Allman feedback.

Homework 5 Solutions

February 25, 2019

$(x^3+2)(x^3-2)$

$= (x+\sqrt[3]{2})(x^2-\sqrt[3]{2}x+\sqrt[3]{4})(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$

§13.4 #4 Determine the splitting field and its degree over $\mathbb{Q}$ for $x^6 - 4$.

Proof. (Thomas) Let $p = 4^{1/6}$ and $w = e^{\frac{2*\pi*i}{6}}$ and observe that over $\mathbb{C}$, $x^6 - 4 = (x - p)(x - wp)(x - w^2p)(x - w^3p)(x - w^4p)(x - w^5p)$. Then the splitting field of $x^6 - 4$ is $F = \mathbb{Q}(p, wp, w^2p, w^3p, w^4p, w^5p) = \mathbb{Q}(4^{1/6}, e^{\frac{2\pi i}{6}}4^{1/6}, e^{\frac{(2)2\pi i}{6}}4^{1/6}, e^{\frac{(3)2\pi i}{6}}4^{1/6}, e^{\frac{(4)2\pi i}{6}}4^{1/6}, e^{\frac{(5)2\pi i}{6}}4^{1/6})$. Note that $4^{\frac{1}{6}} = 2^{\frac{1}{3}}$ and that $(4^{\frac{1}{6}})^5 * w4^{\frac{1}{6}} = w$ so $w \in F$. Then we can express every basis element of F as a vector space as a $\mathbb{Q}$-linear combination of $2^{\frac{1}{3}}$ and w so $F = \mathbb{Q}(2^{\frac{1}{3}}, w)$. Note that $\mathbb{Q}(2^{\frac{1}{3}})$ is the splitting field for $x^3 - 2$ which is irreducible by Eisenstein with 2 and that $w \notin \mathbb{Q}(2^{\frac{1}{3}})$ so $[\mathbb{Q}(2^{\frac{1}{3}})(w) : \mathbb{Q}(2^{\frac{1}{3}})] = \phi(6) = 2$ so the degree of F is $(3)(2) = 6$. □

§13.5 #5 For any prime p and any nonzero $a \in \mathbb{F}_p$ prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$. [For the irreducibility: One approach—prove first that if α is a root then $\alpha + 1$ is also a root. Another approach—suppose it's reducible and compute derivatives.]

Proof. (Thomas) Let $f(x) = x^p - x + a$. We will show that if α is a root then $\alpha + 1$ is also a root. Observe that $f(\alpha+1) = (\alpha+1)^p - (\alpha+1) + a = \alpha^p + 1^p - \alpha - 1 + a = \alpha^p - \alpha + a = f(\alpha)$. It follows inductively that if $f(x)$ has a root in $\mathbb{F}_p$ then $f(x)$ has p distinct roots in $\mathbb{F}_p$ since $\mathbb{F}_p$ has characteristic p. Then we see that every root of $f(x)$ in $\mathbb{F}_p$ is distinct and thus $f(x)$ is seperable.

Suppose for the sake of contradiction that $f(x)$ is reducible over $\mathbb{F}_p$. Then $f(x) = f_1(x) \dots f_n(x)$ for irreducible $f_i(x)$ and assume WOLOG that each $f_i(x)$ is monic. Note that $n > 1$ since $f(x)$ is reducible. Then let α_1 be a root of $f_1(x)$ and note that $f_1(x)$ is the minimimal polynomial of α_1 since otherwise it would be reducible (since minimal polynomials divide any polynomial that shares a root). Similarly, $f_2(x)$ is the minimal polynomial of some α_2. Note that $\alpha_1 = \alpha_2 + \alpha_3$ for some $\alpha_3 \in \mathbb{F}_p$ since any root is simply a translation of every other root by the seperability proof above. Then $f_1(x+\alpha_3)$ has α_2 as a root and is the minimal polynomial of α_2 since shifting a polynomial does not affect reducibility. But this means that $deg(f_1) = deg(f_2)$. Since $f_1(x), f_2(x)$ may be any factors of $f(x)$ up to ordering, we see that every divisor of $f(x)$ has the same degree. Since the degree of $f(x)$ is p, a prime, we see that every factor of $f(x)$ is linear and $f(x)$ has a root in $\mathbb{F}_p$. Let b be a root of $f(x)$ in $\mathbb{F}_p$. Note that since $b \in \mathbb{F}_p$, b is a root of $x^p - x$ so $b^p - b = 0$. Then $0 = f(b) = b^p - b + a = a$ which is a contradiction since $a \neq 0$. It follows then that $f(x)$ does not have any roots in $\mathbb{F}_p$, and we see that $f(x)$ cannot factor linearly which is a contradiction so we see $f(x)$ is irreducible over $\mathbb{F}_p$. □

"linear change of variable"

Good.

§14.1 #1 (a) Show that if the field K is generated over F by the elements $\alpha_1, \dots, \alpha_n$ then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$. In particular show that an automorphism fixes K if and only if it fixes a set of generators for K.

