Mathematics 352 – Abstract Algebra II
Midterm Exam 1 Solutions – February 27, 2008

I. *Terminology.*

A) (5) Let G be a group and let x in G. What is the *conjugacy class* of x in G?

Solution: The conjugacy class of x is

$$C_x = \{g^{-1}xg \in G : g \in G\}.$$

(In other words, this is the equivalence class of x for the conjugacy relation on G.)

B) (5) Let K be an extension field of the field F and let $u \in K$. What does it mean to say that u is *transcendental* over F?

Solution: The element $u \in K$ is transcendental over F if there is no nonzero polynomial $f(x) \in F[x]$ such that $f(u) = 0$ (or, equivalently, that u is not algebraic over F.)

1. C) (5) Let K be an extension field of the field F. What does it mean to say that K is *normal* over F?

Solution: K is a normal extension of F if K is algebraic over F and if $p(x)$ is an irreducible polynomial with one root in K, then $p(x)$ splits completely in $K[x]$ (that is, in $K[x]$,

$$p(x) = c(x - u_1) \ldots (x - u_n),$$

so all the roots of $p(x)$ are in K.)

II.

A) (10) State the Structure Theorem for finite abelian groups.

Solution: Every finite abelian group is a direct sum of cyclic subgroups of prime power order.

B) (10) Let $G = \mathbb{Z}_{42} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{84}$. What are the elementary divisors and invariant factors of G?

Solution: From the factorizations $42 = 2 \cdot 3 \cdot 7$, $36 = 2^2 \cdot 3^2$, and $84 = 2^2 \cdot 3 \cdot 7$, we see that the elementary divisors of G are $2, 4, 4, 3, 3, 3^2, 7, 7$, so

$$G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7.$$

Regrouping these as usual, we see the invariant factors of G are $6, 84, 252$, so that

$$G \simeq \mathbb{Z}_6 \oplus \mathbb{Z}_{84} \oplus \mathbb{Z}_{252}.$$

C) (5) What is the Sylow 7-subgroup of G from part B? Is this a cyclic group?

Solution: The Sylow 7-subgroup is isomorphic to $\mathbb{Z}_7 \oplus \mathbb{Z}_7$ from the decompositions above. It is not cyclic. If we take the original direct sum decomposition $G = \mathbb{Z}_{42} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{84} = \langle a \rangle \oplus \langle b \rangle \oplus \langle c \rangle$ then the Sylow 7-subgroup is generated by $(a^6, 0, 0)$ and $(0, 0, c^{12})$ (two elements of order 7).

III.

1. A) (20) State and prove the First Sylow Theorem for finite groups.

Solution: The First Sylow Theorem states that if G is a finite group and p is a prime number such that $p^n \| |G|$, then G contains a subgroup of order p^n.

The proof is by induction on $|G|$. When $|G| = 1$, there is nothing to prove. So now for the induction step, assume that the statement of the theorem is true for all groups of order $< m$ and consider G of order m. By the Class Equation, we have

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C(g_i)],$$

where the g_i are representatives of the distinct conjugacy classes of size > 1 and $C(g_i)$ is the centralizer of g_i.

Case 1: Assume that there is some i such that $[G : C(g_i)]$ is *not* divisible by p. Then $p^n \| |C(g_i)|$. We must have $|C(g_i)| < |G|$ since $g_i \notin Z(G)$. Therefore, by the induction hypothesis, $C(g_i)$ has a subgroup of order p^n. This subgroup is also a subgroup of G and we are done in this case.

Case 2: Now assume that $p | [G : C(g_i)]$ for all $i = 1, \ldots, t$. Then since $p | |G|$, we also have $p | |Z(G)|$. Now $Z(G)$ is a finite abelian group, so we know by a consequence of the Structure Theorem that $Z(G)$ contains an element x of order p. Let $C = \langle x \rangle$ be the subgroup generated by this x. Since $C \subseteq Z(G)$, C is normal in G and we can form G/C which has order divisible by p^{n-1}. By the induction hypothesis applied to G/C, G/C has a subgroup H of order p^{n-1}. But then the inverse image of H under the quotient map $G \longrightarrow G/C$ is a subgroup of G of order p^n.

B) (10) Use the Sylow Theorems to show that every group of order 33 is cyclic.

Solution: By the Third Sylow Theorem, the number of Sylow 3-subgroups is congruent to 1 mod 3 and divides 33. The only possibility is 1, so let H be the unique Sylow 3-subgroup. Similarly, there is exactly one Sylow 11-subgroup K. This implies that H and K are normal subgroups. Moreover $H \cap K = \{e\}$, since if not any $x \neq e$ would simultaneously have order 3 and order 11, which is impossible. Therefore, $G \simeq H \times K \simeq \mathbb{Z}_3 \times \mathbb{Z}_{11} \simeq Z_{33}$, where the last isomorphism follows because $(3, 11) = 1$.

IV.

A) (5) Let K be an extension field of F, and let $u \in K$. Show that if u^2 is algebraic over F, then u is also algebraic over F.

