Mathematics 352 – Abstract Algebra II
Solutions for Final Exam – May 3, 2008

I. *Terminology.* Answer *any five of the following.* You can earn *up to 10 points Extra Credit* for answering more than five.

(A) (5) What is a *Sylow p-subgroup* of a finite group G?

Solution: If p is prime and $|G| = p^n m$ where $p \not| m$, then a Sylow p-subgroup of G is a subgroup $H \subseteq G$ with $|H| = p^n$.

(B) (5) What is the *class equation* of a finite group?

Solution: The class equation of a group is the equation that says $|G|$ is the sum of the cardinalities of the distinct conjugacy classes. Specifically, since each $c \in Z(G)$ (the center) is the only element in its conjugacy class, we can write the class equation as

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

where $g_1, \ldots, g_t$ are any elements, one from each of the conjugacy classes of size ≥ 2.

(C) (5) What does it mean to say that a point Q in the plane is *constructible*, starting from two given points $O = (0, 0)$, and $P = (1, 0)$?

Solution: It means that Q is obtained after a finite number of steps consisting of constructing new points as the intersection of two lines, or a line and a circle, or two circles, where all lines are formed by joining two previously constructed points (using a straightedge), and all circles have radii with center and opposite endpoint at two previously constructed points.

(D) (5) What is the *degree* of an extension field K of a field F (written $[K : F]$)?

Solution: The degree of K over F is the dimension of K as a vector space over the field of scalars F.

(E) (5) What is the *characteristic* of a field?

Solution: The characteristic of a field is the smallest strictly positive integer n such that

$$n \cdot 1 = 1 + 1 + \cdots + 1 = 0$$

in F, or 0 if there are no such integers $n > 0$.

(F) (5) What is the *Galois group*, $\mathrm{Gal}_F K$, of an extension K of a field F?

Solution: The Galois group is the set of F-automorphisms of K, under the operation of function composition.

(G) (5) What does it mean to say that an extension field K of a field F is *Galois* over F?

Solution: K is Galois over F if $[K : F] < \infty$, and K is normal and separable over F.

(H) (5) What does it mean to say that a finite group G is *solvable*?

Solution: The group G is solvable if there exists a decreasing sequence of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{n-1} \supset G_n = \{e\}$$

such that for each $i = 0, \ldots, n-1$, G_{i+1} is a normal subgroup of G_i, and G_i/G_{i+1} is abelian (equivalently there exists a sequence such that the quotients are cyclic, equivalently, there exists a sequence such that the quotients are cyclic of prime order).

II.

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

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

(B) (20) Classify all finite abelian groups of order $n = 300$. How many different isomorphism classes are there? Give both the elementary divisors and the invariant factors for each isomorphism class.

Solution: Since $300 = 2^2 \cdot 3 \cdot 5^2$, there are four different isomorphism classes. In the diagram below, the left column shows the classification by the elementary divisors and the right shows the classification by the invariant factors:

$$\begin{aligned} \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} &\simeq \mathbb{Z}_{300} \\ (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} &\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{150} \\ \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_5) &\simeq \mathbb{Z}_5 \oplus \mathbb{Z}_{60} \\ (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \oplus \mathbb{Z}_3 \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_5) &\simeq \mathbb{Z}_{10} \oplus \mathbb{Z}_{30}. \end{aligned}$$

III.

(A) (15) State the three Sylow Theorems for finite groups.

Solution: Let G be a finite group

- Sylow I: If and $p^n || |G|$, then G has a subgroup of order p^n.
- Sylow II: If $|G| = p^n m$, where $p \not| m$, then all subgroups of G of order p^n (the Sylow p-subgroups as in I (A)) are conjugate in G.
- Sylow III: The number of Sylow p-subgroups is $\equiv 1 \bmod p$ and divides $|G|$.

(B) (10) Show using the Sylow Theorems that every group G of order $n = 99$ has a non-trivial normal subgroup N (that is, a normal subgroup $N \neq \{e\}, G$).

