Fall 2012
Algebra Qualfying Exam Solutions

Hannah Hoganson, Shelby Kilmer, Allechar Serrano

August 5, 2016

1. Determine, up to isomorphism, the groups of order 154.

   Solution: Let G be a group of order $154 = 2 \times 7 \times 11$. Let n_p be the number of Sylow $p-$subgroups of G, and P_p be a Sylow $p-$subgroup of G. We have that $n_{11}|14$ and $n_{11} \equiv 1 \bmod 11$, hence $n_{11} = 1$, that is, the Sylow $11-$subgroup is normal in G. Consider $N = P_{11}P_7$, N is a subgroup since P_{11} is the unique Sylow $11-$ subgroup. Also $P_{11} \cap P_7$ is trivial, hence $|N| = 77$ and N is normal since it has index 2 in G. Now, NP_2 is also a subgroup of G and $N \cap P_2$ is also trivial, so $|NP_2| = 154 = |G|$. Therefore, $G = N \rtimes_\varphi P_2$, where $\varphi : P_2 \to \mathrm{Aut}(N)$. Since $\mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/11\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/11\mathbb{Z})^\times \times \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})^\times = \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Let $g \in P_2$ be a nontrivial element. Then, under φ, g has order 1 (when φ is trivial) or order 2. Thus we have at most 4 non-isomorphic groups of order 154, namely, $\mathbb{Z}/154\mathbb{Z}, D_{14} \times \mathbb{Z}/11\mathbb{Z}, D_{22} \times \mathbb{Z}/7\mathbb{Z}$, and D_{154}.

2. Let P be a $p-$Sylow subgroup of a group G, and N be a normal subgroup of G. Prove that $P \cap N$ is a $p-$Sylow subgroup of N.

   Solution 1: Let $|G| = p^k m$ where k is maximal (i.e., m contains no factor of p). Then $|P| = p^k$. We will utilize the property that $[G : P] = |G|/|P| = m$ implies p does not divide $[G : P]$, and similarly, if p does not divide $[G : P']$, then P' is a p-Sylow subgroup.

   First, we note $P \cap N \leq P$, and so $|P \cap N| = p^\ell$ where $\ell \leq k$. Since $P \cap N \leq N$, we use the second isomorphism theorem to note:

$$\frac{|PN|}{|P|} = \frac{|N|}{|P \cap N|} (= [N : P \cap N]).$$

If p divides $\frac{|PN|}{|P|}$, then $\frac{|PN|}{|P|} = p^n$ for some $n > 1$. Since $|P| = p^k$, we have $|PN| = p^{n+k}$. But then $|PN|$ is a p-Sylow subgroup of G, which is a contradiction since $n + k > k$.

We then have that p does not divide $\frac{|PN|}{|P|}$, and thus p does not divide $[N : P \cap N]$. By the property noted above, we conclude $P \cap N$ is a Sylow p-subgroup of N.

Solution 2: Choose P_0 to be a Sylow $p-$subgroup of N such that $P \cap N \leqslant P_0$. We have that $P_0 \leqslant gPg^{-1}$ and $P_0 \leqslant N$ since $g^{-1}Pg \leqslant P \cap N$. So $|P \cap N| = |P_0|$ and $P \cap N$ is a Sylow $p-$subgroup of N.

3. Determine the number of 2×2 nilpotent matrices over a finite field $\mathbb{F}_q$.

Solution 1: Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a nilpotent matrix. Then $A^k = 0$ for some $k \leq 2$; this is because A is a 2×2 matrix. If $k = 1$ then $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and there is one matrix of this type.

If $k = 2$ then $A^2 = 0$,

$$A^2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{bmatrix}$$

So we get a system of equations:

$$\begin{cases} a^2 + bc = 0 \\ b(a + d) = 0 \\ c(a + d) = 0 \\ bc + d^2 = 0 \end{cases}$$

Note that we must have $a + d = 0$. If $a = d = 0$ then either $b = 0$ or $c = 0$ so we get two types of matrices:

$$\text{Type 1: } \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \quad \text{Type 2: } \begin{bmatrix} 0 & 0 \\ c & 0 \end{bmatrix}$$

and there are $q - 1$ types of each of these (we have already counted the zero matrix).

