Algebra May 2014, Qualifying Review, Morning Exam Solutions

Problem 1. Let $A$ and $B$ be finite sets with $\gcd(|A|, |B|) = 1$. Let $G$ be a group that acts transitively on $A$ and on $B$. Show that the diagonal action of $G$ on $A \times B$ is transitive.

Solution. Write $n = |A|$ and $m = |B|$. Pick $a \in A$ and $b \in B$, and let $G_a$ and $G_b$ be their stabilizers in $G$. Note that we have a bijection $G/G_a \to A$ given by $gG_a \mapsto ga$, and so $[G : G_a] = n$. Similarly, $[G : G_b] = m$. Let $H = G_a \cap G_b$. Note that $[G : H] = [G : G_a][G_a : H]$, and so $n = [G : G_a]$ divides $[G : H]$. Similarly, $m$ divides $[G : H]$, and so (since $n$ and $m$ are coprime), $nm$ divides $[G : H]$. Now, $H$ is the stabilizer of $(a, b) \in A \times B$, and so the map $f : G/H \to A \times B$ given by $gH \mapsto (ga, gb)$ is injective. Since $A \times B$ has cardinality $nm$ and $G/H$ has cardinality at least $nm$, it follows that $G/H$ has cardinality exactly $nm$ and $f$ is a bijection. This proves transitivity: given any $(a', b') \in A \times B$, there exists $g \in G$ mapping to it under $f$, i.e., $(a', b') = (ga, gb)$.

Problem 2. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Consider $K$ as a $\mathbb{Q}$ vector space. Compute the trace of multiplication by $1 + \sqrt{2}$.

Solution. Define the following elements of $K$:

$$e_1 = 1, \quad e_2 = \sqrt{2}, \quad e_3 = \sqrt{3}, \quad e_4 = \sqrt{6}.$$

These form a basis for $K$ as a $\mathbb{Q}$ vector space. We now compute what multiplication by $1 + \sqrt{2}$ does in this basis. We have

$$
\begin{align*}
(1 + \sqrt{2})e_1 &= 1 + \sqrt{2} = e_1 + e_2 \\
(1 + \sqrt{2})e_2 &= 2 + \sqrt{2} = 2e_1 + e_2 \\
(1 + \sqrt{2})e_3 &= \sqrt{3} + \sqrt{6} = e_3 + e_4 \\
(1 + \sqrt{2})e_4 &= 2\sqrt{3} + \sqrt{6} = 2e_3 + e_4
\end{align*}
$$

Thus the matrix for multiplication-by-$(1 + \sqrt{2})$ in the basis $e_1, e_2, e_3, e_4$ is

$$
\begin{bmatrix}
1 & 1 & 0 & 0 \\
2 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 \\
0 & 0 & 2 & 1
\end{bmatrix}.
$$

This matrix has trace 4, which is (by definition) the trace of multiplication by $1 + \sqrt{2}$.

Remark. One can do the computation more quickly as follows: $\sqrt{2}$ permutes the basis $e_i$ without fixed points, and therefore has trace 0, while the trace of 1 is equal to $[K : \mathbb{Q}] = 4$.

Problem 3. Let $A$ be a real $n \times n$ matrix with no real eigenvalues. Show that there is a polynomial $f \in \mathbb{R}[x]$ so that $f(A)^2 = -\text{Id}$.

Solution. Let $R$ be the $\mathbb{R}$-subalgebra of the matrix algebra generated by $A$. It suffices to show that $R$ contains an element which squares to $-1$. Now, $R$ is isomorphic to $\mathbb{R}[x]/(f(x))$, where $f(x)$ is the minimal polynomial of $A$. Write $f(x) = \prod_{i=1}^k f_i(x)^{e_i}$, where the $f_i(x)$ are distinct monic irreducible polynomials over $\mathbb{R}$, and $e_i \geq 1$. Then, by the Chinese remainder theorem, $R$ is isomorphic to $\prod_{i=1}^k R_i$, where $R_i = \mathbb{R}[x]/(f_i(x)^{e_i})$. It therefore suffices to show that each $R_i$ contains an element that squares to $-1$.

