August 2020, Qualifying Review Algebra, Part II

Problem 1. Can the alternating group A_{2020} be generated by three permutations x, y, and z satisfying $xy = zyx$, $xz = zx$, and $yz = zy$? Be sure to justify your answer.

Solution. No. Suppose this were the case. The second and third equations imply z commutes with x and y; obviously z commutes with itself too. Thus since x, y, and z generate, it follows that z is in the center. But A_{2020} has trivial center, so $z = 1$, and so x and y generate. But the first equation shows that x and y commute, which implies A_{2020} is abelian, a contradiction.

Note: in the exam, the first equation had a typo and was $xy = zxy$. This equation directly implies $z = 1$ (simply cancel the xy from each side), and makes the other two equations redundant. Thus this form of the question simply asks if A_{2020} can be generated by two elements. This is true: one can take x to be a 3-cycle and y to be a 2019-cycle.

Problem 2. Let G be the group of all invertible upper-triangular 2×2 real matrices (with group law matrix multiplication). Let H be the subset of G consisting of all elements of the form g^2 with $g \in G$. Show that H is a subgroup of G and compute its index.

Solution. We claim that H consists of all matrices of the form

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

where a and d are positive real numbers, and b is an arbitrary real number. It is clear that the square of any element of G has this form. Conversely, if $a, d > 0$ then

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} \sqrt{a} & b/(\sqrt{a}+\sqrt{d}) \\ 0 & \sqrt{d} \end{pmatrix}^2,$$

where $\sqrt{\cdot}$ denotes the positive square root, and so all of these matrices belong to H. It is now clear that H forms a group. Moreover, one easily sees that the matrices

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$$

are coset representatives for H in G. Thus $[G : H] = 4$.

Problem 3. Let a and b be rational numbers such that $a^2 + b^2 = 1$, and suppose that $a + bi$ is not a square in the field $\mathbf{Q}(i)$, where $i = \sqrt{-1}$. Let $K = \mathbf{Q}(i, \sqrt{a+bi})$. Show that K is Galois over $\mathbf{Q}$ and describe its Galois group.

Solution. Observe that

$$\sqrt{a - ib} = \frac{1}{\sqrt{a+ib}}$$

since $a^2 + b^2 = 1$, and thus belongs to K. Let

$$f(x) = (x^2 - (a+ib))(x^2 - (a-ib)) = x^4 - 2ax^2 + 1.$$

Thus $f(x)$ has coefficients in $\mathbf{Q}$, and all of its roots belong to K. Moreover, the roots of f generate K (since one can obtain i from $\sqrt{a+ib}$), and so K is exactly the splitting field of f.

Thus $K/\mathbf{Q}$ is a normal extension, and thus Galois (since we're in characteristic 0, or because f is separable). Since $[K:\mathbf{Q}(i)]=2$ and $[\mathbf{Q}(i):\mathbf{Q}]=2$ we have $[K:\mathbf{Q}]=4$, and so $\mathrm{Gal}(K/\mathbf{Q})$ is a group of order 4. Let σ be the unique non-trivial element of $\mathrm{Gal}(K/\mathbf{Q}(i))\cong\mathbf{Z}/2\mathbf{Z}$, and let τ be the restriction of complex conjugation to K (induced by picking an embedding of K into $\mathbf{C}$). Consider the short exact sequence of groups

$$1\to\mathrm{Gal}(K/\mathbf{Q}(i))\to\mathrm{Gal}(K/\mathbf{Q})\to\mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})\to 1.$$

Since σ belongs to and generates $\mathrm{Gal}(K/\mathbf{Q}(i))$ and τ maps to a generator of $\mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})$, it follows that σ and τ generate $\mathrm{Gal}(K/\mathbf{Q})$. Thus $\mathrm{Gal}(K/\mathbf{Q})$ is a group of order 4 generated by two elements of order 2, and is therefore isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$.

Problem 4. Let ℓ be an odd prime number, let p be a prime congruent to 1 modulo ℓ, and let $G=\mathbf{GL}_2(\mathbf{F}_p)$. Give an example of an ℓ-Sylow subgroup of G, and compute how many ℓ-Sylow subgroups G has. You may use without proof the fact that the multiplicative group $\mathbf{F}_p^\times$ is cyclic.

Solution. The order of $\mathbf{GL}_2(\mathbf{F}_p)$ is $(p^2-1)(p^2-p)=p(p-1)^2(p+1)$, since there are p^2-1 choices for the first column and p^2-p choices for the second. Since ℓ is an odd prime dividing $p-1$, it follows that ℓ does not divide p or $p+1$. Thus if ℓ^r is the maximal power of ℓ dividing $p-1$ then ℓ^{2r} is the maximal power of ℓ dividing $\#\mathbf{GL}_2(\mathbf{F}_p)$. Thus any ℓ-Sylow has order ℓ^{2r}.