If $a = -d \neq 0$ then for any nonzero value of b there is a unique solution for c, $c = -b^{-1}a^2$ (we are working in a field so b^{-1} exists). This gives the final type of nilpotent matrix:

$$\text{Type 3:} \begin{bmatrix} a & b \\ -b^{-1}a^2 & -a \end{bmatrix}$$

and there are $(q-1)^2$ of these matrices. So, in total there are $1+2(q-1)+(q-1)^2 = q^2$ nilpotent 2×2 matrices over $\mathbb{F}_q$.

Solution 2: Let M be a nilpotent matrix, then $M^k = 0$ for some k. Therefore, 0 is the only eigenvalue of M and its characteristic polynomial is $x^2 - \text{trace}(M)x + \det(M)$, so we want $\text{trace}(M), \det(M) \equiv 0 \bmod q$. There are q^2 such matrices.

4. Determine, up to conjugacy, all 4×4 matrices M over $\mathbb{Q}$ with $M^5 = -M^3$ and $M^3 \neq 0$.

Solution: M is a root of $x^5 + x^3 = x^3(x^2+1)$ so the minimal polynomial of M divides $x^3(x^2+1)$. Note that the minimal polynomial of M can't be x, x^2 or x^3 because then $M^3 = 0$. This leaves the following possibilities:

Minimal Polynomial	Invariant Factors	Rational Canonical Form
x^2+1	x^2+1, x^2+1	$\begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
$x(x^2+1)$	x^3+x, x	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
$x^2(x^2+1)$	x^4+x^2	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Hence, there are 3 conjugacy classes.

5. Let M be an $n \times n$ matrix over $\mathbb{Q}$ in which each entry is 1. What is the Jordan form of M?

Solution: Note that there are $n-1$ linearly independent columns in the matrix (whose respective eigenvalue is 0), the remaining column is an eigenvector with eigenvalue equal to n. Then, the characteristic polynomial of M is $x^{n-1}(x-n)$. It is easy to verify that the minimal polynomial is $x(x-n)$. Therefore the Jordan form of M has n blocks of size 1, $n-1$ of these blocks correspond to the eigenvalue 0 and the remaining block corresponds to the eigenvalue n.

6. Let $f(x)$ be a monic polynomial with integer coefficients, such that $f(\alpha) = 0 = f(2\alpha)$ for some complex number α. Prove that $f(0) \neq 1$.

   Solution: We don't know how to do this problem. If you figure it out, you should let us know!

7. Let R be a commutative ring with 1

   (a) If a maximal ideal $\mathfrak{m}$ of R is principal, prove that there is no ideal I with $\mathfrak{m}^2 \subsetneq I \subsetneq \mathfrak{m}$.

   Solution: Suppose such ideal I exists, then $\mathfrak{m} = (a)$ for $a \notin I$. Choose $x \in I$, then $x = ay$ for some $y \in R$. If $y \in \mathfrak{m}$, then $y = az$ and $x = a^2 z \in \mathfrak{m}^2$. Otherwise, $\mathfrak{m} + (y) = R$ so $1 = am + yn$. Then $a = a^2 m + ayn = a^2 m + xn \in I$, which is a contradiction.

   (b) Give an example where $\mathfrak{m}$ is maximal, but is an ideal I with $\mathfrak{m}^2 \subsetneq I \subsetneq \mathfrak{m}$.

   Solution: Take $\mathfrak{m} = (x, y)$ since it is a maximal ideal in $R[x, y]$ that is not principal. We have $\mathfrak{m}^2 = (x^2, xy, y^2) \subset (x^2, xy, y) \subset \mathfrak{m}$.

8. Let α be a complex root of $x^6 + 3$. Set $K = \mathbb{Q}(\alpha)$.

   (a) Prove that K contains a primitive $6-$th root of unity.

   Solution: $x^6 + 3$ is irreducible over $\mathbb{Q}$ by Eisenstein for $p = 3$. Consider $\omega = \frac{-1+\alpha^3}{2}$, then $\omega^2 + \omega + 1 = 0$ and $\omega^3 = 1$. Hence $1, \omega, \omega^2, -1, -\omega, -\omega^2$ are all distinct element of K and they are the six roots of $x^6 + 1 = 0$.

   (b) Compute the Galois group of K over $\mathbb{Q}$.

