Mathematics 352 – Abstract Algebra II
Solutions for Midterm Exam 2 – April 16, 2008

Directions: Place all work you want to have considered for credit in the blue exam book. You have until 9:00pm to work on the exam if you need that much time. There are 100 regular and 10 Extra Credit points. Some partial credit will be given for relevant definitions, statements of theorems, etc. Even if you cannot see how to complete some part, don't leave it blank.

I. *Terminology.*

(A) (5) What does it mean to say that a polynomial $f(x) \in F[x]$ is *separable*?

Solution: The polynomial $f(x)$ is separable if it has *distinct* roots in some (hence all) splitting fields.

(B) (5) What is an *F-automorphism* of a field K containing a subfield F?

Solution: An F-automorphism of K is a mapping $\sigma : K \to K$, such that

- σ is one-to-one and onto,
- for all $a, b \in K$, $\sigma(a+b) = \sigma(a) + \sigma(b)$ and $\sigma(ab) = \sigma(a)\sigma(b)$, and
- for all $c \in F$, $\sigma(c) = c$.

(C) (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 $[K : F]$ is finite and K is normal and separable over F.

II.

(A) (5) State a necessary condition for the real number r to be *constructible* by straightedge and compass, starting from two given points $(0, 0)$ and $(1, 0)$.

Solution: A necessary condition is that $[\mathbb{Q}(r) : \mathbb{Q}] = 2^m$ for some $m \geq 1$.

B) (10) Given a *sphere* of radius 1, is it possible to construct the radius of a sphere with 5 times the volume of the original sphere? Why or why not?

Solution: Not it is not possible. The volume of a sphere of radius r is $\frac{4\pi r^3}{3}$. Hence the radius r of the new sphere would have to satisfy $\frac{4\pi r^3}{3} = 5 \cdot \frac{4\pi}{3}$, or $r^3 - 5 = 0$. The polynomial $x^3 - 5$ is irreducible in $\mathbb{Q}[x]$ (by Eisenstein with $p = 5$, for instance). Therefore if r is any root, $[\mathbb{Q}(r) : \mathbb{Q}] = 3$. Since this is not a power of 2, $r = \sqrt[3]{5}$ is not constructible.

III. Let K be a finite field of order 81.

(A) (5) What is the characteristic of K?

Solution: Since $81 = 3^4$, the characteristic of K would be $p = 3$.

(B) (10) Show that the mapping $\varphi : K \to K$ given by $\varphi(x) = x^3$ is an automorphism of K.

Solution: By the "freshman dream," if $a, b \in K$, then

$$\varphi(a+b) = (a+b)^3 = a^3 + b^3 = \varphi(a) + \varphi(b),$$

and by general rules for exponents (which hold since the multiplication in a field is commutative),

$$\varphi(ab) = (ab)^3 = a^3b^3 = \varphi(a)\varphi(b).$$

The mapping φ is onto because K is a splitting field for $f(x) = x^{81} - x$. This implies that for all $a \in K$, $a = a^{81} = (a^{27})^3 = \varphi(a^{27})$. Therefore, φ is onto. Since K is a finite set, this also implies that φ is one-to-one. Hence φ is an automorphism of K.

(C) (5) Does K have a subfield of order 27? Why or why not?

Solution: No, K has no subfield of order $27 = 3^3$, since $81 = 3^4$ and $3 \not| 4$ (in the exponents).

IV.

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

Solution: Let K be a Galois extension of F.

(1) There is a one-to-one correspondence between subgroups H of $\mathrm{Gal}_F K$ and intermediate fields $F \subseteq E \subseteq K$ given by $H \mapsto E_H$ and $E \mapsto \mathrm{Gal}_E K$. In this correspondence, for each intermediate field E, $[E : F] = [\mathrm{Gal}_F K : \mathrm{Gal}_E K]$, and $[K : E] = |\mathrm{Gal}_E K|$.

(2) The intermediate field E is normal over F if and only if $\mathrm{Gal}_E K$ is a normal subgroup of $\mathrm{Gal}_F K$. If so, then $\mathrm{Gal}_F E \simeq \mathrm{Gal}_F K / \mathrm{Gal}_E K$.

(B) (10) Show that if K is a finite dimensional extension of F, H is a subgroup of $\mathrm{Gal}_F K$, and E is the fixed field $E = E_H$, then K is a simple, normal, separable extension of E.

Solution: (This is the content of Lemma 11.7 in Hungerford.) If u is any element of K, then u is algebraic over F, hence over E as well. If $p(x)$ is the minimal polynomial of u over E, then we know $\sigma(u)$ must be a root of $p(x)$ for all σ in H. Let $u = u_1, u_2, \ldots, u_t$ be the distinct images of u under all the elements in H, and form the polynomial

$$f(x) = (x - u_1)(x - u_2) \cdots (x - u_t).$$

Since each $\sigma \in H$ permutes the roots of f, the coefficients of f must be fixed under σ. Therefore $f(x) \in E[x]$ and is a separable polynomial. This shows that every element u in K is the root of a separable polynomial with coefficients in E, so K is separable over E. By the Primitive Element Theorem, we have $K = E(u)$ for some $u \in K$. But, then applying the above argument for the polynomial $f(x)$ constructed from this u, we see that K is the splitting field of $f(x) \in E[x]$. It follows that K is normal over E (by Theorem 10.15 in Hungerford).

