Fall 2015
Algebra Qualfying Exam Solutions

Hannah Hoganson, Allechar Serrano

August 5, 2016

In the problems below, K denotes a field; $\mathbb{F}_q$ denotes the field with q elements; P_p a Sylow p-subgroup and n_p denotes the number of Sylow p subgroups.

1. Determine, up to isomorphism, the groups of order 44.

   Note: *The internet tells us that there are four groups of order 44 up to isomorphism, but we seem to have a valid argument that there are actually five. We assume two of the groups in solution 1 must be isomorphic, but we don't know which, and we don't know why. If you can clarify this, please let us know.*

   Solution 1: Let G be a group of order 44, the Sylow theorems tell us that G has subgroups of orders 2^2 and 11. We also know that $n_p|[G : P_p]$ and $n_p \equiv 1 \bmod p$. Thus $n_{11} = 1$ and P_{11} has no connugate subgroups so is normal in G. Let P_2 be a sylow 2-subgroup, then by reasons of degree $P_{11} \cap P_1 = \{1\}$ so $P_{11}P_2 \leq G$ with $|P_{11}P_2|44$. Thus $P_{11}P_2 = G$ and we can write $G = P_{11} \rtimes_\varphi P_2$ where $\varphi : P_2 \to \text{Aut}(P_{11})$. To determine the possible actions from φ note that $\text{Aut}(P_{11}) = \text{Aut}(\mathbb{Z}/11\mathbb{Z}) \cong \mathbb{Z}/10\mathbb{Z}$ and $P_2 \cong Z/4\mathbb{Z}$ or $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

   <u>Case 1:</u> $P_2 \cong \mathbb{Z}/4\mathbb{Z}$ then we can think of φ as a homomorphism from $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$. Such a homomorphism is determined by where it maps the generator, and because 1 has order 4, $\varphi(1)$ must have order dividing 4. Thus $\varphi(1) \in \{1, 5\}$. If $\varphi(1) = 1$ then $\varphi = id$ and $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \cong \mathbb{Z}/44\mathbb{Z}$. If $\varphi(1) = 5$ then $G \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/11\mathbb{Z}$.

   <u>Case 2:</u> $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ and is determined by $\varphi((1, 0))$ and $\varphi((0, 1))$, which both must be 1 or 5. If both generators map to 1 then $\varphi = id$ and $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/22\mathbb{Z}$, and this is the other abelian case.

   Next consider the homomorphisms

   $$\varphi_1 : \begin{cases} (1,0) \to 1 \\ (0,1) \to 5 \end{cases} \quad , \quad \varphi_2 : \begin{cases} (1,0) \to 5 \\ (0,1) \to 1 \end{cases}$$

   resulting in the groups $G_1 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_{\varphi_1} \mathbb{Z}/11\mathbb{Z}$ and $G_2 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_{\varphi_2} \mathbb{Z}/11\mathbb{Z}$. Then G_1 and G_2 are isomorphic by $\Psi : G_1 \to G_2$ where $\Psi = \psi \times id_{\mathbb{Z}/11\mathbb{Z}}$ and

   $$\begin{aligned} \psi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ (1,0) &\longmapsto (0,1) \\ (0,1) &\longmapsto (1,0) \end{aligned}$$

   The last possibility is

   $$\varphi_3 : \begin{cases} (1,0) \to 5 \\ (0,1) \to 5 \end{cases}$$

resulting in $G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_{\varphi_3} \mathbb{Z}/11\mathbb{Z}$.

Note that groups in case 1 have an element of order 4 while groups found in case 2 do not, so there are no isomorphisms between these groups, and we have found that there are *at most* five groups of order 44 up to isomorphism.

Note: Tables of finite groups online list only 4 groups of order 44 but it is unclear which two of the groups found above are actually isomorphic.

Solution 2: Let G be a group of order 44. By Sylow theorems, the Sylow 11−subgroup is normal in G. We have that $P_{11}P_2$ is a subgroup of G and $P_{11} \cap P_2 = \{1\}$, hence $|G| = |P_{11}P_2|$. So we have that $G = P_{11} \rtimes_\varphi P_2$ where $\varphi : P_2 \to \mathrm{Aut}(\mathbb{Z}_{11})$ and P_2 is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Let $g \in P_2$ be nontrivial, then g has order 1, 2, or 4 under φ and there are 4 such maps. Hence G is isomorphic to either $\mathbb{Z}_{11} \times \mathbb{Z}_4, \mathbb{Z}_{11} \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_{11} \rtimes \mathbb{Z}_4$, or $\mathbb{Z}_{11} \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$.

2. Prove that there is no simple group of order 192.

   Solution: Let G be a group of order $192 = 2^6 \times 3$. Let n_p be the number of Sylow p−subgroups of G. By Sylow theorems, $n_2 \in \{1, 3\}$ and $n_3 \in \{1, 4, 16, 64\}$. Suppose $n_2, n_3 \neq 1$. Then, the number of nontrivial elements in the Sylow 3−subgroups and in the Sylow 2−subgroups is $4(3-1) = 8$ and $3(64-1) = 189$. Then the number of elements in G must be at least 197, a contradiction. Therefore, G is not simple.

