Mathematics 113 Professor A. Ogus
December 18, 2004

# 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 pts.)

1. What is the definition of a *monoid*?
   A monoid is a set $A$ together with an associative binary operation and an identity element.

2. What is the definition of a *normal subgroup* of a group?
   A normal subgroup of a group $G$ is a nonempty subset $H$ of $G$ closed under the group law and inverses, such that $ghg^{-1} \in H$ if $g \in G$ and $h \in H$.

3. 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 set of the form $\{ga : g \in G\}$ for some element $a$ of $A$.

4. What is the definition of a *cycle* in a permutation group?
   A cycle in a permutation group is a permutation with only one non-trivial orbit.

5. What is the definition of an *ideal* in a ring?
   An ideal in a ring $R$ is a subset $I$ of $R$ which is a subgroup under the addition and such that $rx$ and $xr$ belong to $I$ whenever $x \in I$ and $r \in R$.

6. What is the definition of a *prime ideal* in a ring?
   An ideal $I$ of a (commutative) ring $R$ is prime if $ab \in I$ implies that $a$ or $b$ in $I$, and in addition $I \neq R$.

7. If $R$ is an integral domain, what is the definition of a *unit* of $R$?
   An element $r$ of $R$ is a unit if there exist some $s$ such that $sr = 1$.

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

9. If $R$ is an integral domain, what is the definition of a *prime* element of $R$?
   An element $r$ of $R$ is prime if the ideal $(r)$ is prime.

10. What is the definition of the *degree* of a field extension?
    If $F \to E$ is a field extension, then its degree is the dimension of $E$ regarded as an $F$-vector space via its multiplication map and the inclusion $F \to E$.

**Computations. (60 pts.)** Show and explain your work as appropriate. For example, if you claim an element in a ring other than $\mathbf{Z}$ is irreducible, prove that it is.

1. (5 pts) Write the following permutation as a product of disjoint cycles.

$$(2\ 5\ 7\ 1)(2\ 4\ 1\ 5\ 6)(5\ 1\ 8\ 9\ 7)$$

   Answer: $(1\ 8\ 9)(2\ 4)(3)(5\ 7\ 6)$

2. (10 pts) 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.
   Answer: The gcd of 40 and 300 is 20, so $H$ is cyclic, generated by 20. The gcd of 20 and 630 is 10, so $H$ is also generated by 10, and hence has order 63.

3. (10 pts) Find the number of elements of $S_6$ that can be written as $\sigma(1\ 2\ 3\ 4\ 5)\sigma^{-1}$, where $\sigma$ ranges over all the elements of $S_6$. Describe the set of $\sigma \in S_6$ which commute with $(1\ 2\ 3\ 4\ 5)$. Now do the same in the group $A_6$ in place of $S_6$..
   Answer: An element in $S_6$ is conjugate to $(1\ 2\ 3\ 4\ 5)$ iff it is a 5-cycle, and there are $\dfrac{6 \cdot 5 \cdot 4 \cdot 4 \cdot 2}{5} = 144$ of these. Hence the order of the centralizer is $6!/144 = 5$, and the centralizer is exactly the subgroup generated by $(1\ 2\ 3\ 4\ 5)$. Since this group is contained in $A_6$, the number of $A_6$ conjugates is $\dfrac{144}{2} = 72$.

4. (5 pts)Find a positive number $n$ less than 31 such that $7^{92} - n$ is divisible by 31.
   Answer: Since 31 is prime, $7^{30} \equiv 1 \pmod{31}$, so $7^{92} = 7^{30 \cdot 3 + 2} \equiv 7^2 \equiv 49 \equiv 18 \pmod{31}$.

5. (10 pts) Find the number of positive numbers less than 31 which are relatively prime to 31. Do the same with 31 replaced by $31^2$. By 155.
   Answer: We use the fact that $\phi(31) = 30$ since 31 is prime, and that $\phi(31^2) = 31 \cdot 30 = 930$. On the other hand, $\phi(155) = \phi(5 \cdot 31) = \phi(5)\phi(31) = 4 \cdot 30 = 120$.

6. (10 pts) In the polynomial ring $\mathbf{F}_7[x]$, factor the polynomial $x^4 - x^2 - 2$ into irreducible factors. Do the same in the ring $\mathbf{F}_5[x]$.
   Answer: Note that $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$. Mod 7, the answer is $(x - 3)(x + 3)(x^2 + 1)$, since mod 7, $2 = 3^2$, and $-1$ is not a square, so $x^2 + 1$ is irreducible. Mod 5, $2^2 = -1$ and 2 is not a square, so the answer is $(x - 2)(x + 2)(x^2 - 2)$.