Let θ be a generator for $\mathbf{F}_p^\times$, and write $p-1=\ell^r k$. Then θ^k is an element of $\mathbf{F}_p^\times$ of order ℓ^r. Thus the set H of all matrices of the form

$$\begin{pmatrix}\theta^{nk} & 0\\ 0 & \theta^{mk}\end{pmatrix}$$

with $n,m\in\mathbf{Z}$ is an ℓ-Sylow subgroup of $\mathbf{GL}_2(\mathbf{F}_p)$. It is isomorphic to $(\mathbf{Z}/\ell^r\mathbf{Z})^2$.

Since all ℓ-Sylows are conjugate, the number of them is the index of the normalizer of any one of them. Thus we should understand the normalizer of H. Suppose that

$$g=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

normalizes H. Then for any n,m there exists n',m' such that

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\theta^{nk} & 0\\ 0 & \theta^{mk}\end{pmatrix}=\begin{pmatrix}\theta^{n'k} & 0\\ 0 & \theta^{m'k}\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix},$$

that is,

$$\theta^{(n-n')k}a=a,\qquad \theta^{(m-n')k}b=b,\qquad \theta^{(n-m')k}c=c,\qquad \theta^{(m-m')k}d=d.$$

Choose n and m distinct modulo ℓ^r. Then either n' or m' is distinct from n modulo ℓ^r. If $n\neq n'\pmod{\ell^r}$ then $\theta^{(n-n')k}\neq 1$, and so the first equation shows $a=0$; if $n\neq m'\pmod{\ell^r}$ then we similarly find $c=0$. A symmetrical argument shows that $b=0$ or $d=0$. Since g is invertible, we thus find that g has the form

$$\begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}\qquad\text{or}\qquad\begin{pmatrix}0 & b\\ c & 0\end{pmatrix}.$$

Conversely, one easily sees that all of these matrices do normalize H. We thus see that the normalizer of H has order $2(p-1)^2$, and therefore has index $\frac{1}{2}p(p+1)$ in $\mathbf{GL}_2(\mathbf{F}_p)$. The number of ℓ-Sylows is therefore $\frac{1}{2}p(p+1)$.

Problem 5. Let p be a prime number and let K be a field of characteristic p. Let $a, b \in K$, with $a \neq 0$, and let L be the splitting field of $x^p - ax - b$ over K. Show that L/K is Galois and that its Galois group is solvable.

Solution. Let $f(x) = x^p - ax - b$. Then $f'(x) = a$ (a constant polynomial), and so $f(x)$ and $f'(x)$ are coprime. Thus $f(x)$ is a separable polynomial, and so its splitting field is Galois. This shows that L/K is Galois.

Suppose that x and y are distinct roots of f. Then

$$0 = f(x) - f(y) = (x^p - ax) - (y^p - ay) = (x-y)^p - a(x-y),$$

and so $(x-y)^{p-1} = a$. This shows that K contains a $(p-1)$st root of a. Conversely, if u is a $(p-1)$st root of a and x is any root of f then $x+u$ is also a root of f (just reverse the above reasoning). We thus see that the roots of f are exactly $x, x+u, x+2u, \ldots, x+(p-1)u$.

Let $K' = K(u)$. Note that K contains all $(p-1)$st roots of unity, since these are just $\mathbf{F}_p^\times$. Thus, by standard Galois theory, K' is a Galois extension of K and $\mathrm{Gal}(K'/K)$ is a subgroup of $\mathbf{Z}/(p-1)\mathbf{Z}$, and hence abelian. By Galois theory, we have a short exact sequence

$$1 \to \mathrm{Gal}(L/K') \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(K'/K) \to 1.$$

Suppose $\sigma \in \mathrm{Gal}(L/K')$. Then $\sigma(x)$ is a root of f, and therefore of the form $x + ku$ for some $k \in \mathbf{Z}/p\mathbf{Z}$. Since σ fixes u, we see that $\sigma(x + \ell u) = x + (k+\ell)u$ for any $\ell \in \mathbf{Z}/p\mathbf{Z}$. Thus, identifying the roots of f with $\mathbf{Z}/p\mathbf{Z}$ (via $\ell \mapsto x + \ell u$), we see that σ simply induces addition by k on $\mathbf{Z}/p\mathbf{Z}$. It follows that $\mathrm{Gal}(L/K')$ is isomorphic to a subgroup of $\mathbf{Z}/p\mathbf{Z}$, and is therefore abelian. We thus see that $\mathrm{Gal}(L/K)$ is an extension of abelian groups, and is therefore solvable.