Solution: Since $99 = 3^2 \cdot 11$, consider the Sylow 3-subgroups in G. By Sylow III, the number of such subgroups must be congruent to 1 mod 3 and must divide 99. Since the only divisors of 99 are $1, 3, 9, 11, 33, 99$, the only possibility is that there is a unique subgroup of order 9. This is normal because of Sylow II.

(C) (10 Extra Credit) Show that every group of order $n = 99$ is isomorphic either to $\mathbb{Z}_9 \times \mathbb{Z}_{11}$ or to $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$.

Solution: The same type of argument done in part (B) works with the Sylow 11-subgroups too and shows there is a unique, normal Sylow 11-subgroup. Let H be the Sylow 3-subgroup and let K be the Sylow 11-subgroup. We see that $H \cap K = \{e\}$ since any element of the intersection must have order simultaneously a power of 3 and a power of 11. It follows that $HK = G$ since the 99 elements of HK are distinct. Hence $G \simeq H \times K$ by Theorem 8.3 in Hungerford. Now H is a group of order $9 = 3^2$, so Corollary 8.29 in Hungerford shows that $H \simeq \mathbb{Z}_9$ or $H \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$. Since K has prime order, K is cyclic, isomorphic to $\mathbb{Z}_{11}$. This shows what we wanted.

IV. (10) Show that if K is an extension field of F and $[K : F] < \infty$, then every element of K is algebraic over F.

Solution: Say $[K : F] = n$. Let $u \in K$ and consider the set $\{1, u, u^2, \cdots, u^n\} \subset K$. Since this set has cardinality $n + 1$ and it lies in an n-dimensional vector space over the field F, it must be linearly *dependent*. That is, there are scalars $c_0, c_1, \ldots, c_n \in F$, not all zero, such that $c_0 + c_1 u + c_2 u^2 + \cdots + c_n u^n = 0$. But this says that u is a root of the polynomial $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n \in F[x]$, and $f(x)$ is not the zero polynomial. Therefore u is algebraic over F.

V. (15) It can be shown, using some slightly tedious but elementary manipulations with trig identities, that the number $x = 2\cos\left(\frac{2\pi}{7}\right)$ is a root of the equation $x^3 + x^2 - 2x - 1 = 0$. What does this imply about the constructibility of the regular 7-gon? Explain.

Solution: It says that the regular 7-gon is *not constructible* by straightedge and compass. The reason is that this cubic polynomial is *irreducible* in $\mathbb{Q}[x]$. Since it is a polynomial of degree 3, to show irreducibility, it is enough to show the polynomial has no rational roots. But the only possible rational roots (by the Rational Roots Test) would be $x = \pm 1$, and neither of them gives zero. Hence $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{7}\right)\right) : \mathbb{Q}\right] = 3$ (by Theorem 10.7). This is not a power of 2, hence $\cos\left(\frac{2\pi}{7}\right)$ is not constructible, and the regular 7-gon is not constructible.

VI. Let K be the splitting field of $x^{64} - x \in \mathbb{Z}_2[x]$, an extension field of $F = \mathbb{Z}_2$.

(A) (10) Show that the mapping $\varphi : K \to K$ given by $\varphi(x) = x^2$ is an F-automorphism of K.

Solution: K is a finite field of order 64 by our main theorem about finite fields. Since $64 = 2^6$, K has characteristic 2. The mapping φ satisfies

$$\begin{aligned} \varphi(a+b) &= (a+b)^2 = a^2 + b^2 = \varphi(a) + \varphi(b) \text{ (the ``freshman dream'')} \\ \varphi(ab) &= (ab)^2 = a^2 b^2 = \varphi(a)\varphi(b) \text{ (since multiplication is commutative in } K). \end{aligned}$$

In addition, each $a \in K$ satisfies $a^{64} = a$, so $(a^{32})^2 = \varphi(a^{32}) = a$. This shows that φ is onto. Since K is a finite set, this implies that φ is also one-to-one. Finally, if $c = 0, 1$ in $\mathbb{Z}_2$, then $\varphi(c) = c^2 = c$. Therefore, φ is an F-automorphism of K.

