August 2009
Algebra Qualfying Exam Solutions

Hannah Hoganson, Shelby Kilmer, Allechar Serrano

June 16, 2016

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

1: Compute the number of elements of order 4 in the symmetric gorup S_7.

Solution: Elements whose order divides 4 have cycle types made up of 4, 2 and 1 cycles. An element will have order 4 if it's cycle type contains a 4-cycle. So the possible cycle types of an element of order 4 are a single 4 cycle or a 4 cycle and a 2 cycle. There are $\frac{7\cdot6\cdot5\cdot4}{4} = 210$ different 4 cycles in S_7, and so there are $210 \cdot \frac{3\cdot2}{2} = 630$ elements that are a 4 cycle and a 2 cycle. Thus, there are 840 elements of order 4 in S_7.

2: Let G be a group of order p^n where p is a prime number and $n > 0$ is an integer. Prove that the center of G is nontrivial.

Solution: If G is abelian then we are done so assume G is not abelian. Let $Z(G)$ be the center of G, then the class equation says

$$|G| = |Z(G)| + \sum [G : C_G(x_i)]$$

where the sum is taken over representatives of distinct conjugacy classes not in the center. Because each $C_g(x_i) \neq G$ we get that $[G : C_g(x_i)] \neq 1$ and so p divides the sum $\sum [G : C_G(x_i)]$. Because p also divides $|G|$ we get that p divides $|Z(G)|$ so the center of G is nontrivial.

3: Let $E \subseteq F$ be a finite Galois extension of fields. Suppose that there is an element α in F such that $\alpha \notin E$ and such that α is in every proper extension of E contained in F. Show that the Galois group of F over E is cyclic of prime power order.

Solution: We utilize the Galois correspondence to show G is cyclic. Since $\alpha \in E'$ for all $E \subset E' \subset F$, all proper subgroups of G fix α, and $H = \mathrm{Gal}(F/E(\alpha))$ contains all proper subgroups of G.

Consider $\sigma \in G/H$. If $G \neq \langle\sigma\rangle$, then $\langle\sigma\rangle \subset H$. But this contradicts our choice of σ, and we conclude G is cyclic.

Now we show G is of prime power order. Suppose to the contrary that $|G| = nm$ where $(n, m) = 1$. Then,

$$G \cong \mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},$$

and thus G has subgroups $H_1 \cong \mathbb{Z}/n\mathbb{Z}$ and $H_2 \cong \mathbb{Z}/m\mathbb{Z}$ where $H_1 \cap H_2 = \emptyset$. By the above, $H_1 \leq H$ and $H_2 \leq H$ which implies $G = H_1H_2 \leq H$. But then $G = H$, a contradiction.

4: Show that every finitely generated subgroup of $\mathbb{Q}/\mathbb{Z}$ is cyclic.

Solution: The elements of $\mathbb{Q}/\mathbb{Z}$ are of the form $\frac{m}{n} + \mathbb{Z}$ where m, n are integers and $n \neq 0$. Let S be a finitely generated subgroup of $\mathbb{Q}/\mathbb{Z}$, then there exist a finite number of elements in $\mathbb{Q}/\mathbb{Z}$ such that $S = \left\langle \frac{m_1}{n_1} + \mathbb{Z}, \frac{n_2}{m_2} + \mathbb{Z}, \ldots, \frac{m_k}{n_k} + \mathbb{Z} \right\rangle$. Let N be the least common multiple of $n_1, \ldots, n_k$. Then we have that $S = \langle \frac{1}{N} + \mathbb{Z} \rangle$, so S is cyclic.

5: Show that there are no simple groups of order 520.

Solution: Let G be a group of order 520. $520 = 2^3 \cdot 5 \cdot 13$ so from the Sylow theorems we know that G has a subgroup of order 5 and a subgroup of order 13. We also know that the number of Sylow p subgroups is congruent to 1 modulo p and divides the index of the subgroup. A subgroup of order 5 has index 104 and a subgroup of order 13 has index 40; so $n_5 \in \{1, 26\}$ and $n_{13} \in \{1, 40\}$. Say there was only one p-subgroup for some $p \mid 520$, call it H. Then for any $g \in G$ gHg^{-1} is also a p-subgroup, so it must be that $gHg^{-1} = H$ and H is normal so G is not simple. Thus, if G is simple then there are 26 nonoverlapping subgroups of order 5 and 40 nonoverlapping subgroups of order 13. Note that the subgroups of order 5 only overlap with the subgroups of order 13 at the identity (because the order of all other elements is 5 and 13 repectively). So there are at least $1 + 104 + 480 = 621$ elements in G, a contradiction.