   Solution: Then $\alpha, \omega\alpha, \omega^2\alpha, -\alpha, -\omega\alpha, -\omega^2\alpha$ are the six roots of $x^6 + 3 = 0$ and they are all in $K(\alpha)$, which has degree 6 over $\mathbb{Q}$ so $|\operatorname{Gal}(K/\mathbb{Q})| = 6$. The group of automorphisms is transitive. Consider $\sigma : \alpha \longmapsto \omega\alpha, \omega \longmapsto \omega$ and $\tau : \alpha \longmapsto -\alpha, \omega \longmapsto \omega^2$.

Notice that $\tau\sigma(\alpha) = -\omega^2\alpha$ and $\sigma\tau(\alpha) = -\omega\alpha$ so the group is noncommutative. Therefore, $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

9. Let ζ be a primitive $16-$th root of unity over a field K. Determine $[K(\zeta) : K]$ when K is:

   (a) $\mathbb{F}_7$

   Solution: Recall that the Galois group of a finite extension of a finite field $\mathbb{F}_p$ is always cyclic and generated by the Frobenius automorphism, $\varphi(x) = x^p$, where p is the characteristic of the fields.

   $\mathrm{Gal}(\mathbb{F}_7(\zeta)/\mathbb{F}_7)$ is generated by φ_7, and φ_7 acts with order 2 because $\varphi_7^2(\zeta) = \varphi_7(\zeta^7) = \zeta^{49} = \zeta$. Thus,

   $$[\mathbb{F}_7(\zeta) : \mathbb{F}_7] = |\mathrm{Gal}(\mathbb{F}_7(\zeta)/\mathbb{F}_7)| = 2$$

   (b) $\mathbb{F}_9$

   Solution: Here we need to be more careful because $\mathbb{F}_9$ is already a degree 2 extension of $\mathbb{F}_3$. We will consider the tower of fields $\mathbb{F}_3 \subset \mathbb{F}_9 \subset \mathbb{F}_9(\zeta)$. Each extension is finite so the Galois group of $\mathbb{F}_9(\zeta)$ over $\mathbb{F}_3$ is generated by φ_3.

   $$\varphi_3 : \zeta \longmapsto \zeta^3 \longmapsto \zeta^9 \longmapsto \zeta^{27} = \zeta^{11} \longmapsto \zeta^{33} = \zeta$$

   So, $[\mathbb{F}_9(\zeta) : \mathbb{F}_3] = |\mathrm{Gal}(\mathbb{F}_9(\zeta)/\mathbb{F}_3)| = 4$ and thus

   $$[\mathbb{F}_9(\zeta) : \mathbb{F}_9] = \frac{[\mathbb{F}_9(\zeta) : \mathbb{F}_3]}{[\mathbb{F}_9 : \mathbb{F}_3]} = \frac{4}{2} = 2$$

   (c) $\mathbb{F}_{17}$

   Solution: $\mathrm{Gal}(\mathbb{F}_{17}(\zeta)/\mathbb{F}_{17})$ is generated by φ_{17}, and φ_{17} is the identity map because $\varphi_{17}(\zeta) = \zeta^{17} = \zeta$. Thus,

   $$[\mathbb{F}_{17}(\zeta) : \mathbb{F}_{17}] = |\mathrm{Gal}(\mathbb{F}_{17}(\zeta)/\mathbb{F}_{17})| = 1$$

10. Explain (preferably in a sentence!) why $\mathbb{F}_3[x]/(x^2-2)$ and $\mathbb{F}_3[x]/(x^2-2x-1)$ are isomorphic. Then construct an explicit isomorphism.

    Solution: Both $x^2 - 2$ and $x^2 - 2x - 1$ are irreducible polynomials of degree 2 in $\mathbb{F}_3[x]$, hence $\mathbb{F}_3[x]/(x^2 - 2)$ and $\mathbb{F}_3[x]/(x^2 - 2x - 1)$ are isomorphic to $\mathbb{F}_9$. $x + 1$ is a generator for both fields, so we have the explicit isomorphism.

k	1	2	3	4	5	6	7	8
$(x+1)^k \bmod x^2-2$	$x+1$	$2x$	$2x+1$	2	$2x+2$	x	$x+2$	1
$(x+1)^k \bmod x^2-2x-1$	$x+1$	$x+2$	$2x$	2	$2x+2$	$2x+1$	x	1