(B) (10) Show that the mapping φ from part (A) is an element of order 6 in the Galois group $\mathrm{Gal}_F K$. (In fact, $\mathrm{Gal}_F K = \langle\varphi\rangle$ is cyclic of order 6.)

Solution: If $a \in K$ is an arbitrary element, then consider $\varphi^6(a) = (\varphi \circ \varphi \circ \cdots \circ \varphi)(a)$:

$$\varphi^6(a) = \varphi(\varphi(\cdots \varphi(a) \cdots)) = \left((\cdots a^2 \cdots)^2\right)^2 = a^{64}.$$

But every element of K satisfies $a^{64} = a$, so φ^6 is the identity mapping.

(C) (5) Find the orders of all the subfields of K.

Solution: The subfields of K have orders 2^d where $d|6$, so we have subfields of order $2^1 = 2$ (i.e. F), $2^2 = 4$, $2^3 = 8$, and $2^6 = 64$ (i.e K). (*Comment:* Note that these are in one-to-one correspondence with the subgroups of the cyclic group $\langle\varphi\rangle$, so the statements of the Fundamental Theorem of Galois Theory are holding in this example. In fact K is a Galois extension of F.)

VII.

(A) (15) State the Fundamental Theorem of Galois Theory.

Solution: Let K be a Galois extension of F.

(1) The subgroups H of $G = \mathrm{Gal}_F K$ are in one-to-one, inclusion-reversing correspondence with the intermediate fields $F \subseteq E \subseteq K$ via the mappings $H \mapsto E_H = \{a \in K : \sigma(a) = a \text{ for all } \sigma \in H\}$ and $E \mapsto \mathrm{Gal}_E K$. In this correspondence, $[E_H : F] = [G : H]$ and $[K : E_H] = |H|$.

(2) In the correspondence from part (1), the intermediate field E is a normal extension of F if and only if $H = \mathrm{Gal}_E K$ is a normal subgroup of $\mathrm{Gal}_F K$ and if so,

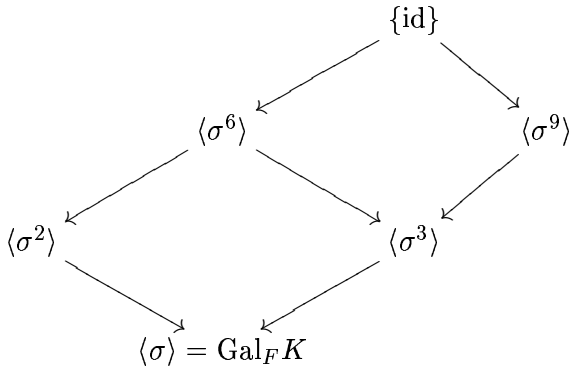
$$\mathrm{Gal}_F K / \mathrm{Gal}_E K \simeq \mathrm{Gal}_F E.$$

(B) (20) Suppose we know that K is a Galois extension of F with $\mathrm{Gal}_F K$ an *abelian* group of order 18 whose Sylow 2- and 3-subgroups are both cyclic. How many intermediate fields E, $F \subseteq E \subseteq K$, are there and what are each of their degrees over F?

