Swarthmore College
Department of Mathematics and Statistics
Honors Examination: Algebra

Spring 2002

Instructions: This is a three-hour exam, consisting of twelve problems, Please try to do *six* problems as thoroughly as possible. Once you have done your best on those, make a second pass through the exam and do as many parts of the remaining problems as you can.

General hints and advice: If you get stuck, work out some examples or special cases. If it makes sense, formulate and solve an easier version of the problem. In general, I am interested in learning where your thoughts are going, even if you do not answer the question completely. When there are multiple parts to a problem, please feel free to do them in any order. In some cases, parts of problems have been marked with an asterisk (*). These may be skipped and returned to on your second pass through the exam.

1. If G is a group, and $g \in G$, let C_g denote the conjugacy class containing g and let $C(g)$ denote the centralizer of g, that is,

$$C_g = \{x \in G \mid x = y^{-1}gy \text{ for some } y \in G\} \quad \text{and} \quad C(g) = \{x \in G \mid xg = gx\}$$

   (a) What can you say in general about the relationship between $|C_g|$, $|C(g)|$, and $|G|$?

   (b) If $G = S_4$, the symmetric group on $\{1,2,3,4\}$, and $g = (12)(34)$, compute $|C_g|$ and $|C(g)|$ and describe the elements in each set.

   (c) Repeat part (b) for $G = S_6$ and $g = (12)(34)(56)$.

   (d) (*) Generalize your answers to (b) and (c) to arbitrary even n.

2. Let G denote the group of rotations of a cube (in $\mathbb{R}^3$).

   (a) What is $|G|$?

   (b) For which integers k does G have a subgroup H of order k? Give an example of an H for all possible values of k.

   (c) Give an example of a nontrivial normal subgroup of G.

   (d) (*) What are the Sylow subgroups of G? Compute the number of Sylow p-subgroups for each prime p. Are any of these normal in G? State any general results that are illustrated here.

   (You may employ whatever notation you wish for describing elements and subgroups of G, but please make it clear to me.)

3. (a) In $\mathbb{Q}[x]$, find the greatest common divisor of x^3+x^2+x+1 and x^4+x^3+x+1, and express it in the form $a(x)(x^3+x^2+x+1)+b(x)(x^4+x^3+x+1)$ for some polynomials $a(x), b(x) \in \mathbb{Q}[x]$.

   (b) In $\mathbb{Z}_2[x]$, find the greatest common divisor of x^3+x^2+x+1 and x^4+x^3+x+1, and express it in the form $a(x)(x^3+x^2+x+1)+b(x)(x^4+x^3+x+1)$ for some polynomials $a(x), b(x) \in \mathbb{Z}_2[x]$.

   (Notation: here $\mathbb{Q}[x]$ denotes the ring of polynomials over the rationals, and $\mathbb{Z}_2[x]$ denotes the ring of polynomials over $\mathbb{Z}_2$, the field with two elements.)

4. (a) Prove *Wilson's Theorem*: If p is a prime, then $(p-1)! = -1 \bmod p$.

   (b) If p is not a prime, is it possible for $(p-1)! = -1 \bmod p$?

   (c) If G is an abelian group with elements $a_1, a_2, \ldots, a_n$, and n is odd, show that $a_1 a_2 \cdots a_n = e$, where e denotes the identity.

   (d) If G is abelian, and has exactly one element z of order 2 (that is, $z^2 = e, z \neq e$), show that $a_1 a_2 \cdots a_n = z$.

   (e) (*) If G is abelian, and has more than one element of order 2, show that $a_1 a_2 \cdots a_n = e$.

5. Let G be a group generated by two elements a and b, satisfying the relations

$$a^4 = e, \quad b^4 = e, \quad a^2 = b^2, \quad b\,a\,b^{-1} = a^{-1}$$

   Here e denotes the identity element of G.

   (a) Show that G is a group with eight elements.

   (b) Describe all groups with eight elements.

   (c) Which one of these groups is G?

6. (a) Define what it means for a matrix to be (i) orthogonal, (ii) symmetric, and (iii) positive definite. *(Three separate questions.)*

   (b) Prove that the only real matrix which is orthogonal, symmetric, and positive definite is the identity matrix.

