Spring 2013
Algebra Qualfying Exam Solutions

Hannah Hoganson, Shelby Kilmer, Anna Romanova, Allechar Serrano

August 5, 2016

In the problems below, K denotes a field; $\mathbb{F}_p$ denotes the field with p elements.

1. Determine the number of Sylow p-subgroups of $GL_2(\mathbb{F}_p)$.

   Solution: First we count the number of elements in $GL_2(\mathbb{F}_p)$. There are p^4 total 2×2 matrices with entries in $\mathbb{F}_p$. A matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is linearly dependent iff $ad - bc = 0$. We count the number of linearly dependent matrices:

   - If $a \neq 0$ then $d = \frac{bc}{a}$ so there are $p^2(p-1)$ matrices of this type.
   - If $a = 0$ then d is free but we must have $bc = 0$.
     - If $b = 0$ then c is also free and there are p^2 matrices of this type.
     - If $b \neq 0$ then $c = 0$ and there are $p(p-1)$ matrices of this type.

   So the total number of linearly dependent matrices is $p^2(p-1) + p^2 + p(p-1) = p^3 + p^2 - p$, and

   $$|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p = p(p-1)^2(p+1)$$

   Now we can move on to the Sylow theory. We know $GL_2(\mathbb{F}_p)$ has a p-Sylow subgroup and that $n_p \mid (p-1)^2(p+1)$ and $n_p \equiv 1 (\bmod p)$. So,

   $$n_p \in \{1, p+1, (p-1)^2, (p-1)^2(p+1)\}$$

   Note that

   $$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

   So, $P = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$ is a p-group and so is $\left\langle \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\rangle$, so $n_p > 1$. We also know that $n_p = [G : N(P)]$ where $N(P)$ is the normalizer of P in G. Note that if $a, d \neq 0$ then

   $$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \cdot \frac{1}{ad} \begin{bmatrix} d & -b \\ 0 & a \end{bmatrix} = \begin{bmatrix} 1 & \frac{ar}{d} \\ 0 & 1 \end{bmatrix} \in \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$$

   So, every matrix of this form is in $N(P)$ and there are $p(p-1)^2$ of them. Thus,

   $$[G : N(P)] = \frac{|G|}{|N(P)|} \leq \frac{p(p-1)^2(p+1)}{p(p-1)^2} = p + 1$$

   and $n_p = p + 1$.

2. Show that $(\mathbb{Q}/\mathbb{Z}, +)$ has one and only one subgroup of order n, for each integer $n \geq 1$, and that this subgroup is cyclic.

Solution: Let $H = \{0 + \mathbb{Z}, 1/n + \mathbb{Z}, 2/n + \mathbb{Z}, \ldots, (n-1)/n + \mathbb{Z}\}$. Then $H = \langle 1/n + \mathbb{Z} \rangle$ has order n. Indeed, $k/n + \mathbb{Z} \in H$ can be expressed as $1/n + \cdots + 1/n = k(1/n)$ and $1/n + \cdots + 1/n = 1 = 0 + \mathbb{Z}$.

We are left to show that this is only subgroups of order n, so let H^* be some other subgroups of order n. We proved earlier that any $H^* \leq \mathbb{Q}/\mathbb{Z}$ which is finitely generated is cyclic, so we can express $H^* = \langle a/b + \mathbb{Z} \rangle$. Assume without loss of generality that a/b is fully reduced. Since H has order n, we know $n(a/b) + \mathbb{Z} = 0 + \mathbb{Z}$, and so $n(a/b) \in \mathbb{Z}$. Thus, $n = bk$ for some integer k. Further, for any $m < n$, $m(a/b) \notin \mathbb{Z}$ (b does not divide m). We can conclude $b = n$.

So, we have $H^* = \langle a/n + \mathbb{Z} \rangle$. Note $a/n \in H$, so $H^* \subset H$. But $|H| = |H^*| = n$, so we conclude $H = H^*$ and we are done.

3. Determine representatives for the conjugacy classes in $GL_3(\mathbb{F}_2)$.

Solution: We have the following possibilities for minimal polynomial, characteristic polynomial and rational canonical form

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

4. Let R be a commutative ring with $1 \neq 0$. Recall that the nilradical of R is the ideal $N(R) = \{x \in R : x^n = 0 \text{ for some positive integer } n\}$ Prove that the following are equivalent:

(i) R has exactly one prime ideal;

(ii) $R/N(R)$ is a field.