Let $J_i$ be the ideal of $R_i$ generated by $f(x)$. Note that this ideal is nilpotent: $J_i^{e_i} = 0$. We will prove inductively that for each $m > 0$ the ring $R_i$ contains an element $x$ such that $x^2 = -1$ modulo $J_i^m$. Taking $m = e_i$ will give an element of $R_i$ squaring to $-1$. We first prove the $m = 1$ case. The roots of $f_i(x)$ are eigenvalues of $A$, and therefore not real. Thus $R_i/J_i = \mathbb{R}[x]/(f_i(x))$ is isomorphic to $\mathbb{C}$. Therefore, if $x$ maps to $\sqrt{-1} \in R_i/J_i$ then $x^2 = -1$ holds modulo $J_i$. Suppose now that we have $x \in R_i$ such that $x^2 = -1$
modulo $J_i^m$, i.e., $x^2 = -1 + y$ with $y \in J_i^m$. Let $z = x(1 + \frac{1}{2}y)$. Then
\[ z^2 = (-1 + y)(1 + y + \frac{1}{4}y^2) = -1 - \frac{1}{4}y^2 + \frac{1}{4}y^3. \]
Since $\frac{1}{4}(y^3 - y^2)$ belongs to $J_i^{m+1}$, we thus see that $z^2 = -1$ modulo $J_i^{m+1}$. This completes the proof.

**Problem 4.** Recall that $\text{SL}_2(\mathbb{Z})$ is the group of $2 \times 2$ integer matrices of determinant 1. Show that the commutator subgroup of $\text{SL}_2(\mathbb{Z})$ is a proper subgroup. (Hint: One proof uses the isomorphism $\text{SL}_2(\mathbb{F}_2) = S_3$.)

**Solution.** Let $f : \text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{F}_2)$ be the reduction mod 2 map. The two matrices
\[ g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad h = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \]
belong to $\text{SL}_2(\mathbb{Z})$. By direct computation, $f(g)$ has order 2 and $f(h)$ has order 3. It follows that $f(g)$ and $f(h)$ generated $\text{SL}_2(\mathbb{F}_2)$, as this group has order 6. Thus $f$ is surjective, since its image contains a generating set. Now, $\text{SL}_2(\mathbb{F}_2)$ is solvable: the subgroup generated by $f(h)$ has index 2, and is therefore normal, and so $\text{SL}_2(\mathbb{F}_2)$ is an extension of $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/3\mathbb{Z}$. Thus the commutator subgroup of $\text{SL}_2(\mathbb{F}_2)$ is a proper subgroup. Since $f$ maps the commutator subgroup of $\text{SL}_2(\mathbb{Z})$ into the commutator subgroup of $\text{SL}_2(\mathbb{F}_2)$, it follows that the commutator subgroup of $\text{SL}_2(\mathbb{Z})$ must also be a proper subgroup.

**Problem 5.** What are the orders of elements in $\text{GL}_2(\mathbb{F}_{13})$? Note that the order of $\text{GL}_2(\mathbb{F}_{13})$ is $(13^2 - 13)(13^2 - 1) = 13 \cdot 12^2 \cdot 14$.

**Solution.** There are three types of elements of $G = \text{GL}_2(\mathbb{F}_{13})$: (1) those that are semi-simple with eigenvalues in $\mathbb{F}_{13}$; (2) those that are semi-simple and whose eigenvalues are Galois conjugate elements of $\mathbb{F}_{13^2}$; and (3) those that are not semi-simple. We compute the orders of each type of elements.

Suppose $g$ is a Type 1 element of $G$. Then it is conjugate to a diagonal matrix, and therefore has the same order as a diagonal matrix. Furthermore, every diagonal matrix is Type 1. The group of diagonal matrices is isomorphic to $\mathbb{F}_{13}^\times \times \mathbb{F}_{13}^\times \cong (\mathbb{Z}/12\mathbb{Z})^2$.

Every element of this group has order dividing 12, and every divisor of 12 occurs. Thus the Type 1 elements have orders 1, 2, 3, 4, 6, and 12.

