Algebra Comprehensive Exam

— Fall 2009 —

(1) (a) Let $\mathbb{F}_p$ denote the field with p elements, and for a field $\mathbb{F}$ let $\mathrm{PSL}_n(\mathbb{F})$ be the quotient of $\mathrm{SL}_n(\mathbb{F})$ (the group of $n \times n$ matrices with coefficients in $\mathbb{F}$ and having determinant 1) by $\{\pm I\}$. Show that $|\mathrm{PSL}_2(\mathbb{F}_7)| = 168$.

(b) How many elements of order 7 are there in $\mathrm{PSL}_2(\mathbb{F}_7)$? (You may assume the known fact that $\mathrm{PSL}_2(\mathbb{F}_7)$ is a simple group.)

Solution. (a) The group $\mathrm{GL}_2(\mathbb{F}_7)$ has $(7^2-1)(7^2-7) = 48 \cdot 42$ elements, since to give an element of $\mathrm{GL}_2(\mathbb{F})$ is to give a nonzero element v of $\mathbb{F}^2$ and an element $w \in \mathbb{F}^2$ not in the span of v. The group $\mathrm{SL}_2(\mathbb{F}_7)$ has $48 \cdot 42/6 = 168 \cdot 2$ elements, since the determinant gives a surjective homomorphism from $\mathrm{GL}_2(\mathbb{F})$ to $\mathbb{F}^*$ with kernel $\mathrm{SL}_2(\mathbb{F})$. Finally, we have $|\mathrm{PGL}_2(\mathbb{F})| = |\mathrm{GL}_2(\mathbb{F})|/2$.

(b) The argument applies to any simple group G of order 168. The number n_7 of 7-Sylow subgroups of G is 1 mod 7 and divides 24. Since G is simple, $n_7 > 1$. Thus $n_7 = 8$. Any two 7-Sylow subgroups intersect only in the identity, and each contains 6 elements of order 7. Thus G contains 48 elements of order 7.

□

(2) Let G be a group whose group of automorphisms is cyclic. Prove that G is abelian.

Solution. Consider the map $\phi : G \to Aut(G)$ given by $\phi(g)(h) = ghg^{-1}$. This is a well defined homomorphism ($\phi(g_1g_2)(h) = (g_1g_2)h(g_2^{-1}g_1^{-1}) = \phi(g_1)(g_2hg_2^{-1}) = \phi(g_1) \circ \phi(g_2)(h))$. Moreover, $\ker \phi = Z(G)$. Indeed, if $g \in Z(G)$ then $\phi(g)(h) = h$ so $\phi(g)$ is the identity automorphism. Conversely if $g \in \ker \phi$ then $\phi(g)(h) = ghg^{-1} = h$ for all h. In other words $gh = hg$ for all $h \in G$ thus $g \in Z(G)$. Thus the first isomorphism theorem says that $G/Z(G)$ is isomorphic to a subgroup of $Aut(G)$, a cyclic group. Thus $G/Z(G)$ is cyclic. But it is well-known that if G/Z is cyclic then G is abelian. (Proof: Suppose G/Z is cyclic with generator yZ. So every element of G/Z is of the form $(yZ)^n$ for some n. Thus every element of G is of the form $y^n a$ for some $a \in Z$. Given two elements g and h in G, write $g = y^n a$ and $h = y^m b$. We have $gh = y^n a y^m b = y^n y^m ab = y^m y^n ab = y^m b y^n a = hg$, where the second and fourth equality follow by $a, b \in Z$. So G is abelian.) □

(3) Let R be an integral domain and let a be a non-zero non-unit of R.

(a) Prove that the ideal (a, x) in the polynomial ring $R[x]$ is not principal.

(b) Use part (a) to show that if K is a field, then the polynomial ring $K[x, y]$ is not a PID.

Solution. (a) If (a, x) is a principal ideal then there is some $p(x) \in R[x]$ such that $(p(x)) = (a, x)$. Since $a \in (a, x) = (p(x))$ there is some $q(x)$ such that $q(x)p(x) = a$. Since R is an integral domain, we know that

$$0 = \deg(a) = \deg(q(x)p(x)) = \deg(q(x)) + \deg(p(x)).$$

Thus $p(x)$ has degree 0, and so $p(x) = p$ for some $p \in R$. Now since $x \in (a, x) = (p(x))$, there is some $r(x)$ such that $r(x)p = x$. Arguing with degrees again, we see that $r(x) = r_1 x + r_0$ and so $r_1 p = 1$ and $r_0 p = 0$. Thus p is a unit in R (and therefore in $R[x]$ as well). Thus $(a, x) = (p) = R[x]$ and $1 \in (a, x)$. So there are polynomials $b(x)$ and $c(x)$ such that

$$b(x)a + c(x)x = 1.$$

There is no constant term in $c(x)x$, so a times the constant term b_0 in $b(x)$ is 1, that is $ab_0 = 1$ and a is a unit in R, contradicting the choice of a.

(b) Note that $K[x]$ is an integral domain (since K is) and that x in not a unit in $K[x]$, since if $p(x)$ were an inverse to x we would have $1 = xp(x)$ but then $0 = \deg 1 = \deg(x) + \deg(p(x)) = 1 + \deg(p(x))$, which is impossible. Thus from part (a), we know that (x, y) is a non-principal ideal in $(K[x])[y] \cong K[x, y]$.

$\square$

(4) Let m, n be positive integers with $n \mid m$. Prove that the natural surjective ring homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ induces a surjective homomorphism $(\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ of unit groups.