   (c) Prove that, if A is real, positive definite, and symmetric matrix, then $A = P^t P$ for some nonsingular real matrix P.

7. Define rings R_1, R_2, R_3, R_4 as follows:

$$R_1 \ = \ \mathbb{Z}, \quad R_2 = \mathbb{Z}[i], \quad R_3 = \mathbb{Z}[x], \quad R_4 = \mathbb{Z}[x, y]$$

   Considering each R_i in turn, determine whether the following statements are true or false. Give reasons and/or examples to justify your conclusions.

   (a) The ideal $\langle 2 \rangle$ is a prime ideal in R_i.

   (b) The ideal $\langle 2 \rangle$ is a maximal ideal in R_i.

   (c) Every prime ideal in R_i is maximal.

   (d) Every maximal ideal in R_i is prime.

   (e) The quotient ring $R_i/\langle 2 \rangle$ is a field.

   (f) Every ideal in R_i is a principal ideal.

   Recall that an ideal J in a commutative ring R is *prime* if, whenever $ab \in J$, either $a \in J$ or $b \in J$.

   (Notation: if R is a ring and $\alpha \in R$, then $\langle \alpha \rangle$ denotes the ideal generated by α, i.e., the smallest ideal in R containing α. The rings $\mathbb{Z}[x]$ and $\mathbb{Z}[x, y]$ are polynomial rings, and $\mathbb{Z}[i]$ denotes the set of complex numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$.)

8. Determine whether the following statements are true or false. Give reasons to justify your conclusions.

   (a) $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field.

   (b) $\mathbb{R}[x]/\langle x^2+1\rangle$ is isomorphic to $\mathbb{C}$ (the field of complex numbers).

   (c) $\mathbb{R}[x]/\langle x^2+x+1\rangle$ is a field.

   (d) $\mathbb{R}[x]/\langle x^2+x+1\rangle$ is isomorphic to $\mathbb{C}$.

   (e) $\mathbb{R}[x]/\langle x^2-1\rangle$ is not a field.

   (f) $\mathbb{R}[x]/\langle x^2-1\rangle$ is isomorphic to the ring $\mathbb{R}\times\mathbb{R}$.

   (g) $\mathbb{R}[x]/\langle x^2\rangle$ is not a field.

   (h) $\mathbb{R}[x]/\langle x^2\rangle$ is isomorphic to the ring $\mathbb{R}\times\mathbb{R}$.

   In each case where you assert that there is an isomorphism, please describe it explicitly.

9. Consider the following statement:

   > *If G is a finite group with more than two elements, then G has a nontrivial automorphism.*

   Is this statement true? If so, give a proof. If not, find a counterexample.

10. An $n\times n$ matrix A is *nilpotent* if $A^k=0$ for some $k>0$.

    (a) Give examples of two nonzero 3×3 nilpotent matrices A and B that are not similar to each other. *(Two matrices A and B are similar if there exists an invertible C such that $B=C^{-1}AC$.)*

    (b) Prove that every nonzero 3×3 nilpotent matrix is similar to either A or B.

    (c) Prove that, if an $n\times n$ matrix is nilpotent, then $A^n=0$.

11. Let K denote the splitting field of the polynomial $p(x)=x^4-4$ over $\mathbb{Q}$, and let G denote the Galois group of K over $\mathbb{Q}$. Let L denote the splitting field of $q(x)=x^4-1$ over $\mathbb{Q}$, and let H denote the Galois group of L over $\mathbb{Q}$.

    (a) Is L a subfield of K? Is H a subgroup of G? Explain these relationships exactly.

    (b) Compute $|G|$ and $|H|$, and describe the elements of G and H explicitly.

    (c) Find all fields F such that $\mathbb{Q}\subseteq F\subseteq K$, and describe exactly how each one corresponds to a subgroup of G.

    (d) Show that G is abelian.

    (e) Show that each subfield F with $\mathbb{Q}\subseteq F\subseteq K$ is a splitting field.

    (f) Consider the last two properties in general. Does (d) always imply (e)? Does (e) always imply (d)? Are the two properties equivalent? State any general results you are using here.

12. Would any of the answers to problem 10 be different if we had taken K instead to be the splitting field of the polynomial $r(x)=x^4-3$? Explain.