Homework 3 Solutions

February 10, 2019

13.4.1 Determine the splitting field and its degree over $\mathbb{Q}$ for x^4-2.

Solution. (Thomas) Note that over $\mathbb{C}$, $x^4-2=(x^2+\sqrt{2})(x^2-\sqrt{2})=(x+i2^{1/4})(x-i2^{1/4})(x+2^{1/4})(x-2^{1/4})$. Then the splitting field of x^4-2 over $\mathbb{Q}$ is $\mathbb{Q}(2^{1/4},-2^{1/4},i2^{1/4},-i2^{1/4})=\mathbb{Q}(2^{1/4},i)=\big(\mathbb{Q}(2^{1/4})\big)(i)$. Since x^4-2 is irreducible over $\mathbb{Q}$ by Eisenstein, we note that this is the minimal polynomial of $2^{1/4}$ so $[\mathbb{Q}(2^{1/4}):\mathbb{Q}]=4$ and, since this minimal polynomial of i over $\mathbb{Q}$ is famously x^2+1, $[\mathbb{Q}(2^{1/4})(i):\mathbb{Q}(2^{1/4})]=2$ so $[\mathbb{Q}(2^{1/4},i):\mathbb{Q}]=[\mathbb{Q}(2^{1/4})(i):\mathbb{Q}(2^{1/4})][\mathbb{Q}(2^{1/4}):\mathbb{Q}]=(2)(4)=8$. □

!

13.4.2 Determine the splitting field and its degree over $\mathbb{Q}$ for x^4+2.

Solution. (Thomas) Note that over $\mathbb{C}$, $x^4+2=(x^2+i\sqrt{2})(x^2-i\sqrt{2})=(x^2-i^3\sqrt{2})(x^2-i\sqrt{2})=(x+\sqrt{i\sqrt{2}})(x-\sqrt{i\sqrt{2}})(x+\sqrt{i^3\sqrt{2}})(x-\sqrt{i^3\sqrt{2}})$. Note that $\sqrt{i}=\sqrt{2}/2+i\sqrt{2}/2$ and $\sqrt{i^3}=-\sqrt{2}/2+i\sqrt{2}/2$. Then $(x+\sqrt{i\sqrt{2}})(x-\sqrt{i\sqrt{2}})(x+\sqrt{i^3\sqrt{2}})(x-\sqrt{i^3\sqrt{2}})=(x+(-\sqrt{2}/2+i\sqrt{2}/2)2^{1/4})(x-(-\sqrt{2}/2+i\sqrt{2}/2)2^{1/4})(x+(\sqrt{2}/2+i\sqrt{2}/2)2^{1/4})(x-(\sqrt{2}/2+i\sqrt{2}/2)2^{1/4})=(x-(-2^{3/4}/2+i2^{3/4}/2))(x-(2^{3/4}/2-i2^{3/4}/2))(x-(2^{3/4}/2+i2^{3/4}/2))(x-(-2^{3/4}/2-i2^{3/4}/2))$. So the splitting field over $\mathbb{Q}$ of x^4+2 is $\mathbb{Q}(2^{3/4}/2-i2^{3/4}/2, 2^{3/4}/2+i2^{3/4}/2, -2^{3/4}/2-i2^{3/4}/2, -2^{3/4}/2+i2^{3/4}/2)=\mathbb{Q}(2^{3/4},i)$. Note that x^4-8 is irreducible over $\mathbb{Z}/3\mathbb{Z}$ and thus irreducible over $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. Then since x^4-8 has $2^{3/4}$ as a root we see $[\mathbb{Q}(2^{3/4}):\mathbb{Q}]=4$ so the degree of $\mathbb{Q}(2^{3/4},i)$ is 8. □

13.4.3 Determine the splitting field and its degree over $\mathbb{Q}$ for x^4+x^2+1.

Solution. (Thomas) Note that $x^4+x^2+1=(x^2+x+1)(x^2-x+1)$. Then by the quadratic formula, x^4+x^2+1 has the roots $\pm\frac{1}{2}\pm\frac{\sqrt{3}}{2}i$ so the splitting field for x^4+x^2+1 is $\mathbb{Q}(\pm\frac{1}{2}\pm\frac{\sqrt{3}}{2}i)=\mathbb{Q}(\sqrt{-3})$ which is the root of the irreducible polynomial (by Eisenstein) x^2+3 so the degree of $\mathbb{Q}(\sqrt{-3})$ is 2. □

13.4.4 Determine the splitting field and its degree over $\mathbb{Q}$ for x^6-4.

6?

Solution. (Thomas) Note that $x^6-4=(x^3-2)(x^3+2)$ so the splitting field for x^6-4 is $\mathbb{Q}(2^{1/4},2^{1/3},i)=\mathbb{Q}(2^{1/3},i)$ which has degree 8 by 13.4.1. □

impossible

$3!=6$ and $8 \nmid 6$.

§13.4 #5 Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$. [Use Theorems 8 and 27].