Suppose $g$ is a Type 2 element. Let $H$ be the subgroup of $\text{GL}_2(\mathbb{F}_{13^2})$ consisting of elements of the form
\[ \begin{bmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{bmatrix}, \]
where $\alpha$ is a non-zero element of $\mathbb{F}_{13^2}$, and $\overline{\alpha}$ is its Galois conjugate. Then $g$ is conjugate over $\mathbb{F}_{13^2}$ to an element of $H$, and therefore has the same order as an element of $H$. Furthermore, every element of $H$ is conjugate to some element of $G$ (the matrix for the multiplication-by-$\alpha$ map on $\mathbb{F}_{13^2}$ is conjugate to the above matrix). The group $H$ is isomorphic to $\mathbb{F}_{13^2}^\times \cong \mathbb{Z}/168\mathbb{Z}$. Every element of this group has order dividing 168, and every divisor of 168 occurs. Thus the Type 2 elements have orders 1, 2, 3, 4, 6, 7, 8, 12, 14, 21, 24, 28, 42, 56, 64, and 168.

Finally, suppose that $g$ is a Type 3 element. Then $g$ is conjugate to a matrix of the form
\[ \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix} \]
where $a \in \mathbb{F}_{13}^\times$, and every matrix of this form is a Type 3 element. Note that
\[ \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & a^{-1} \\ 0 & 1 \end{bmatrix} = g_1g_2. \]
The order of $g_1$ is just the order of $a$ in $\mathbb{F}_{13}^\times$, and therefore divides 12; furthermore, by choosing $a$ appropriately, the order of $g_1$ can be any divisor of 12. The order of $g_2$ is equal to 13. Since $g_1$ and $g_2$ commute and have coprime orders, the order of $g_1g_2$ is just the product of the orders of $g_1$ and $g_2$. We thus see that the Type 3 elements have orders 13, 26, 39, 52, 78, and 156.
In conclusion, the orders of elements of $G$ are:

1, 2, 3, 4, 6, 7, 8, 12, 13, 14, 21, 24, 26, 28, 39, 42, 52, 56, 78, 84, 156, and 168.

Thus, while $|G|$ has 48 divisors, only 22 of them actually occur as orders of elements.
Algebra May 2014, Qualifying Review, Afternoon Exam Solutions

Problem 1. Let $G$ and $H$ be finite groups with $|G| = |H| = n$. Let $K$ be a subgroup of $G \times H$ with $|K| = n$ and $K \cap (G \times \{ e \}) = K \cap (\{ e \} \times H) = \{ e \}$. Show that $G \cong H$.

Solution. Let $f : G \times H \to G$ and $g : G \times H \to H$ be the two projection maps. The kernel of $f$ is $\{ e \} \times H$. Therefore, $\ker(f) \cap K = \{ e \}$, and so the restriction of $f$ to $K$ is injective. Since $|K| = |G|$, it follows that the restriction of $f$ to $K$ is bijective, and so $f$ induces a group isomorphism $K \to G$. Similarly, $g$ induces a group isomorphism $K \to H$. Since isomorphism is transitive, $G$ and $H$ are isomorphic.

Problem 2. Let $f(x)$ be a degree 6 polynomial with rational coefficients, whose splitting field over $\mathbb{Q}$ has Galois group $S_6$ and let $\beta$ be a root of $f$. Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be algebraic numbers all of whom are of degree $\leq 5$. Show that $\beta$ is not in $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$.

Solution. Let $K$ be the splitting field of $f$, which is the Galois closure of $\mathbb{Q}(\beta)$. Let $L_i$ be the Galois closure of $\mathbb{Q}(\alpha_i)$, and let $G_i$ be the Galois group of $L_i$ over $\mathbb{Q}$. Then the compositum $L = L_1 \cdots L_r$ is the Galois closure of $\mathbb{Q}(\alpha_1, \ldots, \alpha_r)$, and its Galois group $G$ is a subgroup of $G_1 \times \cdots \times G_r$. If $\beta$ were contained in $\mathbb{Q}(\alpha_1, \ldots, \alpha_r)$ then $K$ would be contained in $L$, and so $\text{Gal}(K/\mathbb{Q}) = S_6$ would be a quotient of $\text{Gal}(L/\mathbb{Q}) = G$. However, each $G_i$ is a subgroup of $S_n$ with $1 \leq n \leq 5$, and so this is impossible. (Consider the Jordan–Hölder constituents: $S_6$ has the simple group $A_6$ as a constituent, but $A_6$ does not occur as a constituent of any subgroup of $S_n$ with $n \leq 5$, and therefore does not occur as a constituent of $G$.)