6: Let M be a matrix with real coefficients such that $M^2 + M + I = 0$. Give

the possible canonical forms for M

(a) Over the real numbers $\mathbb{R}$ (rational canonical form)

(b) Over the complex numbers $\mathbb{C}$ (Jordan canonical form)

Solution:

(a) Since the minimal polynomial of M is x^2+x+1, the companion matrix associated to the minimal polynomial is

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

Hence, the rational form of M has blocks of this companion matrix.

(b) Since we can factor $x^2 + x + 1 = \left(x + \frac{1+i\sqrt{3}}{2}\right)\left(x + \frac{1-i\sqrt{3}}{2}\right)$, then the Jordan canonical form of M can have blocks of $\text{diag}\left\{\frac{-1-i\sqrt{3}}{2}, \frac{-1+i\sqrt{3}}{2}\right\}$ and either blocks of $\frac{-1-i\sqrt{3}}{2}$ or $\frac{-1+i\sqrt{3}}{2}$, or just blocks of size 1 of $\frac{-1\pm i\sqrt{3}}{2}$

7: Let R be a commutative ring, and let S be a multiplicative subset of R ($1 \in S$, and if s and t are in S, then st is in S). Show that an ideal I that is maximal with the property the $S \cap I = \emptyset$ is prime.

Solution: Suppose $ab \in I$ and I is not prime. Then $a, b \notin I$. Therefore, the ideal (I, a) is strictly larger than I, so $(I, a) \cap S \neq \emptyset$. Then there exists $s_a \in S$ such that $s_a = i + ra$ for $i \in I, r \in R$. Similarly, there exists $s_b = j + tb$ for $j \in I, t \in R$. We have that $i, j, ab \in I$, so $s_a s_b = (i + ra)(j + tb) \in I \cap S$, a contradiction.

8: Determine for which integers q the polynomial $x^3 + 1$ has three distinct roots in the field with q elements.

Solution: First note that 0 is never a root of $f(x) = x^3 + 1$ so any roots of f live in $(\mathbb{F}_q)^x \cong \mathbb{Z}/(q-1)\mathbb{Z}$. If an element a satisfies $a^3 + 1 = 0$ then $a^3 = -1$ and $a^6 = 1$, so either a has order 6 or $a = -1$. $\mathbb{Z}/(q-1)\mathbb{Z}$ has elements of order 6 iff 6 divides $q - 1$ iff $q \equiv 1 \pmod 6$. In this case there are $\phi(6) = (2-1)(3-1) = 2$ elements of order 6 and these along with -1 make up the 3 distinct roots of $f(x)$.

9: Show that there exists a Galois extension of the field $\mathbb{Q}$ of rational numbers with Galois group $\mathbb{Z}\backslash 5\mathbb{Z}$.

Solution: Let $\zeta_{11} = e^{\frac{2\pi i}{11}}$, then we know the minimal polynomial of ζ_{11} is $\Phi_{11}(x) = x^{10} + x^9 + ... + x + 1$ and the Galois group of $\mathbb{Q}(\zeta_{11})/\mathbb{Q}$ is $\mathbb{Z}/10\mathbb{Z}$. Then $\mathbb{Z}/2\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}/10\mathbb{Z}$ (because abelian). The fundamental theorem of Glaois theory tells us there is an intermediate normal field extension, so Galois, with Galois group $(\mathbb{Z}/10\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$.

10: State and prove the Eisenstein Irreducibility Criterion.

Solution: Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there exists a prime p such that $p|a_i$ for all $i \in n-1, \ldots, 1$, $p \nmid a_n$, and $p^2 \nmid a_0$, then $P(x)$ is irreducible in $\mathbb{Q}$.

Proof: Suppose $P(x)$ is reducible and we have nonconstant polynomials such that $P(x) = R(x)Q(x)$. Let $\overline{P(x)}$ denote $P(x)$ reduced mod p. We have that $\overline{P(x)} = a^n x^n = \overline{R(x)Q(x)}$, hence the constant terms of R and Q are divisible by p, so the constant term of P is divisible by p^2, a contradiction.