Solution: We assume the fact that the Nilradical of a ring is the intersection of all prime ideals.

(i) $\Rightarrow$ (ii) Because the Nilradical of a ring is the intersection of all prime ideals it is itself a prime ideal. We know that every maximal ideal of a ring is prime and every ring contains

a maximal ideal, so $N(R)$ must be the prime and maximal ideal. We also know that a commutative ring modulo a maximal ideal is a field.

(ii) $\Rightarrow$ (i) If $R/N(R)$ is a field then $N(R)$ is a maximal ideal. Because $N(R) = \bigcap_{I \text{ prime}} I$ it must be that there is only one distinct prime ideal, otherwise $N(R)$ would be a proper subset of each, contradicting maximality.

5. If I, J are ideals in the commutative ring R, prove that $R/I \otimes_R R/J \cong R/(I+J)$, as R-modules.

Solution: *Tensor products were not covered in the fall 2015 - spring 2016 Algebra qualifying exam sequence, so we don't anticipate them showing up on the Fall 2016 qualifying exam. But we include a solution to this problem for fun.*

First note that we can put a standard form on $R/I \otimes_R R/J$: every element can be written as $(1+I) \otimes (r+J)$ for some $r \in R$ because

$$(a+I) \otimes (b+J) = a(1+I) \otimes (b+J) = (1+I) \otimes a(b+J) = (1+I) \otimes (ab+J)$$

Define

$$\begin{aligned} \varphi : R/I \times R/J &\to R/(I+J) \\ (a+I, b+J) &\longmapsto (ab) + (I+J) \end{aligned}$$

Then φ is well defined because if $a_1 - a_2 \in I$ and $b_1 - b_2 \in J$ then

$$\begin{aligned} \varphi(a_1+I, b_1+J) &= a_1 b_1 + (I+J) \\ &= b_1(a_1 - a_2) + a_2(b_1 - b_2) + a_2 b_2 + (I+J) \\ &= a_2 b_2 + (I+J) = \varphi(a_2+I, b_2+J) \end{aligned}$$

φ is also R-balanced because for $r \in R$:

$$\begin{aligned} \varphi(a+I, (b_1+b_2)+J) &= (ab_1 + ab_2) + (I+J) = \varphi(a+I, b_1+J) + \varphi(a+I, b_2+J) \\ \varphi((a_1+a_2)+I, b+J) &= (a_1 b + a_2 b) + (I+J) = \varphi(a_1+I, b+J) + \varphi(a_2+I, b+J) \\ \varphi((a+I)r, b+J) &= arb + (I+J) = \varphi(a+I, r(b+J)) \end{aligned}$$

So, φ induces an R-module homomorphism $\Phi : R/I \otimes_R R/J \to R/(I+J)$. Φ is surjective because for any $r \in R$,

$$r + (I+J) = \Phi((1+I) \otimes (r+J)$$

and Φ is injective because if $\Phi((1+I) \otimes (a+J)) = I+J$ then $a \in I+J$ so we can write $a = r+s$ with $r \in I$ and $s \in J$.

$$\begin{aligned} (1+I) \otimes (a+J) &= (1+I) \otimes (r+s+J) = (1+I) \otimes (r+J) \\ &= (r+I) \otimes (1+J) = \overline{0} \otimes (1+J) = \overline{0} \end{aligned}$$

so Φ is an R-module isomorphism between $R/I \otimes_R R/J$ and $R/(I+J)$.

6. In the category of $\mathbb{Z}$-modules: (a) Is $\mathbb{Z}$ injective? (b) Is $\mathbb{Z}/8\mathbb{Z}$ projective?

Solution: This material was not covered in the fall 2015 - spring 2016 algebra qualifying exam sequence so we do not anticipate it showing up on the fall 2016 qualifying exam.

7. Show that if p is an odd prime, the polynomial $x^{p^n} - x + 1$ is irreducible over $\mathbb{F}_p$ only when $n = 1$.

   Recall:

   - Every finite extension of a finite field is Galois.

