Homework 6

Aleck Zhao

March 28, 2017

1. (a) Let $F \to \overline{F}$ be an algebraic closure of F and let $F \to E$ be a finite field extension. Show that there exists an F-embedding of E into $\overline{F}$.

   Proof. Since E and $\overline{F}$ are fields, any homomorphism from E to $\overline{F}$ is injective, so E embeds into $\overline{F}$, as desired.
   (this was too easy, I think I did something wrong) □

   (b) It can be shown that (a) continues to hold when E is only assumed to be algebraic over F. Assuming this fact, show that any two algebraic closures of F are isomorphic as F-algebras.

2. Let F be a field and let $F \to \overline{F}$ an algebraic closure. As a continuation of 6.3 Ex. 21, show that a finite field extension $F \to E$ is normal $\iff$ all F-embeddings of E into $\overline{F}$ have the same image.

Section 6.2: Algebraic Extensions

7. Find the minimal polynomial of $u = \sqrt{3} - i$

   (a) over $\mathbb{R}$.

   Solution. We have $\overline{u} = \sqrt{3} + i$, where

$$\begin{aligned} u + \overline{u} &= 2\sqrt{3} \\ u\overline{u} &= 4 \end{aligned}$$

   so the minimal polynomial over $\mathbb{R}$ is given by

$$m = x^2 - 2\sqrt{3}x + 4$$

□

   (b) over $\mathbb{Q}$.

   Solution. We have

$$\begin{aligned} u^2 &= (\sqrt{3} - i)^2 = 2 - 2\sqrt{3}i \\ \implies u^2 - 2 &= -2\sqrt{3}i \\ \implies (u^2 - 2)^2 &= -12 \\ \implies u^4 - 4u^2 + 16 &= 0 \end{aligned}$$

   which is irreducible over $\mathbb{Q}$ by the Rational Root Theorem, so the minimal polynomial over $\mathbb{Q}$ is given by

$$m = x^4 - 4x^2 + 16$$

□

19. Let $\mathbb{C} \supseteq E \supseteq \mathbb{Q}$, where E is a field, and assume that $[E : \mathbb{Q}] = 2$. Show that $E = \mathbb{Q}(\sqrt{m})$, where m is a square-free integer.

Proof. Consider an element $u \in E \setminus \mathbb{Q}$. Since $[E : \mathbb{Q}] = 2$, a polynomial $f \in \mathbb{Q}[x]$ exists of degree 1 or 2 such that $f(u) = 0$. If $\deg f = 1$, then $f = x - u$, but $u \notin \mathbb{Q}$, so f would not be in $\mathbb{Q}[x]$, so f must have degree 2.

Suppose $f = ax^2 + bx + c$ for $a, b, c \in \mathbb{Q}$. Then u is algebraic over $\mathbb{Q}$ with degree 2, so $[\mathbb{Q}(u) : \mathbb{Q}] = 2$, and since $\mathbb{Q} \subseteq E$ and $u \in E$, it follows that $\mathbb{Q}(u) \subseteq E$, and since $[\mathbb{Q}(u) : \mathbb{Q}] = [E : \mathbb{Q}] = 2$, we must have $\mathbb{Q}(u) = E$. Now, solving for u, we have

$$u = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

so

$$\begin{aligned}\mathbb{Q}(u) &= \mathbb{Q}\left(\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}\right) \\ &= \mathbb{Q}(\sqrt{b^2 - 4ac})\end{aligned}$$

if $b^2 - 4ac$ is not square-free, then suppose $b^2 - 4ac = n^2 m$ where n is as large as possible and m is square-free. Then

$$\mathbb{Q}(\sqrt{b^2 - 4ac}) = \mathbb{Q}(\sqrt{n^2 m}) = \mathbb{Q}(n\sqrt{m}) = \mathbb{Q}(\sqrt{m})$$

as desired. □

21. Let $E \supseteq F$ be fields, and let $u, v \in E$ be algebraic over F of degrees m, n.

(a) Show that $[F(u, v) : F] \leq mn$.

