Mathematics 250A

Professor A. Ogus
December, 2010

Algebra Final Exam Solutions

1. Automorphisms of groups.

   (a) Define: the *center* of a group, an *inner automorphism* of a group.
   Solution: The center of a group G is the set of $z \in G$ which commute with all elements of G. An inner automorphism of G is an automorphism of the form $\alpha_h = g \mapsto hgh^{-1}$ for some $h \in G$.

   (b) Prove or disprove that every automorphism of S_3 is inner.
   Solution: This is true. For every group G we have a natural map $\alpha\colon G \to \mathrm{Aut}(G)$ sending h to α_h whose kernel is the center of G. Since the center of S_3 is trivial, this map is injective. Now every automorphism a of S_3 preserves the set of transpositions. Since there are three transpositions, we get a map $\mathrm{Aut}(S_3) \to S_3$, and since these transpositions generate S_3, this map is injective. The composite $S_3 \to S_3$ must be bijective, hence the map α is surjective.

   (c) Prove or disprove: every automorphism of A_4 is inner.
   Solution: This is not true. Conjugation by a transposition in S_4 induces an automorphism of A_4 which is not inner. This is because (1 2 3) is not conjugate to (1 3 2) in A_4.

2. Give a list of all isomorphism classes of all groups of as described below, with each isomorphism class occuring exactly once in your list.

   (a) The abelian groups of order 36. No proofs needed here.
   Solution: $\mathbf{Z}/36\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}18\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$, $\mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$.

   (b) All groups of order 10. Prove your results.
   Solution: There are just two, the cyclic group of order 10 and the dihedral group of order 10. By the Sylow theorems, there is at least one subgroup of order 5, and clearly there can only be one. Then it is normal, and we denote it by N. Let H be a subroup of order 2. If H is normal our group is abelian and necessarily cyclic.

In any case it is a semidirect product, given by the action α of H on N by conjugation. Now $\mathrm{Aut}(N)$ is cyclic of order 4, so has a unique element of order two, and hence there is just one nontrivial possibility for this action. This gives the dihedral group.

3. State and prove the theorem on the linear independence of characters.
Solution:

Theorem: Let M be a monoid and let K be a field. Then the set of monoid homomorphisms from M to the multiplicative monoid of K is a linearly independent subset of the K-vector space K^M.

Proof: It is enough to prove that if $\chi_1, \ldots, \chi_n$ is a sequence of distinct homorphisms $M \to K$ and $c_1, \ldots, c_n$ is a sequence in K such that $\sum c_i\chi_i = 0$, then each $c_i = 0$. We do this by induction on n. If $n = 1$, we have $c_1 = c_1\chi_1(1) = 0$, so $c_1 = 0$. For the induction step, observe that for any $g, h \in M$, we have

$$\begin{aligned} c_1\chi_1(g) + \cdots + c_n\chi_n(g) &= 0 \\ c_1\chi_1(gh) + \cdots + c_n\chi_n(gh) &= 0 \end{aligned}$$

Multiply the first equation by $\chi_n(h)$ and subtract from the second equation to obtain

$$c_1\chi_1(g)(\chi_1(h) - \chi_n(h)) + \cdots + c_{n-1}\chi_{n-1}(g)(\chi_{n-1}(h) - \chi_n(h)) = 0$$

Fixing h and letting g vary, we see that

$$c_1(\chi_1(h) - \chi_n(h))\chi_1 + \cdots + c_{n-1}(\chi_{n-1}(h) - \chi_n(h))\chi_{n-1} = 0.$$

By the induction assumption, $c_i(x_i(h) - \chi_n(h)) = 0$ for all h and $1 \leq i < n$. Since $\chi_i \neq \chi_n$ if $i < n$, this implies that $c_i = 0$ if $i < n$. Then $c_n\chi_n = 0$ and it follows also that $c_n = 0$. □

4. Let k be a field, let A be a finite dimensional commutative k-algebra, and let X denote the set of homomorphisms of k-algebras from A to an algebraic closure K of k.

(a) Show that the cardinality of X is less than or equal to the k-dimension of A over k.
Solution: This is because the elements of X define characters from A to K which must be linearly independent in the K-vector space $\mathrm{Hom}_k(A, K)$. But the K-dimension of this is the k-dimension of A.

(b) Define a natural action of the group $\mathrm{Aut}(K/k)$ on X, and prove that the orbits of the action can be naturally identified with the set of prime ideals of A.
Solution: If $g \in \mathrm{Aut}(K/k)$ and $x \in X$, we define gx to be the composite $g \circ x$. For each x, $\mathrm{Ker}\, x$ is a prime ideal of A, and $\mathrm{Ker}\, x = \mathrm{Ker}\, gx$, so we get a map from the orbit space $\overline{X}$ to the set of prime ideals. If P is a prime ideal of A, then A/P is a finite integral domain, hence a finite field extension of k, and hence admits an embedding into K. Thus there is an x with $\mathrm{Ker}(x) = P$. Furthermore, since K/k is normal, any two such embeddings differ by an automorphis of K/k, so the action of Aut on the set of all x with a given kernel is transitive.

(c) Define what it means for A to be separable over k. Assuming that A is separable, prove that it is a field if and only the action of $\mathrm{Aut}(K/k)$ on X is transitive.
Solution: A is separable if its dimension is equal to the cardinality of X. If this is the case and the action of $\mathrm{Aut}(X/k)$ is transitive, there is just one prime ideal P and since the nilradical of A must vanish, $P = 0$ and A is a domain.

(d) Give an example to show that this is not true without the separability assumption.
Solution: Take $A = k[t]/(t^2)$.

