Mathematics 113 Professor A. Ogus
April 18, 2008

Algebra Midterm Exam 2 Solutions

1. Conjugacy in groups

   (a) Let G be a group and let g be an element of G. Define what is meant by the *conjugacy class* of g and the *centralizer* of g.
   The conjugacy class of g is the set of all elements of the form aga^{-1} for all $a \in G$. The centralizer of g is the set of all elements which commute with g; it is a subgroup of G.

   (b) Describe the conjugacy class and centralizer of the following elements in the given groups.

      i. The element 3 in the group $\mathbf{Z}$ under addition.
      This group is abelian so the conjugacy class of 3 is the singleton set $\{3\}$ and its centralizer is the entire group $\mathbf{Z}$.

      ii. The element (1 2) in the group S_4.
      We know that this is the set of transpositions. There are 6 of these, so the centralizer H of τ has index 6 and hence order 4. It contains (1 2) and (3 4), hence is in fact the subgroup of S_4 generated by these elements, which is a product of two groups of order 2.

      iii. The element (1 2 3 4) in the group S_5.
      This is the set of all 4-cycles. There are 30 of these, so the order of the centralizer is 4, and must be the cyclic group (of order 4) generated by (1 2 3 4)

   (c) Write the class equation for a finite group. Use it to show that every nonabelian group of order 39 has a subgroup of order 13.

      The class equation says that $|G| = |Z| + \sum |C_i|$, where Z is the center of G and the C_i are the nontrivial conjugacy classes. Thus $39 = |Z| + \sum |C_i|$. Suppose there is no subgroup of order 13. The centralizer of each element not in the center is a nontrivial proper subgroup of G, which must have order 3, hence index 13. Hence

$|C_i| = 13$ for every i. Then $39 = |Z| + n13$ for some n, hence $|Z|$ is divisible by 13. Since G is not abelian, Z is a proper subgroup of order divisible by 13, hence has order 13, a contradiction.

2. Rings and ideals

(a) What is the definition of an *ideal* in a (not necessarily commutative) ring R? Show that if I is an ideal in R, then there is a unique binary operation on R/I which is compatible with the multiplication on R.

An ideal in R is a subset I of R which forms a subgroup under addition and with the property that rx and xr belong to I whenever $x \in I$ and $r \in R$. Any binary operation on R/I compatible with the multiplication on R must satisfy $\pi(a)\pi(b) = \pi(ab)$, and since π is surjective, this determines the operation uniquely. We must check that the right hand side is independent of the choices of a and b. If $\pi(a') = \pi(a)$ and $\pi(b') = \pi(b)$, then $a' = a + x$ and $b' = b + y$, where $x, y \in I$. Then

$$\pi(a'b') = \pi((a + x)(b + y)) = \pi(ab + xb + ay + xy) = \pi(ab),$$

since ay, xb, and xy belong to I.

(b) What is the definition of an *irreducible element* in an integral domain?

An element r of an integral domain R is irreducible if it is not a unit (invertible) and whenever $r = ab$, either a or b is a unit.

Show that if R is a principal ideal domain and $r \in R$ is an irreducible element, then $R/I(r)$ is a field, where $I(r)$ is the principal ideal generated by r.

Since r is not a unit, $I(r) \neq R$ so $R/I(r)$ is not the zero ring. Suppose that $a \notin I(r)$. Consider the ideal $I(a, r)$ of all linear combinations of a and r. Since R is a PID, this is a principal ideal. Let b be a generator of $I(a, r)$. Then $r \in I(b)$, say $r = bc$. Since r is irreducible, either b or c is a unit. If c is a unit, then $I(r) = I(b)$, which is not possible, since $a \in I(b)$ and $a \notin I(r)$.

Hence b is a unit, and hence $I(a,r) = R$ and $1 \in I(a,r)$. If $1 = xa + yr$, $x + I$ is an inverse to $a + I$.

3. Polynomials

Let F be a field and let $F[x]$ be the ring of polynomials with coefficients in F. Let F^F denote the ring of functions from F to F, with the usual (pointwise) operations. The map $\phi\colon F[x] \to F^F$ taking a polynomial f to the function $a \mapsto f(a)$ is a ring homomorphism.

(a) Show that if F is infinite, ϕ is injective but not surjective.
Hint: Use what you know about the roots of a polynomial.
If $\phi(f) = 0$, $f(a) = 0$ for every $a \in F$. But a nonzero polynomial in $F[x]$ has only finitely many roots. Hence $f = 0$ and hence $\mathrm{Ker}(\phi) = \{0\}$. This implies that ϕ is injective. On the other hand, consider the function δ defined by $\delta(a) = 0$ if $a \neq 0$ and $\delta(0) = 1$. It is clear that δ does not belong to the image of ϕ; otherwise there would exist a nonzero polyonomial f with $f(a) = 0$ for all $a \neq 0$.

(b) Show that if F is finite, ϕ is surjective but not injective.
Hint: Don't give the details of the surjectivity, just quote a construction from the exercises.
The surjectivity of ϕ can be seen from the Lagrange interpolation formula; we know that given any two finite sequences $(a_1, \ldots, a_r)$, and $(b_1, \ldots, b_n)$ with $a_i \neq a_j$ for $i \neq j$, there is a polynomial $f \in F[x]$ such that $f(a_i) = b_i$ for all i. But ϕ can't be injective, since $F[x]$ is infinite but F^F is finite.

(c) Show it if $F = \mathbf{Z}_p$, then the kernel of ϕ is the ideal generated by $x^p - x$.
Hint: First show that $x^p - x$ belongs to the kernel. How many elements are there in F^F?
For any element $a \in Z_p$, $a^p = a$, so $\phi(x^p - x) = 0$. The elements of the quotient $F[x]/I(x^p - x)$ can be represented by the polynomials of degree less than p, and there are p^p of these. On the other hand, F^F has p^p elements. Thus the map $F[x]/I(x^p - x) \to F^F$ induced by ϕ is a surjective map between two sets with the same cardinality, and hence is bijective.