Mathematics 113 Professor A. Ogus
May 16, 2008

Algebra Final Exam Solutions

Note: Be sure to write in complete sentences. You will be graded on your style as well as content. I may deduct points for material you write that is correct but irrelevant, as well for material that is relevant but incorrect.

Definitions. (30 points, 3 for each problem)

1. What is the definition of an *equivalence relation* on a set A?
   An equivalence relation on A is a subset R of $A \times A$ such that $(a, a) \in R$ for every $a \in A$, $(a, b) \in R$ whenever $(b, a) \in A$, and $(a, c) \in R$ whenever (a, b) and $(b, c) \in R$.

2. What is the definition of a *monoid*?
   A monoid is a set M together with an associative binary operation which admits a two-sided identity element.

3. What is the definition of a *normal subgroup* of a group?
   A normal subgroup H of G is a nonempty subset which contains ab^{-1} and gag^{-1} whenever $a, b \in H$ and $g \in G$.

4. What is the definition of a *permutation* of a set S?
   A permutation of S is a bijective function from S to S.

5. If G is a group and A is a G-set, what is the definition of an *orbit* of A?
   An orbit of A is a subset of A of the form $\{ga : g \in G\}$ for some $a \in A$.

6. What is the definition of an *ideal* in a ring?
   And ideal in a ring R is a nonempty subset I which contains $a + b$ and ra and ar whenever $a, b \in I$ and $r \in R$.

7. What is the definition of a *maximal ideal* in a ring?
   A maximal ideal of R is an ideal $I \neq R$ such that there are no ideals K with $I \subset K \subset R$.

8. If R is an integral domain, what is the definition of a *unit* of R?
   A unit of R is an element u such that there exists an element v of R such that $uv = 1$.

9. If R is an integral domain, what is the definition of an *irreducible element* of R?
   An element r of R is irreducible if it is not zero, not a unit, and whenever $= ab$, either a or b is a unit.

10. If R is an integral domain, what is the definition of a *prime* element of R?
    An element r of R is prime if $r \notin R^*$ and whenever $r|ab$, $r|a$ or $r|b$.

Computations. (60 pts.) Show and explain your work as appropriate.

1. (25 points) Write the following permutation as a product of disjoint cycles, then compute its sign, order, the size of its conjugacy class, and its centralizer in the group S_9.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 8 & 7 & 3 & 4 & 6 & 1 & 2 \end{pmatrix}.$$

   Warning: if you get the first part wrong you will receive no partial credit if the rest of your answers are consequently wrong.

   (a) cycle decomposition: (1 5 3 8)(2 9)(4 7 6)

   (b) sign: even

   (c) order: 12

   (d) number of conjugates in S_9. This is $\frac{9!}{4\cdot 2\cdot 3} = 15120$

   (e) centralizer in S_9. This clearly contains the product of the groups generated by the cycles: $\langle(1\ 5\ 3\ 8)\rangle\langle(19)\rangle\langle(4\ 7\ 6)\rangle$. This group has order $4 \cdot 2 \cdot 3$, hence its index is the number of conjugates, hence it is the entire centralizer.

2. (15 points) In the cyclic group $(\mathbf{Z}_{630}, +)$ of order 630, let H be the smallest subgroup containing [40] and [300]. Find the order of H. Is H cyclic? If not, explain why not. If it is, find a generator.
   Any subgroup of a cyclic group is cyclic, so H is surely cyclic. In fact, the greatest common divisor of 40 and 300 is 20, so H is generated by [20]. The greatest common divisor of 20 and 630 is 10, so H is also generated by [10]. Evidently this group has order 63.

3. (10 points) Find two positive integers n less than 31 such that $n^{92} + n^{31} - 6$ is divisible by 31.
   If n is not divisible by 31, then n^{30} is congruent to 1 mod 31, so it enough to find n such that $n^2 + n - 6$ is divisible by n. $n = 2$ and $n = -3$ satisfy this. Thus $n = 2$ and $n = 28$ will work.