3. Let $R = \mathbb{Q}[x, y]$ and let $I = \langle x, y \rangle$. Compute the vector rank space of $\mathrm{Ext}^1_R(I, R)$ over $\mathbb{Q}$.

   Solution: Homological algebra was not covered in the Fall 2015 - Spring 2016 Algebra sequence, so we assume this material will not appear on the Fall 2016 qualifying exam.

4. Let M be a 3×3 complex matrix with $M^6 = M^4$ and $M^4 + M^2 = 3M^3$. Determine the possible Jordan forms of M.

   Solution: M satisfies the polynomials $x^6 - x^4 = x^4(x-1)(x+1)$ and $x^4 - 2x^3 + x^2 = x^2(x-1)^2$. Therefore, the factor x can appear at most twice and the factor $x - 1$ can appear at most once in the factorization of the minimal polynomial. We have the following possibilities

Minimal polynomial	Characteristic polynomial	Jordan form
x	x^3	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
$x-1$	$(x-1)^3$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
x^2	x^3	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$
$x(x-1)$	$x^2(x-1)$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
	$x(x-1)^2$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
$x^2(x-1)$	$x^2(x-1)$	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

5. (a) List the prime ideals of the ring $R = \mathbb{Z}[x, y]/\langle 3 + x, y(y-1) + x^2, x\rangle$.
   (b) Give an example of an integral domain with exactly two prime ideals.

Solution: (i) We can first observe that

$$R = \mathbb{Z}[x, y]/\langle 3 + x, y(y-1) + x^2, x\rangle \cong \mathbb{Z}[y]/\langle 3, y(y-1)\rangle \cong \mathbb{Z}_3[y]/\langle y(y-1)\rangle.$$

We have a one-to-one correspondence between

$$\text{Prime Ideals in } R \longleftrightarrow \text{Prime Ideals in } \mathbb{Z}_3[y] \text{ containing } y(y-1).$$

An ideal is prime in $\mathbb{Z}_3[y]$ if and only if it is generated by an irreducible polynomial, if it also contains the ideal generated by $y(y-1)$ there are only two possibilities: (y) and $(y-1)$. Thus, there are two prime ideals in R and they are the ideals generated by $(\overline{y})$ and $(\overline{y-1})$.

(ii) Consider the localization of $\mathbb{Z}$ at some prime, say $p = 3$:

$$\mathbb{Z}_{(3)} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, 3 \nmid b\right\}$$

$\mathbb{Z}_{(3)}$ has exactly two prime ideals: the ideals generated by (3) (which is the only non-invertible prime left) and the zero ideal. One could also use the one-to-one correspondence of ideals in a ring and its localization (Not covered Fall 15-Spring 16).

6. Suppose that $R = \mathbb{Z}[i]$ is the Gaussian integers. Let M and N be finitely generated $R-$modules such that

$$M \oplus R^{\oplus 2} \oplus R/(2) \cong N \oplus R \oplus R/(1+i) \oplus R \oplus R/(1-i)$$

Is it true that $M \cong N$?

Note: *This material was not covered in the 2015-2016 algebra sequence.*

Solution: We know that $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}_2 \cong \mathbb{Z}[i]/(1-i)$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \ncong \mathbb{Z}[i]/(2) \cong \mathbb{Z}_4$, hence $M \ncong N$.

7. Prove that $\mathbb{F} = \mathbb{Z}[t]/\langle 3, t^3 - t^2 + 1\rangle$ is a field. Find the number of solutions of $x^{13} + 1 = 0$ in $\mathbb{F}$, and also the number of solutions of $x^{13} - 1 = 0$ in $\mathbb{F}$.

Solution:

$$\mathbb{F} = \mathbb{Z}[t]/\langle 3, t^3 - t^2 + 1\rangle \cong \mathbb{F}_3[t]/\langle t^3 - t^2 + 1\rangle$$

Let $g(t) = t^3 - t^2 + 1$ and note that g has no roots in $\mathbb{F}_3$. Thus g has no linear factors in $\mathbb{F}_3[t]$ and because g is degree 3 it does not factor in $\mathbb{F}_3[t]$. So, g is an irreducible polynomial and $\langle t^3 - t^2 + 1\rangle$ is a maximal ideal, so $\mathbb{F} = \mathbb{F}_3[t]/\langle t^3 - t^2 + 1\rangle$ is a field.