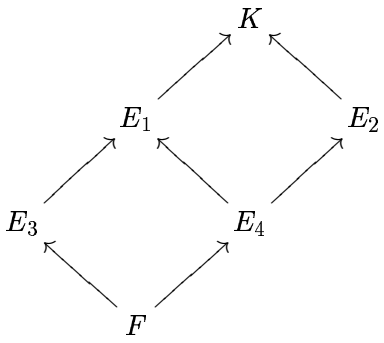
Solution: By the Structure Theorem for finite abelian groups, we must have $\mathrm{Gal}_F K \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_9 \simeq \mathbb{Z}_{18}$, hence this Galois group is cyclic, say $\mathrm{Gal}_F K = \langle\sigma\rangle$. Every subgroup of a cyclic group of order n is cyclic, with order some $d|n$. Moreover, there is exactly one such subgroup for each d. Here $n = 18$, so there are subgroups of orders $1, 2, 3, 6, 9, 18$:

- order 1: $\langle \mathrm{id} \rangle$
- order 2: $\langle \sigma^9 \rangle$
- order 3: $\langle \sigma^6 \rangle$
- order 6: $\langle \sigma^3 \rangle$
- order 9: $\langle \sigma^2 \rangle$
- order 18: $\langle \sigma \rangle = \mathrm{Gal}_F K$.

The following diagram shows the inclusions:



The corresponding diagram of intermediate fields is



where $E_1 = E_{\langle\sigma^6\rangle}$, $E_2 = E_{\langle\sigma^9\rangle}$, $E_3 = E_{\langle\sigma^2\rangle}$, and $E_4 = E_{\langle\sigma^3\rangle}$. By part (1) of the FTGT, we have $[E : F] = [\mathrm{Gal}_F K : \mathrm{Gal}_E K]$ for each intermediate field E. Here

- $[E_1 : F] = [\langle\sigma\rangle : \langle\sigma^6\rangle] = 18/3 = 6$,
- $[E_2 : F] = [\langle\sigma\rangle : \langle\sigma^9\rangle] = 18/2 = 9$,
- $[E_3 : F] = [\langle\sigma\rangle : \langle\sigma^2\rangle] = 18/9 = 2$,
- $[E_4 : F] = [\langle\sigma\rangle : \langle\sigma^3\rangle] = 18/6 = 3$.

VIII. Let p be a prime number and let

$$\zeta_p = \cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right),$$

be the primitive pth root of 1 in $\mathbb{C}$.

(A) (10) Show that if F is a field containing ζ_p and K is the splitting field of the polynomial $x^p - a \in F[x]$ for some $a \in F$ that is not the pth power of any element of F, then $\mathrm{Gal}_F K$ is isomorphic to the additive group $(\mathbb{Z}_p, +)$ (cyclic of order p).

Solution: Let u be any one root of $x^p - a$ in K. Then the roots are $\{u, \zeta_p u, \zeta_p^2 u, \ldots, \zeta_p^{p-1} u\}$. Since $\zeta_p \in F$, this implies that

$$K = F(u, \zeta_p u, \zeta_p^2 u, \ldots, \zeta_p^{p-1} u) = F(u),$$

and the simple extension $K = F(u)$ is actually the splitting field, hence normal. If $\sigma \in \mathrm{Gal}_F K$, then $\sigma(u) = \zeta_p^i u$ for some $i = 0, 1, \ldots, p-1$. Assume $i > 0$, and consider the composition σ^k. We have

$$\sigma^k(u) = (\zeta_p^i)^k u = \zeta_p^{ki} u.$$

Since the smallest positive power of ζ_p that equals 1 is $\zeta_p^p = 1$, and p is prime, this implies the first time we get $\sigma^k(u) = u$ is for $k = p$. In other words, σ is an element of order p in $\mathrm{Gal}_F K$. But since $x^p - a$ has degree p, the dimension $[K : F] \leq p$. It follows that $[K : F] = |\mathrm{Gal}_F K| = p$. Hence $\mathrm{Gal}_F K \simeq \mathbb{Z}_p$.

(B) (10) Show that $\mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta_p)$ is isomorphic to the multiplicative group $(\mathbb{Z}_p^*, \cdot)$ (cyclic of order $p-1$).