Solution: (Method 1) If u^2 is algebraic over F, then there is some nonzero polynomial $p(x) \in F[x]$ such that $p(u^2) = 0$. This implies that the polynomial $q(x) = p(x^2)$ has u as a root. Therefore u is also algebraic over F. (Note: If $p(x) = a_n x^n + \cdots + a_1 + a_0$, then the polynomial $q(x)$ is just $q(x) = a_n x^{2n} + \cdots + a_1 x^2 + a_0$.)

Solution: (Method 2) Since u^2 is algebraic over F, we know that $[F(u^2) : F] = n$, the degree of the minimal polynomial of u^2 in $F[x]$. Now consider the polynomial $x^2 - u^2 \in F(u^2)[x]$. This has u as a root, so u is algebraic over $F(u^2)$, and $[F(u^2)(u) : F(u^2)] = [F(u) : F(u^2)] \le 2$. Therefore $[F(u) : F] = [F(u) : F(u^2)][F(u^2) : F] \le 2n$ is finite, which implies that u is algebraic over F.

B) (10) Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field of $f(x) = x^4 + 2x^3 - 8x^2 - 6x - 1$ over $\mathbb{Q}$. (Hint: Look for quadratic factors of $f(x)$.)

Solution: The factorization of $f(x)$ in $\mathbb{Q}[x]$ is $f(x) = (x^2 + 4x + 1)(x^2 - 2x - 1)$. The roots of the first factor are $x = \frac{-4 \pm \sqrt{16-12}}{2} = -2 \pm \sqrt{3}$. The roots of the second factor are $x = \frac{2 \pm \sqrt{4+4}}{2} = 1 \pm \sqrt{2}$. Hence the splitting field of $f(x)$ over $\mathbb{Q}$ is, by definition,

$$K = \mathbb{Q}(-2 + \sqrt{3}, -2 - \sqrt{3}, 1 + \sqrt{2}, 1 - \sqrt{2}).$$

We claim that $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The inclusion $K \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is clear since each root of f is contained in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. The other inclusion follows since $\sqrt{2} = \frac{1}{2}(1 + \sqrt{2}) + \frac{-1}{2}(1 - \sqrt{2})$ and $\sqrt{3} = \frac{1}{2}(-2 + \sqrt{3}) + \frac{-1}{2}(-2 - \sqrt{3})$ are both in K. So $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq K$.

V. (15) Show that if $F \subseteq E \subseteq K$ are field extensions and $[E : F], [K : E]$ are both finite, then $[K : F] = [K : E][E : F]$.

Solution: Say $\{u_1, \ldots, u_m\}$ is a basis for E over F and $\{v_1, \ldots, v_n\}$ is a basis for K over F. Then each element a in K can be written as

$$a = c_1 v_1 + \cdots + c_n v_n$$

for some $c_i \in E$. Similarly, we have $c_i = a_{i1} u_1 + \cdots + a_{im} u_m$ were $a_{ij} \in F$. Substituting into the last displayed equation,

$$\begin{aligned} a &= (a_{11} u_1 + \cdots + a_{1m} u_m) v_1 + \cdots + (a_{n1} u_1 + \cdots + a_{nm} u_m) v_n \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} v_i u_j. \end{aligned}$$

This shows that the $m \cdot n$ elements $v_i u_j$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ span K over F. To show that these form a basis of K over F, we need to show that they are linearly independent. Suppose there are $a_{ij} \in F$ such that

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} v_i u_j \\ &= (a_{11}u_1 + \cdots + a_{1m}u_m)v_1 + \cdots + (a_{n1}u_1 + \cdots + a_{nm}u_m)v_n. \end{aligned}$$

Since the v_i are linearly independent over E, this shows that

$$a_{i1}u_1 + \cdots + a_{im}u_m = 0$$

for all $i = 1, \ldots, n$. But then, the u_j are linearly independent over F, so all $a_{ij} = 0$. This shows the linear independence so $\{v_j u_i : 1 \le i \le n, 1 \le j \le m\}$ is a basis of K over F and

$$[K : F] = m \cdot n = [E : F][K : E].$$

Extra Credit (10) Let $p(x)$ and $q(x)$ be irreducible polynomials in $F[x]$ such that $\deg p(x)$ and $\deg q(x)$ are relatively prime integers. Show that if u is a root of $p(x)$ in some extension field of F, then $q(x)$ is also irreducible in $F(u)[x]$.

Solution: If u is a root of $p(x)$ in some extension field of F, then by Theorem 10.7, $[F(u) : F] = \deg p(x) = m$. Similarly if v is a root of $q(x)$, we have $[F(v) : F] = \deg q(x) = n$. Since $m = \deg p(x)$ and $n = \deg q(x)$ are relatively prime, it follows as in Exercise 11 from Section 10.3 of Hungerford that $[F(u,v) : F] = mn$. From the tower $F \subseteq F(u) \subseteq F(u,v)$, we get $[F(u,v) : F] = mn = [F(u,v) : F(u)][F(u) : F]$, so $[F(u,v) : F(u)] = n$. This says that the minimal polynomial of v over $F(u)$ must have degree n, and it must be a divisor of $q(x)$. Since $q(x)$ has degree n itself, that minimal polynomial must be $q(x)$, and hence $q(x)$ is still irreducible in $F(u)[x]$.