^2$ not in the span of the first column. Thus the number of Sylow p-subgroups is given by

$$\frac{|\mathrm{GL}_2(\mathbf{F}_p)|}{|N|} = \frac{(p^2-1)(p^2-p)}{(p-1)(p^2-p)} = p+1.$$

Problem 4. Let $F/\mathbf{Q}$ be a field extension such that F is contained in the ring $M_n(\mathbf{Q})$ of $n \times n$ matrices over $\mathbf{Q}$ (i.e. there is an injective ring homomorphism $F \to M_n(\mathbf{Q})$). Prove that the degree of the extension $F/\mathbf{Q}$ satisfies $[F : \mathbf{Q}] \leq n$.

Solution. The extension $F/\mathbf{Q}$ is finite since it is contained in $M_n(\mathbf{Q})$ and separable since $\mathbf{Q}$ has characteristic 0. Hence $F = \mathbf{Q}(\alpha)$ for some element α by the primitive element theorem. From linear algebra (the Cayley-Hamilton theorem), the image A of α in $M_n(\mathbf{Q})$ must satisfy $p(A) = 0$, where $p(x) = \det(xI - A)$ is the degree n characteristic polynomial of A. Hence α also satisfies $p(\alpha) = 0$ and $[\mathbf{Q}(\alpha) : \mathbf{Q}] \leq n$.

Alternate solution: Note that the inclusion $F \hookrightarrow M_n(\mathbf{Q})$ makes $\mathbf{Q}^n$ into an F-vector space. Then the result follows by taking dimensions of vector spaces.

Problem 5. Let p be a prime, let $a \in \mathbf{F}_p$ be a nonzero element, and consider the polynomial $f(x) = x^p - x + a \in \mathbf{F}_p[x]$. Let L be the splitting field of $f(x)$. Prove that the field extension $L/\mathbf{F}_p$ is Galois, and determine the Galois group.

You may use without proof that $f(x)$ is an irreducible polynomial.

Solution. Note that $f'(x) = -1$ is relatively prime to $f(x)$, so $f(x)$ is separable. Thus L is Galois. Moreover, if α is a root of $f(x)$, then for any $c \in \mathbf{F}_p$ we have

$$f(\alpha + c) = \alpha^p + c^p - \alpha - c + a = f(\alpha) + c^p - c = 0,$$

since $c^p = c$. Thus the set of all roots of $f(x)$ is given by $\{\alpha + c \mid c \in \mathbf{F}_p\}$. This means that $L = \mathbf{F}_p(\alpha)$ is obtained by adjoining the single root α to $\mathbf{F}_p$. Thus $L/\mathbf{F}_p$ is a degree p extension, since $f(x)$ is an irreducible polynomial. It follows that $\mathrm{Gal}(L/\mathbf{F}_p)$ is a group of order p, and hence isomorphic to $\mathbf{Z}/p$.