Proof. We have

$$[F(u, v) : F] = [F(u, v) : F(v)][F(v) : F]$$

Since $[F(u) : F] = m$, that means the minimal polynomial $f \in F[x]$ of u has degree m. Then consider the minimal polynomial of u in $F(v)[x]$. Obviously since this field contains $F[x]$, the minimal polynomial must have degree at most m, so $[F(u, v) : F(v)] \leq m$. Thus,

$$[F(u, v) : F] = [F(u, v) : F(v)][F(v) : F] \leq mn$$

as desired. □

(b) If m and n are relatively prime, show that $[F(u, v) : F] = mn$.

Proof. Since

$$\begin{aligned}[F(u, v) : F] &= [F(u, v) : F(v)][F(v) : F] = n \cdot [F(u, v) : F(v)] \\ [F(u, v) : F] &= [F(u, v) : F(u)][F(u) : F] = m \cdot [F(u, v) : F(u)]\end{aligned}$$

it follows that m and n both divide $[F(u, v) : F]$, and since they are relatively prime, we must have $[F(u, v) : F] \geq mn$. This and the result of part (a) show that $[F(u, v) : F] = mn$, as desired. □

(c) Is the converse to (b) true?

Solution. No. Let $E = \mathbb{C}, F = \mathbb{Q}, u = \sqrt{2}, v = \sqrt{3}$. Then $m = n = 2$ are not relatively prime, but $[\mathbb{Q}(\sqrt{2}, \sqrt{3} : \mathbb{Q}] = 4 = 2 \cdot 2$ but 2 is not relatively prime with 2. □

32. Let p and q in $\mathbb{Q}$ satisfy $\sqrt{p} \notin \mathbb{Q}$ and $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$.

(a) Show that $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.

Proof. Let $u = \sqrt{p} + \sqrt{q}$. Then

$$u^3 = (p + 3q)\sqrt{p} + (q + 3p)\sqrt{q} \in \mathbb{Q}(u) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q})$$

Now, we have

$$\begin{aligned} u^{-1} &= \frac{1}{\sqrt{p} + \sqrt{q}} = \frac{\sqrt{p} - \sqrt{q}}{p - q} \\ \implies (p - q)u^{-1} &= \sqrt{p} - \sqrt{q} \end{aligned}$$

so

$$\begin{aligned} u + (p - q)u^{-1} = 2\sqrt{p} &\implies \sqrt{p} \in \mathbb{Q}(u) \\ u - (p - q)u^{-1} = 2\sqrt{q} &\implies \sqrt{q} \in \mathbb{Q}(u) \end{aligned}$$

Thus, $\mathbb{Q}(\sqrt{p}, \sqrt{q}) \subseteq \mathbb{Q}(u)$, so in fact

$$\mathbb{Q}(u) = \mathbb{Q}(\sqrt{p} + \sqrt{q}) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$$

as desired. □

(b) Use Theorem 5 to find a basis of $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ over $\mathbb{Q}$.

Solution. Let $K = \mathbb{Q}(\sqrt{p})$ and $L = \mathbb{Q}(\sqrt{p}, \sqrt{q}) = K(\sqrt{q})$. Since $\sqrt{p} \notin \mathbb{Q}$, the minimal polynomial of $\sqrt{p}$ in $\mathbb{Q}$ has degree 2, and is $x^2 - p$, so a $\mathbb{Q}$-basis for K is $\{1, \sqrt{p}\}$.
Now, we claim that $x^2 - q$ is the minimal polynomial of $\sqrt{q}$ over K. Clearly $\sqrt{q}$ is a root of this polynomial. If $\sqrt{q}$ was the root of the degree 1 polynomial $x - \sqrt{q}$, then we must have $\sqrt{q} \in K = \mathbb{Q}(\sqrt{p})$, but this is a contradiction since we know $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. Thus, $\{1, \sqrt{q}\}$ is a K-basis for L.
Thus by Theorem 5,

$$[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = [K(\sqrt{q}) : K][K : \mathbb{Q}] = 4$$

and a $\mathbb{Q}$ basis for $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ is $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$. □

(c) Deduce that $x^4 - 2(p + q)x^2 + (p - q)^2$ is the minimal polynomial of $\sqrt{p} + \sqrt{q}$ over $\mathbb{Q}$.