7. (5 pts)In the ring of Gaussian integer $\mathbf{Z}[i]$, factor 182 into irreducible factors.
   Answer: Note that $182 = 2{\cdot}7{\cdot}13$. Since $7 \equiv 3 \pmod 4$ it is irreducible. On the other hand $2 = N(1+i)$ and $13 = N(2+3i)$, so $1+i$ and $2+3i$, as well as their conjugates, are irreducible. Thus the answer is

$$182 = (1 + i)(1 - i)7(2 + 3i)(1 - 3i).$$

8. (5 pts)In the ring $R := \mathbf{Z}[\sqrt{-5}]$, factor 46 into irreducible factors in two essentially different ways.
   Answer: $46 = 2 \cdot 23$ is the prime factorization of 46 in $\mathbf{Z}$. It is clear by inspection that neither 2 nor 23 can be written as $a^2 + 5b^2$, *i.e.*, neither of these is a norm. It follows that 2 and 23 are irreducible in $R$. On the other hand, $46 = 1 + 5 \cdot 3^2 = N(\alpha)$, where $\alpha = 1 + 3\sqrt{-5}$. Since 2 and 23 are not norms, $\alpha$ and $\overline{\alpha}$ are irreducible in $R$. Thus we also have $46 = \alpha\overline{\alpha}$ is an irreducible factorization.

**Theory and proofs. (60 pts)** 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. (10 pts) Let $G$ be a finite cyclic group of order $n$ and $g$ a generator of $G$. Prove that $n$ is the smallest positive integer such that $g^n = e$.
   First observer that if $1 \leq i < j$, then $g^i = g^j$ iff $g^{j-i} = e$. Since $G$ is finite, there must exist such a pair, hence there must exist a positive number $m$ such that $g^m = e$. The same argument shows that if $1 \leq i < j \leq m$, then $g^i \neq g^j$, so $m \leq n$. On the other hand, any element $k$ of $\mathbf{Z}$ can be written as $k = mq + r$ with $r \in [1, m]$, so $g^k = g^r$, so that $n \leq m$.

2. (10 pts) Let $G$ be a finite group and let $X$ be a nonempty transitive $G$-set. Prove that the number of elements of $X$ divides the number of elements of $G$.
   If $X$ is notempty transitive, there exists $x \in X$ such that the map $G \to X$ sending $g$ to $gx$ is surjective. Furthermore, two elements in $G$ have the same image iff they differ by an element in the isotropy subgroup $G_x$ of $x$. Hence the cardinality of $X$ equals the index of $G_x$ in $G$, which divides the order of $G$.

3. (15 pts)Let $G$ be a group of order 77. Use the Sylow theorems to prove:

   (a) that $G$ contains a subgroup $K$ of order 11 and a subgroup $H$ of order 7;
   This follows directly from the Sylow theorems, since 11 and 7 are primes dividing 77.

   (b) that $H$ and $K$ are normal in $G$;
   It suffices to prove that $H$ and $K$ are unique. But the number of 7 Sylow subgroups divides 11 and is congruent to 1 mod 7, hence is 1, and similarly the number of 11 Sylow subgroups divides 7 and is congruent to 1 mod 11, hence is 1.

   (c) that $G$ is cyclic.
   Since $H$ and $K$ have prime order, they are cyclic. Choose generators $h$ and $k$. Then the commutator $[h, k]$ belongs to $H \cap K = \{e\}$. Hence $h$ and $k$ commute, and hence the order of $hk$ is the gcd of the orders of $h$ and $k$.

4. (10 pts)Let $\theta\colon A \to B$ be a homomorphism of rings. Prove that the kernel of $\theta$ is an ideal of $A$.
   The kernel of $\theta$ is the set $K$ of elements of $A$ such that $\theta(a) = 0$. In particular, $\theta(0) \in K$, and if $a, b \in K$, then $a + b \in K$. If $a \in K$ and $r \in A$, $\theta(ra) = r\theta(a) = r0 = 0$, and similarly for $ar$.

5. (15 pts)Let $p$ be a prime of $\mathbf{Z}$ which is congruent to 1 modulo 4. Prove

   (a) that $-1$ is a square mod $p$.
   Since $p \equiv 1 \pmod 4$, $\mathbf{F}_p^*$ is a cyclic group whose order is divisible by 4, and hence it has two elements or exact order 4. The square of either of these has exact order 2, and hence is $-1$.

   (b) that $p$ can be written as a sum of two squares in $\mathbf{Z}$.
   By the previous part, there is an integer $n$, such that $n^2 + 1$ is divisible by $p$. Then $p$ divides $(n + i)(n - i)$ in the PID $\mathbf{Z}[i]$, but does not divide either factor. Hence $p$ is not irreducible. Hence $p = \alpha\beta$, where $\alpha$ and $\beta$ are not units. Hence $p^2 = N(\alpha)N(\beta)$, and hence $N(\alpha) = p$.

   You may use some major theorems to do this, but state them.