4. (10 points) In the ring of Gaussian integer $\mathbf{Z}[i]$, factor 70 into irreducible factors. (You need not prove that your factors are irreducible, just explain.)
We have $70 = 2 \cdot 7 \cdot 5$. Since 7 is congruent to 3 mod 4, it is irreducible in $\mathbf{Z}[i]$. Thus

$$70 = (1+i)(1-i)7(1+2i)(1-2i).$$

The remaining numbers are irreducible since their norms are prime.

Theory and proofs. (60 points, 15 for each problem) In the following problems, you may use a theorem stated in the book, but not if it reduces the problem to a triviality. Explain yourself carefully.

1. Let G be a finite group.

   (a) Let S be a finite G-set. Write an equation relating the cardinality of S, the number of fixed points, and the indexes of certain subgroups of G. Explain very carefully what these subgroups are, using complete sentences.

   Choose an element s_i from each nontrivial orbit of S and let $G_i := \{g : gs_i = s_i\}$. Then if S^G denotes the set of fixed points,

   $$|S| = |S^G| + \sum_i [G : G_i].$$

   (b) Suppose that the p is prime and that G is a p-group, *i.e.*, that the order of G is a power of p. Prove that the cardinality of S is congruent to the cardinality of the fixed point set S^G mod p.
   If G is a p-group, each $[G : G_i]$ is divisible by p, since G_i is a proper subgroup of G.

   (c) Use the previous result (with a suitably chosen S) to prove that the center of every p-group is nontrivial.
   Let G act on itself by conjugation. Then the set of fixed points is just the center Z of G, and the equation shows that its cardinality is divisible by p. Since $e \in Z$, Z has at least p elements.

2. Let $\theta\colon A \to B$ be a homomorphism of rings. Prove that the kernel of θ is an ideal of A. Prove that if A is commutative and B is an integral domain, then the kernel of θ is a prime ideal of A.

   Let K be the kernel of θ. If k and k' belong to K, $\theta(k+k') = \theta(k) + \theta(k') = 0$, so $k + k' \in K$. Furthermore, $0 \in K$. Finally, if $a \in A$, $\theta(ak) = \theta(a)\theta(k) = \theta(a)0 = 0$, and similarly for $\theta(ka)$. Hence ak and ka belong to K also. If B is an integral domain and aa' belongs to the kernel, then $\theta(a) = \theta(a')$ in B, hence either $\theta(a)$ or $\theta(a')$ is zero, hence a or a' belongs K. This means that it is a prime ideal.

3. Consider the subring $R := \mathbf{Z}[\sqrt{-11}]$ of $\mathbf{C}$ consisting of all numbers of the form $a + b\sqrt{-11}]$, where a and b are integers. In the following problems, use the norm map $N\colon R \to \mathbf{Z}$ sending α to $\alpha\overline{\alpha}$.

   (a) Find all the units of R.

   An element $\alpha = a + b\sqrt{-11}$ of R is a unit if and only if $N(\alpha)$ is a unit, iff it is 1. But $N(\alpha) = a^2 + b^2 11$, which can only equal 1 if $b = 0$ and $a = \pm 1$.

   (b) Show that 5 is irreducible in R.

   Say $3 = \alpha\beta$. Then $9 = N(\alpha)N(\beta)$, Since 3 is not the norm of anything, either $N(\alpha)$ or $N(\beta) = 1$, hence one of them is a unit.

   (c) Show that 3 is not prime in R. (Hint: look at 3^3.)

   $3^3 = 27 = 16 + 11 = (4 + \sqrt{-11})(4 - \sqrt{-11})$, but 3 does not divide $(4 + \sqrt{-11})$.

4. Let F be a finite field and let f be an irreducible element of $F[X]$. Suppose that f has a root e in an extension field E of f. Prove that f splits in E.

   Hint: It is enough to prove this when $E = F[e]$. Use the fact that $Aut(E/F)$ has order d, where d is the degree of E over F. (You do not need to prove this fact.)

   If $g \in Aut(E/F)$, then $g(e)$ is another root of f. If $h \in Aut(E/F)$ and $g(e) = h(e)$, $g = h$, since $E = F[e]$. Thus the number of roots of g is at least as big as the size of $Aut(E/F)$. In our case, we know this is d, the degree of g. So g has d roots in E, so it splits.