Solution. Since $[\mathbb{Q}(\sqrt{p} + \sqrt{q}) : \mathbb{Q}] = 4$, the minimal polynomial has degree 4. It remains to verify that $\sqrt{p} + \sqrt{q}$ is actually a root. We have

$$\begin{aligned} (\sqrt{p} + \sqrt{q})^4 &= p^2 + 4p\sqrt{pq} + 6pq + 4q\sqrt{pq} + q^2 \\ -2(p + q)(\sqrt{p} + \sqrt{q})^2 &= -2p^2 - 2q^2 - 4pq - 4(p + q)\sqrt{pq} \\ (p - q)^2 &= p^2 - 2pq + q^2 \end{aligned}$$

and summing these equations yields 0 on the RHS, as desired. □

Section 6.3: Splitting Fields

3. If $2 \neq 0$ in the field F, show that the splitting field E of x^4+1 over F is a simple extension of F and factors x^4+1 completely in $E[x]$. What happens if $2=0$ in F?

   Proof. If E is a splitting field of x^4+1, then

   $$x^4+1=(x-u_1)(x-u_2)(x-u_3)(x-u_4)$$

   for $u_1, u_2, u_3, u_4 \in E$. Expanding the RHS, the coefficient of x^3 is $-(u_1+u_2+u_3+u_4)$ which must be 0 by comparing coefficients.

   If $2=0$ in F, then $x^4+1=x^4+4x^3+6x^2+4x+1=(x+1)^4$ splits entirely in F. □

21. Show that the following conditions are equivalent for fields $E \supseteq F$:

    1. E is the splitting field of a polynomial in $F[x]$.
    2. $[E:F]$ is finite and every irreducible polynomial in $F[x]$ with a root in E splits completely in $E[x]$.

    Proof. $1 \implies 2$: Suppose E is the splitting field of $f \in F[x]$ where $\deg f = n$. Then f factors into n linear factors:

    $$f=a(x-u_1)\cdots(x-u_n)$$

    where $u_i \in E$ and since $E=F(u_1,\cdots,u_n)$, this is a finite extension so $[E:F]$ is finite. If $p \in F[x]$ is irreducible over F with a root $u \in E$, and let v be a root of p in a field $K \supseteq E$. Then since p is the minimal polynomial of both u and v so $F(u) \cong F(v)$. Let $\sigma : F(u) \to F(v)$ be an isomorphism. Since E is the splitting field of f over $F(u)$ and $E(v)$ is the splitting field of f over $F(v)$, it follows from Theorem 3 that $E \cong E(v)$ by extending σ. Thus

    $$\begin{aligned} [E:F(u)] &= [E(v):F(v)] \\ \implies [E:F] &= [E:F(u)][F(u):F] \\ &= [E(v):F(v)][F(v):F] \\ &= [E(v):F] \end{aligned}$$

    so since E is a vector space over F contained in $E(v)$, we must have $E=E(v)$, so $v \in E$. Thus, p splits completely in $E[x]$, as desired.

    $2 \implies 1$: Since $[E:F]$ is finite, E is a finite extension of F, so by Theorem 6, we have $E=F(u_1,\cdots,u_n)$ for $u_i \in E$ algebraic over F. Let $f_1,\cdots,f_n$ be the minimal polynomials of $u_1,\cdots,u_n$, respectively, in $F[x]$. Since each of the f_i has a root in E, it splits entirely in $E[x]$, so does the product $f=f_1\cdots f_n$, and E is the splitting field of $f \in F[x]$. □