Because $\{1, t, t^2\}$ form a basis for $\mathbb{F}$ over $\mathbb{F}_3$ we have $[\mathbb{F} : \mathbb{F}_3] = 3$ so $\mathbb{F} \cong \mathbb{F}_{27}$. Now let K be a splitting field for $x^{13} + 1$ over $\mathbb{F}$. Because $\mathbb{F} \subseteq K$ is a finite extension of finite fields the extension is Galois with $\text{Gal}(K/\mathbb{F})$ generated by $\varphi_{27} : x \longmapsto x^{27}$. Let ζ be any root of $x^{13} + 1$, then

$$\varphi_{27}(\zeta) = \zeta^{27} = (\zeta^{13})^2\zeta = (-1)^2\zeta = \zeta$$

so $\varphi = id$ and $K = \mathbb{F}$ and all 13 solutions of $x^{13} + 1 = 0$ live in $\mathbb{F}$.

Now let E be the splitting field of $x^{13} - 1$ over $\mathbb{F}$. Again this extension is Galois with Galois group generated by φ_{27}. Let ξ be any root of $x^{13} - 1$, then

$$\varphi_{27}(\xi) = \xi^{27} = \xi$$

so again $\varphi = id$ and $\mathbb{F} = E$ so all 13 solutions of $x^{13} - 1$ live in $\mathbb{F}$.

8. Compute the Galois group of $x^4 - 2$ over $\mathbb{Q}$.

   Solution: $x^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 2$. The roots of $f(x) = x^4 - 2$ are $\{\pm 2^{\frac{1}{4}}, \pm i2^{\frac{1}{4}}\}$ so the splitting field of f is $\mathbb{Q}(2^{\frac{1}{4}}, i)$ and the minimal polynomial of i over $\mathbb{Q}(2^{\frac{1}{4}})$ is $x^2 + 1$, so

   $$[\mathbb{Q}(2^{\frac{1}{4}}, i) : \mathbb{Q}] = [\mathbb{Q}(2^{\frac{1}{4}}, i) : \mathbb{Q}(2^{\frac{1}{4}})][\mathbb{Q}(2^{\frac{1}{4}} : \mathbb{Q}] = 2 \cdot 4 = 8$$

   So, $|\text{Gal}(f)| = 8$ and because $\mathbb{Q}(2^{\frac{1}{4}})$ is an intermediate field which is not Galois (because $2^{\frac{1}{4}}$ has minimal polynomial f which does not split over $\mathbb{Q}(2^{\frac{1}{4}})$), $\text{Gal}(f)$ has a non-normal subgroup and is not abelian. We also know that $\text{Gal}(f) \leq S_4$ so it must be that $\text{Gal}(f) \cong D_8$.

9. Let E be the splitting field of $f(x) = x^{14} + 1$ over $\mathbb{F}_2$, and let K be the splitting field $g(x) = x^{21} + 1$ over $\mathbb{F}_2$. Prove that K contains an isomorphic copy of E, and compute the extension degree of K over E.

   Solution: First note that over $\mathbb{F}_2$, $f(x) = x^{14} - 1 = (x^7 - 1)^2$ and $g(x) = x^{21} - 1 = (x^7 - 1)(x^{14} + x^7 + 1)$. So E is the splitting field of $x^7 - 1$ which divides $g(x)$ so $E \subseteq K$.

   Because K, E are finite extensions of $\mathbb{F}_2$ and finite fields of the same size are isomorphic we have $E \cong \mathbb{F}_{2^m}$ and $K \cong \mathbb{F}_{2^n}$ with $m \leq n$. Both $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$ are Galois extensions of $\mathbb{F}_2$ and both Galois groups are generated by $\varphi_2 : x \longmapsto x^2$. We want to know the extension degree of K over E so we will calculate both of their extension degrees over $\mathbb{F}_2$.

   $E \supseteq \mathbb{F}$: Let ζ be a 7th root of unity (a root of f), then

   $$\varphi_2 : \zeta \longmapsto \zeta^2 \longmapsto \zeta^4 \longmapsto \zeta^8 = \zeta$$

   so φ_2 acts with order 3, so $|\text{Gal}(E/\mathbb{F})| = 3$ and $[E : \mathbb{F}_2] = 3$.

   $K \supset \mathbb{F}$: Let ξ be a 21st root of unity (a root of g), then

   $$\varphi_2 : \xi \longmapsto \xi^2 \longmapsto \xi^4 \longmapsto \xi^8 \longmapsto \xi^{16} \longmapsto \xi^{32} = \xi^{11} \longmapsto \xi^{22} = \xi$$

   so $[K : \mathbb{F}_2] = 6$ and thus $[K : E] = 2$.

10. Let $f(x)$ be a degree 5 polynomial in $\mathbb{Q}[x]$ that is not solvable by radicals. Let L be its splitting field over $\mathbb{Q}$.

    (i) Prove that there is at most one field K with $\mathbb{Q} \subset K \subset L$ and $[K : \mathbb{Q}] = 2$.

    (ii) If α, β are irrational elements in L such that α^2 and β^2 are rational, prove that $\alpha\beta$ is rational.

    Solution: We didn't have time to work on this problem. If someone decides to write up a solution, please email it to Anna and she'll update this.