5. Compute the degree and the Galois group of the splitting fields of:

(a) $X^{15} + 2$ over $\mathbf{Q}$
Solution: The splitting field K contains μ_{15}. Let E be the field extension of $\mathbf{Q}$ obtained by adjointing μ_{15}. This extension has Galois group $(\mathbf{Z}/15\mathbf{Z})^*$, which has order 8. The extension F obtained by adjoining just one root of the polynomial has degree 15 (since the polynomial is irreducible). Then $F \cap E$ is trivial, and it

follows that $Gal(K/F) \cong Ga(E/\mathbf{Q})$ and hence has degree 8. Then the degree of $K/\mathbf{Q}$ is $15 \times 8 = 120$. We have an exact sequence:

$$1 \to Gal(K/E) \to Gal(K\mathbf{Q}) \to Gal(E/\mathbf{Q}) \to 1$$

Furthermore, $Gal(K/E)$ is canonically isomorphic to μ_{15}, a cyclic group of order 15, and $Gal(E/\mathbf{Q})$ to $Aut(\mu_{15} \cong (\mathbf{Z}/15\mathbf{Z})^* \cong (\mathbf{Z}/5\mathbf{Z})^* \times \mathbf{Z}/3\mathbf{Z}^* \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. This is a noncyclic abelian group of order 8 and is isomorphic to any of the 2-Sylow subgroups of $Gal(K/\mathbf{Q})$. Choose such a group H. Then G is the semidirect product of H and $\mathbf{Z}/15\mathbf{Z}$. The canonical action of $(\mathbf{Z}/15\mathbf{Z})^*$ on $\mathbf{Z}/15\mathbf{Z}$ is the action of H by conjugation, and this determines the semidirect product.

(b) $X^3 + 4x + 2$ over $\mathbf{Q}$.
Solution: This polynomial is irreducible by Eisenstein's criterion. So the degree of the splitting field is either 3 or 6. On the other hand, the derivative of this polynomial is $3x^2 + 4$ which is always positive, so there is only one real root, hence two complex roots. Hence the Galois group contains complex conjugation, an element of order 2. Thus the group has order 6, and hence is S_3.

6. Let K/k be a finite Galois extension with group G.

(a) State the normal basis theorem.
Solution: This asserts that there is an element w of K such that $\{gw : g \in G\}$ is a k-basis of K. In other words, that K is a free $k[G]$-module of rank one.

(b) Find a normal basis for the splitting field of the polynomial $f(x) := x^3 - x - 1$ over the finite field with 3 elements. Explain why your answer really is a normal basis.
Solution: There are many correct answers. For example, if a is a root of f, then a^2 will be a normal basis. To see this, recall that the Galois group is cyclic, generated by the Frobenius element ϕ. Thus $\phi a = a^3 = a + 1$, so

$$\phi(a^2) = (a+1)^2 = a^2 + 2a + 1$$

$$\begin{aligned} \phi^2(a^2) &= \phi(a^2 + 2a + 1) \\ &= a^2 + 2a + 1 + 2(a+1) + 1 \\ &= a^2 + a + 2. \end{aligned}$$

Since (a^2, a^2+2a+1, a^2+a+2) is linearly indepedent, we are done.

(c) Is a root of f a normal basis? Explain.
Solution: No it is not, since the sequence $(a, a+1, a+2)$ does not span K.

7. Let R be a ring and let $\mathcal{A}_R$ be the category of commutative R-algebras. Let $F\colon \mathcal{A}_R \to \mathcal{S}ets$ be the forgetful functor from the category $\mathcal{A}_R$ to the category of sets.

(a) What is meant by a *natural transformation* $F \to F$?
Solution: This means a collection of set maps $\{\eta_A A \to A : A \in \mathcal{A}_R\}$ such that for every homomorphism $\theta\colon A \to B$, the diagram

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & A \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta} \\ B & \xrightarrow{\eta_B} & B \end{array}$$

commutes.

(b) Define an R-algebra structure on the set of natural transformations $F \to F$ by using "pointwise" addition and multiplication.
Solution: If α and β are natural transformations, we define $(\alpha_A + \beta_A)(a) := \alpha_A(a) + \beta_A(a)$ for all $a \in A$. Then if $\theta\colon A \to B$, we get

$$\begin{aligned} \theta(\alpha_A + \beta_A)(a) &= \theta(\alpha_A(a) + \beta_A(a)) \\ &= \theta(\alpha_A(a) + \theta\beta_A(a)) \\ &= \alpha_B(\theta(a)) + \beta_B(\theta(a)) \\ &= (\alpha_B + \beta_B)\theta(a) \end{aligned}$$

Thus $\alpha + \beta$ is a natural transformation. The proof for multipication is similar. Finally, if $r \in R$, we define a natural transformation $\hat{r}\colon F \to F$ by letting r_A be the constant map sending A to the image of r in A. This is clearly natural, and $r \to \hat{r}$ is a ring homomorphism.

(c) Identify the R-algebra of natural transformations $F \to F$ with a familiar and elementary object in $\mathcal{A}_R$. Prove your result. You need not verify that your isomorphism is compatible with the algebra structures.

Solution: The R-algebra Nat of natural transformations is isomorphic to $R[x]$, the polynomial ring in one variable. Indeed, if $f \in R[x]$, we get a natural transformation $\eta_f \colon F \to F$ by sending a to $f(a)$. In fact we know that $F \cong \mathrm{Hom}_{\mathcal{A}_R}(R[x], \ )$, and by Yoneda,

$$\mathrm{Mor}(F, F) \cong F(R[x]) = R[x].$$

It remains to verify that this map is compatible with the algebra structures.