     If $E \subseteq F$ are finite fields then $E = \mathbb{F}_{p^n}$ and $F = \mathbb{F}_{p^{nm}}$. Because $\mathbb{F}_{p^{nm}}$ is Galois over $\mathbb{F}_p$ (it is the splitting field of $x^{p^{nm}} - x$ which has distinct roots), it is also Galois over $\mathbb{F}_{p^n}$.

   - The Galois group of an extension $\mathbb{F}_{p^n} \subseteq E$ is generated by the automorphism φ_{p^n} defined by $\varphi_{p^n}(x) = x^{p^n}$.

     Pf: We know that $E = \mathbb{F}_{p^{nm}}$ for some m and $\mathrm{Gal}(\mathbb{F}_{p^{nm}}/\mathbb{F}_p) = \langle \varphi_p \rangle \cong \mathbb{Z}/(mn)\mathbb{Z}$. Because $\mathrm{Gal}(\mathbb{F}_{p^{nm}}/\mathbb{F}_{p^n})$ is a subgroup it is also cyclic generated by φ_p^k for some k, and by reasons of degree has order m. Because φ_p^n has order m and fixes $\mathbb{F}_{p^n}$ it must be that
     $$\mathrm{Gal}(\mathbb{F}_{p^{nm}}/\mathbb{F}_{p^n}) = \langle \varphi_p^n \rangle = \langle \varphi_{p^n} \rangle$$

   Solution: Assume f is irreducible with a root α. Then f is the minimal polynomial of α so $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = p^n$. Because $\mathbb{F}_p \subset \mathbb{F}_p(\alpha)$ is a finite extension of finite fields it is Galois, i.e. the extension is Normal and seperable. Thus, all roots of f live in $\mathbb{F}_p(\alpha)$.

   Now note that for all $b \in \mathbb{F}_{p^n}$, $\alpha + b$ is a root of f because $b^{p^n} = b$ so

   $$(\alpha + b)^{p^n} - (\alpha + b) + 1 = \alpha^{p^n} + b^{p^n} - \alpha - b + 1 = \alpha^{p^n} - \alpha + 1 = 0$$

   Thus, $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p(\alpha)$, and as a finite extension of finite fields is Galois. The Galois group is generated by φ_{p^n} and $\varphi_{p^n}(\alpha) = \alpha^{p^n} = \alpha - 1$. So, the orbit of α is

   $$\{\alpha - j \mid 0 \leq j \leq p - 1\}$$

   and $[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] = |\mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_{p^n}| = p$.

   We get the following tower of fields:

   $$\begin{array}{c} \mathbb{F}_p(\alpha) \\ p \,\big|\, \\ \mathbb{F}_{p^n} \\ n \,\big|\, \\ \mathbb{F}_p \end{array}$$

   Where $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = p^n$, so $np = p^n$ and because $p \neq 2$ it must be that $n = 1$.

8. Show that $f(x) = x^4 + 4x^2 + 2$ is irreducible over $\mathbb{Q}$, and find its Galois group over $\mathbb{Q}$.

   Solution: The polynomial is irreducible by Eisentein's criteria because 2 divides all the (non-leading) coefficients and 2^2 does not the constant term.

   Over $\mathbb{C}$ f has roots $\{\sqrt{-2+\sqrt{2}}, -\sqrt{-2+\sqrt{2}}, \sqrt{-2-\sqrt{2}}, -\sqrt{-2-\sqrt{2}}\}$, all of which are purely imaginary. Note that

- $(\sqrt{-2+\sqrt{2}})^2 = -2+\sqrt{2}$ so $\sqrt{2} \in \mathbb{Q}(\sqrt{-2+\sqrt{2}})$
- $\left(\sqrt{-2+\sqrt{2}}\right)\left(\sqrt{-2-\sqrt{2}}\right) = \sqrt{2}$ so $\sqrt{-2-\sqrt{2}} \in \mathbb{Q}(\sqrt{-2+\sqrt{2}})$