Problem 3. Let $p$ be a prime and let $q = p^e$ for some positive integer $e$. How many elements of $\mathbb{F}_q$ are of the form $x^p - x$, for $x \in \mathbb{F}_q$?

Solution. Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be the map given by $f(x) = x^p - x$. Regarding $\mathbb{F}_q$ as an $\mathbb{F}_p$ vector space, this map is linear. Its kernel is exactly $\mathbb{F}_p^\times$. (Proof: every element of $\mathbb{F}_p^\times$ belongs to the kernel, by Fermat’s little theorem, which gives $p$ distinct roots of the degree $p$ polynomial $f$, and so there are no other roots.) Thus $f$ is a map of $e$ dimensional vector spaces whose kernel is one dimensional. It follows that the image of $f$ is $e - 1$ dimensional, and thus contains $p^{e - 1}$ elements.

Problem 4. Let $1 \to H \to G \xrightarrow{\pi} C \to 1$ be a short exact sequence of finite groups, with $C$ cyclic and $\text{GCD}(|H|, |C|) = 1$. Show that there is a map of groups $\sigma : C \to G$ with $\pi(\sigma(x)) = x$ for all $x \in C$.

Solution. Let $n = |H|$ and $m = |C|$. Since $\pi$ is surjective, there exists an element $x \in G$ such that $\pi = \pi(x)$ is a generator of $C$. Choose an integer $a$ such that $an = 1$ modulo $m$, which is possible since $n$ and $m$ are relatively prime, and put $y = x^a$. Then $\pi(y) = \pi^a = \pi : \pi^{an - 1} = \pi$ since $an - 1$ is divisible by $m$ and $C$ has order $m$. On the other hand, $y^n = x^{am}$. Since $\pi^m = 1$, it follows that $\pi(x^m) = 1$, and so $x^m$ belongs to $H$. Since $H$ has order $n$, it follows that $(x^m)^n = 1$. Thus $y^n = 1$. We can therefore define a group homomorphism $\sigma : C \to G$ by $\sigma(\pi^k) = y^k$. This map is well-defined since every element of $C$ is of the form $\pi^k$, for some $k \in \mathbb{Z}/m\mathbb{Z}$, and $y^m = 1$. We have $\pi(\sigma(\pi^k)) = \pi(\sigma(\pi))^k = \pi(y)^k = \pi^k$, and so $\pi \circ \sigma$ is the identity.

Problem 5. Let $A$ and $B$ be two $n \times n$ matrices over a field $K$.

(a) Show that the matrices $AB$ and $BA$ need not be similar.

(b) Show that $AB$ and $BA$ have the same characteristic polynomial.

Solution. (a) Take

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$
Then $AB$ is non-zero but $BA$ is zero, and so they are not similar.

(b) First suppose that $A$ is invertible. Then $AB$ and $BA$ are similar, as $AB = A(BA)A^{-1}$, and so have the same characteristic polynomial. We now handle the general case. For a matrix $M$, let $c_i(M)$ be the $i$th coefficient of the characteristic polynomial of $M$. Note that this is a polynomial in the entries of $M$. Define a polynomial $f(t)$ by

$$f(t) = c_i((A - tI_n)B) - c_i(B(A - tI_n)).$$

Suppose that $t \in K$ is not an eigenvalue of $A$. Then $A - tI_n$ is invertible, and so $(A - tI_n)B$ and $B(A - tI_n)$ have the same characteristic polynomial, and so $f(t) = 0$. Thus $f(t) = 0$ for infinitely many elements $t \in K$, as $A$ has finitely many eigenvalues. It follows that $f(t)$ is the zero polynomial. In particular, $0 = f(0) = c_i(AB) - c_i(BA)$. Thus $c_i(AB) = c_i(BA)$ for all $i$, and so the characteristic polynomials of $AB$ and $BA$ agree.