V. Let K be a Galois extension of F with $\mathrm{Gal}_F K = \langle \sigma \rangle$ a cyclic group of order 12.

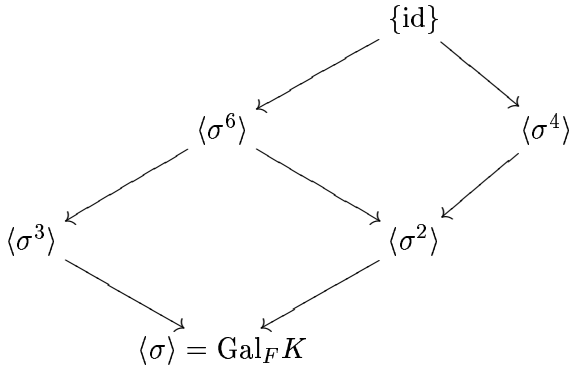
(A) (10) What would the Galois correspondence look like in this case? (Construct the parallel diagrams of subgroups and intermediate fields, showing inclusions, giving the intermediate fields other than F and K "generic" names like E_1, E_2, etc.)

Solution: 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 $n = 12$, so there are subgroups of orders $1, 2, 3, 4, 6, 12$:

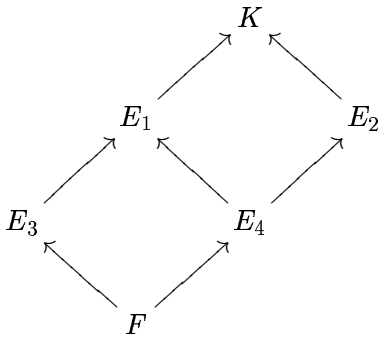
- order 1: $\langle \mathrm{id} \rangle$

- order 2: $\langle \sigma^6 \rangle$
- order 3: $\langle \sigma^4 \rangle$
- order 4: $\langle \sigma^3 \rangle$
- order 6: $\langle \sigma^2 \rangle$
- order 12: $\langle \sigma \rangle = \mathrm{Gal}_F K$.

The following diagram shows the inclusions:



The corresponding diagram of intermediate fields is



where $E_1 = E_{\langle \sigma^6 \rangle}$, $E_2 = E_{\langle \sigma^4 \rangle}$, $E_3 = E_{\langle \sigma^3 \rangle}$, and $E_4 = E_{\langle \sigma^2 \rangle}$.

(B) (5) What are the degrees of each of the intermediate fields over F?

Solution: By part (1) of the FTGT, we have $[E : F] = [\mathrm{Gal}_F K : \mathrm{Gal}_E K]$ for each intermediate field E. Here

- $[E_1 : F] = [\langle \sigma \rangle : \langle \sigma^6 \rangle] = 12/2 = 6$,
- $[E_2 : F] = [\langle \sigma \rangle : \langle \sigma^4 \rangle] = 12/3 = 4$,
- $[E_3 : F] = [\langle \sigma \rangle : \langle \sigma^3 \rangle] = 12/4 = 3$,
- $[E_4 : F] = [\langle \sigma \rangle : \langle \sigma^2 \rangle] = 12/6 = 2$.

(C) (10) Let $E = E_H$ for $H = \langle \sigma^3 \rangle$. Is E a normal extension of F? Why or why not? What is $\mathrm{Gal}_F E$?

Solution: By part (2) of the FTGT, E is normal over F if and only if $\mathrm{Gal}_E K$ is a normal subgroup of $\mathrm{Gal}_F K$. The Galois group $\mathrm{Gal}_F K$ is abelian here so all its subgroups are normal, and the answer to the first part of the question is *yes*. Then

$$\mathrm{Gal}_F E \simeq \mathrm{Gal}_F K / \mathrm{Gal}_E K = \langle \sigma \rangle / \langle \sigma^3 \rangle \simeq \mathbb{Z}_3.$$

Extra Credit (10) Let K be the splitting field of the polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. By Discussion 2, we know that $G = \mathrm{Gal}_{\mathbb{Q}} K \simeq S_3$. What is the fixed field E_H if H is the cyclic subgroup of G of order 3? (In S_3, this is the subgroup generated by the permutation (123).) Compute the fixed field using a basis for K over $\mathbb{Q}$.

Solution: The splitting field of $f(x)$ is $\mathbb{Q}(\alpha, \omega)$, where $\alpha = \sqrt[3]{2}$, and $\omega = \frac{-1+i\sqrt{3}}{2}$ is a primitive cube root of 1, which satisfies $\omega^2 + \omega + 1 = 0$. By Theorem 10.4, a basis for K over $\mathbb{Q}$ is

$$\{1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2\}.$$

The cyclic subgroup of G of order 3 consists of the identity mapping, σ and σ^2 where

$$\begin{aligned} \sigma : \alpha &\mapsto \omega\alpha \\ \omega &\mapsto \omega. \end{aligned}$$

Hence

$$a = a_0 + a_1\alpha + a_2\alpha^2 + a_3\omega + a_4\omega\alpha + a_5\omega\alpha^2$$

is in the fixed field if and only if

$$\begin{aligned} a = \sigma(a) &= a_0 + a_1\omega\alpha + a_2\omega^2\alpha^2 + a_3\omega + a_4\omega^2\alpha + a_5\alpha^2 \\ &= a_0 + a_1\omega\alpha + a_2(-1-\omega)\alpha^2 + a_3\omega + a_4(-1-\omega)\alpha + a_5\alpha^2 \\ &= a_0 - a_4\alpha + (a_5 - a_2)\alpha^2 + a_3\omega + (a_1 - a_4)\omega\alpha - a_2\omega\alpha^2 \end{aligned}$$

Equating coefficients gives

$$\begin{aligned} -a_4 &= a_1 \\ a_5 - a_2 &= a_2 \\ a_1 - a_4 &= a_4 \\ a_5 &= -a_2. \end{aligned}$$

From the second and fourth equations, we get $a_2 = a_5 = 0$. Then the other two equations imply $a_1 = a_4 = 0$ as well. The coefficients a_0, a_3 are arbitrary. Hence the fixed field is $\mathbb{Q}(\omega)$.