Proof. We first suppose that every irreducible polynomial in $F[x]$ with a root in K splits completely in $K[x]$. Suppose K has basis elements $\alpha_1,\alpha_2,\ldots,\alpha_n$. Then if $M=\{m_{\alpha_i,F}(x)\}$ is the collection of minimal polynomials for the α_i, K is a splitting field for M: clearly, all the irreducible polynomials in M have a root in K, so they split completely in $K[x]$, and as the set $\{\alpha_i\}$ is a basis for K, the minimality condition for K to be a splitting field is satisfied as well.

Next, suppose K is a splitting field for some collection of polynomials in $F[x]$. Because K is finite, we may assume that K is in fact the splitting field for some single polynomial $f(x)\in F[x]$. Let $\sigma: K\to\sigma(K)$ be an F-embedding of K into $\overline{F}$. Choose $\alpha\in K\setminus F$. Then by the minimality of splitting fields, α is a root of f.

No.

No: Eg. $f(x)=(x^2-2)(x^2-\sqrt{3})$ then $\sqrt{2}+\sqrt{3}$ is not a root of $f(x)$, but is an element of its s.f.

Because σ is the identity on F, we have that $\sigma(f(\alpha)) = \sigma(0) = 0$, while $\sigma(f(\alpha)) = f(\sigma(\alpha))$. Thus, $\sigma(\alpha)$ is a root of f. We note two things: first, that $\sigma(\alpha) \in K$, and second that σ injectively permutes the roots of f, and as there are only finitely many roots of any polynomial, σ must be a bijection from K to K - i.e., σ is in fact an automorphism of K.

Choose a new, arbitrary $\alpha \in K$ and let $m_\alpha(x)$ be the minimal polynomial of α over F. Let $\{\alpha_i\}$ be the conjugates of α in $\overline{F}$ - the other roots of $m_\alpha(x)$. Because $m_\alpha(x)$ is irreducible, we know that for each i, there exists an F-embedding σ mapping α to α_i. However, we know that all such F-embeddings are K-automorphisms, so $\alpha_i \in K$, and $m_\alpha(x)$ splits entirely over K. □

§13.4 #6 Let K_1 and K_2 be finite extensions of F contained in the field K, and assume both are splitting fields over F.

(a) Prove that their composite K_1K_2 is a splitting field over F.

(b) Prove that $K_1 \cap K_2$ is a splitting field over F. [Use the preceding exercise.]

Proof:

(a) Suppose K_1 is the splitting field for some collection of polynomials $\{f_i\} \subseteq F[x]$, and K_2 is the splitting field for some other collection of polynomials $\{g_i\} \subseteq F[x]$. Then we claim K_1K_2 is the splitting field for the collection $\{f_i \cdot g_j\} \subseteq F[x]$.

Clearly, K_1K_2 contains all the roots of polynomials of the form $f_i \cdot g_k(x)$, as all the roots of f_i are in K_1, and all the roots of g_k are in K_2. Moreover, the splitting field for $\{f_i \cdot g_k\}$ must contain all the roots of all the polynomials f_i and all the roots of the polynomials g_k, and the composite field K_1K_2 is the smallest extension field containing both K_1 and K_2. Thus, K_1K_2 is minimal, and the splitting field for the collection $\{f_i \cdot g_k\}$ over F. □

See notes.

(b) Once again, suppose K_1 is the splitting field for some collection of polynomials $\{f_i\} \subseteq F[x]$, and K_2 is the splitting field for some other collection of polynomials $\{g_i\} \subseteq F[x]$. Then we claim that $K_1 \cap K_2$ is the splitting field for $\{f_i\} \cap \{g_k\}$.

Suppose $k(x) \in \{f_i\} \cap \{g_k\}$. Then $k(x)$ splits completely over both K_1 and K_2, so all the roots of $k(x)$ will be in both K_1 and K_2, and therefore in $K_1 \cap K_2$. Thus, $k(x)$ splits completely over $K_1 \cap K_2$. Conversely, suppose $\alpha \in K_1 \cap K_2$. If $m(x)$ is the minimal polynomial for α, then since $\alpha \in K_1$, by the previous exercise $m(x)$ splits completely over $K_1[x]$, and $m(x) \in \{f_i\}$. Similarly, since $\alpha \in K_2$, we have that $m(x) \in \{g_k\}$, so $m(x) \in \{f_i\} \cap \{g_k\}$. Thus, $K_1 \cap K_2$ is minimal, and is the splitting field for $\{f_i\} \cap \{g_k\}$. □

Slight problem. If $f_1 = 2x^2+2$ and $g_1 = x^2+1$ then $\{f_1\} \cap \{g_1\} = \emptyset$, but $K_1 \cap K_2 = \mathbb{Q}(i)$.

$\sqrt{2}$. Prove that the following are equivalent for a field L:

(a) Every polynomial of positive degree over L has a root in L.

(b) Every polynomial in $L[x]$ has all its roots in L.

(c) The only irreducible polynomials over L are the linear ones: $ax + b$, $a \neq 0, a, b \in L$.

(d) If M is an algebraic extension of L, then $M = L$.