Solution. The map which sends $a + m\mathbb{Z}$ to $a + n\mathbb{Z}$ is well-defined because $n \mid m$, and it is obviously surjective and a homomorphism. Restricting to $(\mathbb{Z}/m\mathbb{Z})^*$ gives a homomorphism $(\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ of unit groups. We need to show that this homomorphism is surjective. Suppose $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ is a unit. Then $a \in \mathbb{Z}$ and $(a, n) = 1$. We want to prove that there exists $x \in \mathbb{Z}$ such that $x \equiv a \pmod{n}$ and $(x, m) = 1$. Let $p_1, \ldots, p_k$ be the primes dividing m but not n; by the Chinese Remainder Theorem, we can solve the simultaneous congruences $x \equiv 1 \pmod{p_1 \cdots p_k}$ and $x \equiv a \pmod{n}$, and any solution to this congruence will be relatively prime to m.

$\square$

(5) Let F be a field and $p(x) \in F[x]$ a polynomial. Prove there is a field extension F' of F in which $p(x)$ has a root (note we are not assuming $p(x)$ is irreducible). (In this problem you must construct the field F', you cannot cite a theorem for its existence.)

Solution. We can assume $p(x)$ is monic. Write $p(x) = p_1(x) \ldots p_k(x)$ where the p_i are monic irreducible. If any of the p_i are linear then $p(x)$ has a root in F so take the extension to be $F' = F$. Otherwise all the p_i have degree greater than one. Let $K = F[x]/(p_1)$. Since p_1 is irreducible (p_1) is a maximal ideal so K is a field and F naturally a subfield of K (just the constants in $F[x]$ projected into K). Let $\theta = x + (p_1)$ in K. Now $p_1(\theta) = p_1(x) + (p_1) = (p_1) = 0$ (in K). So θ is a root of p_1 and hence of p in K.

$\square$

(6) Let $p(x) = x^3 - 2$ and let F be the smallest subfield of $\mathbb{C}$ in which $p(x)$ factors into linear factors. Determine $[F : \mathbb{Q}]$, and find a basis for F as a vector space over $\mathbb{Q}$.

Solution. Let $\alpha = \sqrt[3]{2}$ and let $F' = \mathbb{Q}(\alpha)$. Since p is irreducible over $\mathbb{Q}$, we see that $[F' : \mathbb{Q}] = 3$. Now let α' be a second root of p over $\mathbb{C}$. Let $F'' = F(\alpha') = \mathbb{Q}(\alpha, \alpha')$. If $F'' = F'$ then $\alpha \in F'$ but we know the other two roots of p are complex so this is not possible. Thus $[F'' : F'] = 2$ or 3, but $p(x) = (x - \alpha)q(x)$ for some quadratic polynomial $q(x)$. We know that $q(x)$ is irreducible over F' (or it would have a root and F'' would then be F'). Since α' is a root of $q(x)$ we know $[F'' : F'] = 2$. The polynomial $p(x)$ factors completely over F'', and is clearly the smallest subfield of $\mathbb{C}$ with this property. So $F = F''$ and $[F : \mathbb{Q}] = 6$. We can take a basis for F to be $1, \alpha, \alpha^2, \alpha', \alpha'\alpha, \alpha'\alpha^2$.

$\square$

(7) If λ is an eigenvalue of an $n \times n$ matrix A with complex coefficients, and $p(x) \in \mathbf{C}[x]$ is any polynomial, show that $p(\lambda)$ is an eigenvalue of $p(A)$. Is every eigenvalue of $p(A)$ of the form $p(\lambda)$ for some eigenvalue λ of A?

Solution. Replacing A by a similar matrix, we may assume (by Schur's theorem, or by the Jordan Canonical Form) that A is upper triangular. In this case, a simple computation shows that $p(A)$ is upper triangular, and that the i^{th} diagonal element of $p(A)$ is $p(a_{ii})$.

Since the eigenvalues of an upper triangular matrix are just the diagonal entries, we have shown that the eigenvalues of $p(A)$ are exactly the complex numbers of the form $p(\lambda)$, where λ is an eigenvalue of A.

$\square$

(8) Let V be a finite-dimensional complex vector space, and let S, T be diagonalizable linear transformations from V to itself. Prove that S and T are simultaneously diagonalizable if and only if $ST = TS$.

Solution. If S and T are simultaneously diagonalizable, then there is a basis B for V with respect to which $[S]_B$ and $[T]_B$ are both diagonal matrices. Since diagonal matrices commute, it follows that S and T commute.

Conversely, suppose S and T commute. If v is an eigenvector for S, then $S(Tv) = T(Sv) = \lambda Tv$, so Tv is also an eigenvector for S (with the same eigenvalue). In other words, each λ-eigenspace V_λ of S is invariant under T. Fix λ, and let T_λ be the restriction of T to V_λ. Then T_λ is diagonalizable, since T is. (This follows, for example, from the fact that a linear transformation over $\mathbb{C}$ is diagonalizable iff its minimal polynomial is squarefree; note that the minimal polynomial of T_λ divides the minimal polynomial of T.) Thus V_λ has a basis of eigenvectors for T, which are also eigenvectors for S. Concatening the resulting bases for each eigenvalue λ of S, we see that there is a basis for $V = \oplus V_\lambda$ consisting of eigenvectors for both S and T. This is precisely what it means for S and T to be simultaneously diagonalizable.

$\square$