Solution: The primitive pth root of unity ζ_p is a root of

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 \in \mathbb{Q}[x].$$

This is an irreducible polynomial, so $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$. The roots of $f(x)$ are $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$, and there are elements of the Galois group mapping ζ_p to each of these powers. Say $\sigma_i(\zeta_p) = \zeta_p^i$. Then $\sigma_i(\sigma_j(\zeta_p)) = (\zeta_p^j)^i = \zeta_p^{(ij)}$. Hence $\sigma_i \circ \sigma_j = \sigma_{ij \bmod p}$. This shows that the mapping

$$\begin{array}{rcl} \varphi : \mathbb{Z}_p^* & \to & \mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta_p) \\ i \bmod p & \mapsto & \sigma_i \end{array}$$

is an isomorphism of groups.

IX. Let ζ_p be as in question VIII, and let K be the splitting field of $x^p - 2 \in \mathbb{Q}[x]$.

(A) (10) Show carefully that $[K : \mathbb{Q}] = p(p-1)$.

Solution: First, note that by the arguments in VIII (A), the field $K = \mathbb{Q}(\alpha, \zeta_p)$ where $\alpha = \sqrt[p]{2}$ (the real, positive root). Note that $\gcd(p, p-1) = 1$ automatically. Hence the desired statement about the degree follows directly from the result we proved in Exercise 11 of Section 10.3. Here is the way this result follows "from first principles." We consider the towers of extensions

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, \zeta_p)$$
$$\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\alpha, \zeta_p)$$

The polynomial $x^p - 2$ is irreducible in $\mathbb{Q}[x]$ (by Eisenstein for the prime 2). Therefore we know $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$. The degree $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ by VIII (B). Hence $[K : \mathbb{Q}]$ must be divisible by both p and $p-1$. However, since $\gcd(p, p-1) = 1$, this implies that the degree must be divisible by $p(p-1)$. But this implies that $[K : \mathbb{Q}] = p(p-1)$ for the following reason. The degree $[K : \mathbb{Q}(\zeta_p)] \leq p$ because the minimal polynomial of α over $\mathbb{Q}(\zeta_p)$ must be some factor of $x^p - a$. Hence $[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_p)][\mathbb{Q}(\zeta_p) : \mathbb{Q}] \leq p(p-1)$. Since $[K : \mathbb{Q}] \leq p(p-1)$, and is divisible by $p(p-1)$, it must equal $p(p-1)$.

(B) (5) Is $\mathrm{Gal}_{\mathbb{Q}} K$ a solvable group? Why or why not?

Solution: Yes, $\mathrm{Gal}_{\mathbb{Q}}K$ *is solvable.* A "fast" proof is to use the Galois Criterion: The Galois group of the splitting field of a polynomial is solvable if and only if the polynomial is solvable by radicals. This is clearly true for the polynomial $f(x) = x^p - a$. We have that the distinct roots are $x = \zeta_p^i \sqrt[p]{a}$ for $i = 0, 1, \ldots, p-1$ (!)

Here is an alternate proof "from first principles." Consider the second tower in the solution for part A. The intermediate field $\mathbb{Q}(\zeta_p)$ is normal over $\mathbb{Q}$, since it is the splitting field of the polynomial $x^p - 1$ in $\mathbb{Q}[x]$. Hence by the second part of the FTGT, we have that the subgroup G_1 corresponding to $\mathbb{Q}(\zeta_p)$ in $G = \mathrm{Gal}_{\mathbb{Q}}K$ is normal and by VIII (B)

$$G/G_1 \simeq \mathrm{Gal}_{\mathbb{Q}}\mathbb{Q}(\zeta_p) \simeq \mathbb{Z}_p^*,$$

which is an abelian group. Moreover by the first part of the FTGT, $G_1 = \mathrm{Gal}_{\mathbb{Q}(\zeta_p)}K$, and this group is isomorphic to $\mathbb{Z}_p$ by VIII (A). This is also abelian. Hence the chain of subgroups

$$G = G_0 \supset G_1 \supset \{id\}$$

shows that G is a solvable group.