So, the splitting field of f is $\mathbb{Q}(\sqrt{-2+\sqrt{2}})$ and $[\mathbb{Q}(\sqrt{-2+\sqrt{2}}) : \mathbb{Q}] = 4$. So the Galois group is either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $\sigma \in \mathrm{Gal}(f)$ be the element which maps $\sqrt{-2+\sqrt{2}} \longmapsto \sqrt{-2-\sqrt{2}}$. Then

$$\sigma(\sqrt{2}) = \sigma(\sqrt{-2+\sqrt{2}})^2 = -2-\sqrt{2}$$

So,

$$\begin{aligned}\sigma^2\left(\sqrt{-2+\sqrt{2}}\right) &= \sigma\left(\sqrt{-2-\sqrt{2}}\right) \\ &= \sigma\left(\frac{\sqrt{2}}{\sqrt{-2+\sqrt{2}}}\right) \\ &= \frac{-2-\sqrt{2}}{\sqrt{-2-\sqrt{2}}} = \sqrt{-2-\sqrt{2}}\end{aligned}$$

So, $\sigma^2 \neq id$ and it must be that $\mathrm{Gal}(f) = \mathbb{Z}/4\mathbb{Z}$.

9. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree $n \geq 4$ and let K be a splitting field of f over $\mathbb{Q}$. Suppose that $\mathrm{Gal}(K/\mathbb{Q})$ is the symmetric group S_n. If $\alpha \in K$ is a root of $f(x)$, show that $\alpha^n \notin \mathbb{Q}$.

Solution: Suppose that $\alpha^n \in \mathbb{Q}$. Then for all $\sigma \in S_n$,

$$(\sigma(\alpha))^n = \sigma(\alpha^n) = \alpha^n,$$

so $\sigma(\alpha) = \xi_n \alpha$, where ξ_n is an nth root of unity. Since the Galois group is S_n, it acts transitively on the roots of $f(x)$. This implies that all roots have the form $\xi_n^m \alpha$ for some $1 \leq m \leq n$. Thus, $K = \mathbb{Q}(\xi_n, \alpha)$. We know that $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n) \leq n-1$, and since $\alpha^n \in \mathbb{Q}$, $[\mathbb{Q}(\xi_n)(\alpha) : \mathbb{Q}(\xi_n)] \leq n$. Therefore,

$$n! = |S_n| = [K : \mathbb{Q}] \leq n(n-1),$$

which implies that $n = 3$ or $n = 2$, which contradicts the assumption that $n \geq 4$. So $\alpha^n \notin \mathbb{Q}$.

10. Let A be a real $n \times n$ matrix. We say that A is a difference of two squares if there exist real $n \times n$ matrices B and C with $BC = CB = 0$ and $A = B^2 - C^2$.

(a) If A is a diagonal matrix, show that it is a difference of two squares.

(b) If A is a symmetric matrix that is not necessarily diagonal, again show that it is a difference of two squares.

(c) Suppose A is a difference of two squares, with corresponding matrices B and C as above. If B has a nonzero real eigenvalue, prove that A has a positive real eigenvalue.

Solution: a) We can conjugate A so that $MAM^{-1} = \begin{pmatrix} p_1 & & & & & \\ & \ddots & & & & \\ & & p_k & & & \\ & & & m_{k+1} & & \\ & & & & \ddots & \\ & & & & & m_n \end{pmatrix}$

where $p_1, \ldots, p_k \geq 0$ and $m_{k+1}, \ldots, m_n < 0$.

If we let $B = \begin{pmatrix} \sqrt{p_1} & & & & & \\ & \ddots & & & & \\ & & \sqrt{p_k} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$ and $C = \begin{pmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & \sqrt{|m_{k+1}|} & & \\ & & & & \ddots & \\ & & & & & \sqrt{|m_n|} \end{pmatrix}$,
then $MAM^{-1} = B^2 - C^2$ and $A = (M^{-1}BM)^2 - (M^{-1}CM)^2$. Further, $BC = CB = 0$.

b) Symmetric matrices are diagonalizable. So, $MAM^{-1} = D = B^2 - C^2$ by part a. And so $A = (M^{-1}BM)^2 - (M^{-1}CM)^2$.

c) Let λ be the nonzero eigenvalue Then $Bv = \lambda v$, and $Av = B^2v - C^2v = \lambda^2 v - C^2 v$. I claim $C^2v = 0$. Indeed, $0 = CBv = \lambda Cv$, and so $Cv = 0$. Thus, $\lambda^2 > 0$ is an eigenvalue for A.