Proof. We first show that (a) implies (b). So, suppose that every polynomial of positive degree over L has a root in L. If f is a polynomial in $L[x]$, then we will show that f has all its roots in L via induction on $n = \deg f$. Suppose $n = 1$. Then f has only one root, and by assumption, that root must be in L.

So, suppose that all polynomials of degree strictly less than n have all their roots in L, and suppose f has degree n. By assumption, f has a root in L, which we will call α. Then

$f(x) = (x - \alpha)f_1(x)$, where the degree of $f_1(x)$ is strictly less than n. By the inductive hypothesis, all the roots of $f_1(x)$ are in L, so all the roots of f are in L.

Next, we will show that (b) implies (c). If all the polynomials in $L[x]$ have all their roots in L, then every polynomial in $L[x]$ splits completely in L - that is, we can factor it into linear factors. Thus, if f is a nonconstant, nonlinear polynomial, it factors nontrivially into linear factors. As the constant polynomials are units, this leaves only the linear polynomials (which are always irreducible) as the only irreducible elements of $L[x]$.

To see that (c) implies (d), we first let M be an algebraic extension of L. Then choose $\alpha \in M$, and let $m(x)$ be the minimal polynomial for α. Because $m(x)$ must be irreducible, it must be a linear polynomial, and therefore α must be in L. Thus, $M = L$.

Finally, we will show that (d) implies (a). Let $f(x)$ be a polynomial of positive degree in over L, and let α be a root of L. Then $L(\alpha)$ is an algebraic extension of L. However, by assumption, $L(\alpha) = L$, so $\alpha \in L$, and f has a root in L. $\square$

Nice.

13.4

#6b. Consider $K_1 \cap K_2$ and $\alpha \in K_1 \cap K_2$. Since $\alpha \in K_1$ and K_1 is a splitting field over F, by the last problem (#5), the minimal polynomial $m_{\alpha,F}(x)$ has all its roots in K_1. Similarly, all the conjugates of α are in K_2. Thus, all the conjugates of α are in $K_1 \cap K_2$. Either again by #5 or by taking $S = \{m_{\alpha,F}(x) \mid \alpha \in K_1 \cap K_2\}$, we see that $K_1 \cap K_2$ is a splitting field over F.

Homework 3 solution

due: February 11, 2019

Because I think I am going to like Jeremy's solution, I am writing up mine too (which I also like).

13.4 : 2 Determine the splitting field and its degree over $\mathbb{Q}$ for $f(x) = x^4 + 2$

Proof. First we prove the following claim.

Claim: The splitting field of $f(x)$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\omega, \sqrt[4]{2})$ where ω is a primitive 8th root of unity.

First note that the roots of $f(x)$ are $\omega\sqrt[4]{2}$, $\omega^3\sqrt[4]{2}$, $\omega^5\sqrt[4]{2}$, and $\omega^7\sqrt[4]{2}$, and therefore K contains a splitting field for $f(x)$ over $\mathbb{Q}$. By the last problem, if $L = \mathbb{Q}(i, \sqrt[4]{2})$, then $[L : \mathbb{Q}] = 8$. Indeed, $L = K$ since it is clear that $L \subseteq K$ and since $\omega = \dfrac{\sqrt{2}}{2}(1+i) \in Q(i, \sqrt[4]{2})$, $K \subseteq L$. Thus, we have established that the splitting field of $f(x)$ over $\mathbb{Q}$ is contained in K and has degree dividing 8.

Consider now the intermediate field $\mathbb{Q}(\omega\sqrt[4]{2})$, $\mathbb{Q} \subseteq \mathbb{Q}(\omega\sqrt[4]{2}) \subseteq K = L$ which has degree 4 over $\mathbb{Q}$. Then $M = \mathbb{Q}(\omega\sqrt[4]{2})$ does not contain the root $\omega^3\sqrt[4]{2}$ of $f(x)$ since if it did, then as the following computations hold this field would also contain the elements i, $\sqrt{2}$, ω, and $\sqrt[4]{2}$:

$$i = \frac{\omega^3\sqrt[4]{2}}{\omega\sqrt[4]{2}} = \omega^2, \quad \frac{(\omega\sqrt[4]{2})^3}{\omega^3\sqrt[4]{2}} = \sqrt{2}, \qquad \omega = \frac{\sqrt{2}}{2}(1+i), \quad \sqrt[4]{2} = \frac{\omega\sqrt[4]{2}}{\omega}.$$

and the degree of M over $\mathbb{Q}$ would be 8 since $M = K = L$, and not 4.

Finally, since M is not the splitting field of $f(x)$ over $\mathbb{Q}$, $[K : M] = 2$, and K does contain a splitting field of $f(x)$ over $\mathbb{Q}$, the claim follows. Since $K = L$, the degree over $\mathbb{Q}$ is 8.

Alternatively, and this is the way I actually solved the problem, once you establish that M is *not* the splitting field of $f(x)$ over $\mathbb{Q}$, we could show that $\omega \notin M$ has minimal polynomial

$$m(x) = x^2 - (\omega\sqrt[4]{2})^2 x - 1 \in M[x],$$

and the result follows. $\square$