Swarthmore College
Department of Mathematics and Statistics
Honors Examination: Algebra
Spring 2006

Instructions: This exam contains eleven problems. Try to solve six problems as completely as possible. Do not be concerned if some problems are unfamiliar; you have a lot of choice so that one exam can cover several syllabi. Once you are satisfied with your answers to your six problems, make a second pass through the exam and complete as many parts of the remaining problems as possible. I am interested in your thoughts on a problem even if you do not completely solve it. In particular, turn in your solution even if you can't do all the parts of a multiple part problem. You might also formulate and solve special cases if you cannot solve a problem in the most general case. When there are multiple parts to a problem, you can answer a later part without solving all the earlier ones.

1. A commutative ring A is called a *local ring* if it has a unique maximal ideal $\mathfrak{m}$.

(a) Show that if A is a commutative ring in which all the non-invertible elements of A form an ideal, then A is a local ring.

(b) Suppose A is a local ring with unique maximal ideal $\mathfrak{m}$. Show that $\mathfrak{m}$ consists of all the non-invertible elements of A.

(c) Which of the following are local rings?

(i) The ring $\mathbb{Z}$ of integers.

(ii) The field $\mathbb{C}$ of complex numbers.

(iii) The polynomial ring $\mathbb{C}[x]$.

2. Define $\alpha = \sqrt{2} + \sqrt{3}$.

(a) Show that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(b) Find the minimum polynomial of α over $\mathbb{Q}$.

(c) Show that the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal.

(d) Compute the Galois group of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

3. For this exercise, define

$$R = \left\{ \left(\begin{array}{cc} a & b \\ -b & a \end{array} \right) \middle| \; a, b \in \mathbb{R} \right\}, \quad S = \left\{ \left(\begin{array}{cc} a + bi & c + di \\ -c + di & a - bi \end{array} \right) \middle| \; a, b, c, d \in \mathbb{R} \right\}.$$

(a) Justify that R and S are rings with the usual matrix operations of addition and multiplication.

(c) Show that R is a field isomorphic to the field of complex numbers.

(b) Show that S is a division ring, meaning that each nonzero element of S has a multiplicative inverse.

(d) Show that S is not a field.

4. Let p be prime, n be a positive integer, and $q = p^n$.

(a) Show that if $f(x), g(x) \in \mathbb{F}_q[x]$ are distinct polynomials of degree at most $q-1$, then they are different as functions; i.e., there exists $\alpha \in \mathbb{F}_q$ such that $f(\alpha) \neq g(\alpha)$. [Hint: consider $h(x) = f(x) - g(x)$. Show that if $h(x)$ is not the zero polynomial, then it cannot be the zero function.]

(b) How many distinct functions are there from $\mathbb{F}_q$ to $\mathbb{F}_q$? How many distinct polynomials are there of degree at most $q-1$ with coefficients in $\mathbb{F}_q$? Conclude that every function from $\mathbb{F}_q$ to $\mathbb{F}_q$ can be represented as a polynomial of degree at most $q-1$ with coefficients in $\mathbb{F}_q$.

(c) Show that if ψ is an automorphism of a finite field $\mathbb{F}_q$, then ψ is of the form $\psi(x) = x^{p^k}$.

5. Let $\alpha \in S_5$ be the permutation $(12)(34)$.

(a) Determine the conjugacy class of α in S_5

(b) Determine all the elements of S_5 that commute with α.

(c) Determine the conjugacy class of α in A_5.

6. Given a field k, $\mathrm{GL}_n(k)$ denotes the group of all $n \times n$ invertible matrices with entries in k, and $\mathrm{SL}_n(k)$ denotes the group of all $n \times n$ matrices with determinant 1. Define $\mathrm{PSL}_n(k)$ to be the quotient of $\mathrm{SL}_n(k)$ by its center.

(a) Prove that $\mathrm{SL}_n(k)$ is a normal subgroup of $\mathrm{GL}_n(k)$.

(b) Prove that the center of $\mathrm{GL}_n(k)$ is the set of all matrices of the form λI_n where $\lambda \in k$.

(c) What is the the center of $\mathrm{SL}_n(\mathbb{C})$?

(d) Prove that $\mathrm{PSL}_2(\mathbb{F}_2) \cong S_3$.

7. Consider the partition of $\{1, \ldots, nm\}$ given by

$$\begin{aligned} \mathcal{P}_1 &= \{1, \ldots, m\}, \\ \mathcal{P}_2 &= \{m+1, \ldots, 2m\}, \\ &\vdots \\ \mathcal{P}_n &= \{m(n-1)+1, \ldots, nm\}. \end{aligned}$$

Let $\mathcal{W}$ be the subgroup of S_{nm} consisting of all permutations that preserve this partition; that is, for all $\sigma \in \mathcal{W}$, if $i, j \in \mathcal{P}_k$, then for some ℓ, we have $\sigma(i), \sigma(j) \in \mathcal{P}_\ell$.

(a) Show that $\mathcal{W}$ acts transitively on $\{1, \ldots, nm\}$, meaning that for any $1 \leq i, j \leq nm$, there exists $\sigma \in \mathcal{W}$ such that $\sigma(i) = j$.

(b) Show that $\mathcal{W}$ has a normal subgroup N isomorphic to $S_m \times S_m \times \cdots \times S_m$ that fixes each $\mathcal{P}_i$.

(c) Show that $\mathcal{W}/N$ is isomorphic to S_n.

8. For which values of n between 3 and 6 is it possible to construct the regular n-gon by straightedge and compass? As usual, justify all your answers.

9. Let p be an odd prime and let e be an integer with $1 \le e \le p-2$ and $\gcd(p-1, e) = 1$.

(a) Prove there exists a positive integer d such that $de \equiv 1 \pmod{p-1}$ and $1 \le d \le p-2$.

(b) The *Pohlig-Hellman Cryptosystem* consists of two functions from $\mathbb{Z}_p$ to $\mathbb{Z}_p$: enciphering is accomplished by the map

$$\mathcal{E}(m) = m^e \pmod{p}$$

and deciphering is accomplished by the map

$$\mathcal{D}(m) = m^d \pmod{p}.$$

Show that $\mathcal{E}$ and $\mathcal{D}$ are inverse functions.

10. Let G be a group with 110 elements.

(a) Prove that G has exactly one Sylow 11-subgroup.

(b) Classify all the groups of order 110.

(c) Prove that G must contain a subgroup of order 10.

11. Let n be a positive integer, S_n the symmetric group on n characters, and V an n-dimensional vector space over a field k with basis $\{v_1, \ldots, v_n\}$. Define an action of S_n on V via

$$\sigma v_i = v_{\sigma(i)}.$$

If $\varphi : S_n \to GL_n(k)$ is the corresponding matrix representation, prove that

$$\det \varphi(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ is an even permutation;} \\ -1, & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

12. Let $d \in \mathbb{Z}$ be square-free and $x, y \in \mathbb{Q}$.

(a) If $d \equiv 3 \pmod{4}$, then under what conditions is $x + y\sqrt{d}$ an algebraic integer?

(b) Show that $\mathbb{Z}[\sqrt{-5}]$ is integrally closed.

(c) Show that $\mathbb{Z}[\sqrt{-5}]$ is not a Unique Factorization Domain.

(d) If $d \equiv 1 \pmod{4}$, then under what conditions is $x + y\sqrt{d}$ an algebraic integer?

(e) Show that $Z[\sqrt{5}]$ is not integrally closed.

(f) Show that $\mathbb{Z}[\sqrt{5}]$ is a Unique Factorization Domain.