Proof. (Thomas) Let $x \in K$ and note that $x = \frac{f(\alpha_1,\dots,\alpha_n)}{g(\alpha_1,\dots,\alpha_n)}$ for $g \neq 0$. Then $\sigma(x) = \sigma(\frac{f(\alpha_1,\dots,\alpha_n)}{g(\alpha_1,\dots,\alpha_n)}) = \sigma(f(\alpha_1, \dots, \alpha_n))\sigma(g(\alpha_1, \dots, \alpha_n))^{-1} =$
$f(\sigma(\alpha_1), \dots, \sigma(\alpha_n))g(\sigma(\alpha_1), \dots, \sigma(\alpha_n))^{-1} = \frac{f\left(\sigma(\alpha_1),\dots,\sigma(\alpha_n)\right)}{g\left(\sigma(\alpha_1),\dots,\sigma(\alpha_n)\right)}$ since σ is an automorphism (respecting addition and multiplication) that fixes F. Thus σ is entirely determined by $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$.

It follows immediately that if an automorphism fixes the generators of K, it fixes K. Since an automorphism that fixes K fixes the generators of K, we see that an automorphism fixes K if and only if it fixes a set of generators for K. □

(b) Let $G \leq \mathrm{Gal}(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \dots, \sigma_k$ are generators for G. Show that the subfield E/F is fixed by G if and only if it is fixed by the generators $\sigma_1, \dots, \sigma_k$.

Proof. (Thomas) Suppose the subfield E/F is fixed by G. Then since the generators of G are in G, we see that E/F is fixed by the generators $\sigma_1, \dots, \sigma_k$.
Suppose E/F is fixed by the generators $\sigma_1, \dots, \sigma_k$ of G. Then choose $g \in G$ and note that g is a product of the generators of G so g fixes E/F. □

§14.1 #2 Let τ be the map $\tau : \mathbb{C} \to \mathbb{C}$ defined by $\tau(a + bi) = a - bi$ (*complex conjugation*). Prove that τ is an automorphism of $\mathbb{C}$.

Proof. (Thomas) Let $x, y \in \mathbb{C}$ and note that $\tau(xy) = \overline{xy} = \bar{x}\bar{y} = \tau(x)\tau(y)$ and that $\tau(x+y) = \overline{x+y} = \bar{x} + \bar{y} = \tau(x) + \tau(y)$ so τ is operation preserving and is thus a homomorphism.

Note that $\tau(\tau(z)) = \tau(\bar{z}) = z$ so $\tau = \tau^{-1}$ and τ is a bijection.

Then τ is an isomorphism from $\mathbb{C}$ to $\mathbb{C}$ and is thus an automorphism. □

§14.1 #3 Determine the fixed field of complex conjugation on $\mathbb{C}$.

Solution: The fixed field of complex conjugation on $\mathbb{C}$ is the real line $\mathbb{R}$. For $x \in \mathbb{R}$, we have that $x = x + 0i \in \mathbb{C}$, so $\tau(x) = \tau(x+0i) = x - 0i = x$, so τ fixes $\mathbb{R}$. Moreover, for $a+bi \in \mathbb{C} \setminus \mathbb{R}$, we have that $b \neq 0$, and as $1, i$ form a basis for $\mathbb{C}$, $\tau(a+bi) = a - bi \neq a + bi$. Therefore, τ fixes only the real line $\mathbb{R}$.

§14.1 #5 Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly.

$\mathbb{Q}(\sqrt{2})[x]$

Solution: Notice that $\mathbb{Q}(\sqrt[4]{2})$ is the splitting field for the irreducible polynomial $x^2 - \sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$, so $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$. So the automorphism group has precisely two elements, the identity automorphism, and σ with defined by $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$.

§14.1 #6 Let k be a field.

(a) Show that the mapping $\varphi : k[t] \to k[t]$ defined by $\varphi(f(t)) = f(at + b)$ for fixed $a, b \in k$, $a \neq 0$ is an automorphism of $k[t]$ which is the identity on k.

Proof. First, note that as a subset of $k[t]$, k is the set of constant polynomials, so as changing the variable in a constant polynomial does not affect it, φ fixes k.
Next, notice that φ has a natural inverse $\varphi^{-1}(f(t)) = f\left(\frac{t-b}{a}\right)$, which is well-defined as $a \neq 0$, so f must be a bijection.
Choose $f, g \in k[t]$. Then

$$\varphi((f+g)(t)) = (f+g)(at+b) = f(at+b) + g(at+b) = \varphi(f(t)) + \varphi(g(t)).$$

Similarly,

Good.

$$\varphi((f \cdot g)(t)) = (f \cdot g)(at+b) = f(at+b)g(at+b) = \varphi(f(t))\varphi(g(t)).$$

Therefore, φ is a ring automorphism of $k[t]$. □

(b) Conversely, let φ be an automorphism of $k[t]$ which is the identity on k. Prove that there exist $a, b \in k$ with $a \neq 0$ such that $\varphi(f(t)) = f(at + b)$ as in (a).

✓ not quite. That exercise was about generators of a field. This is a (true) claim about generators of a ring.

Proof. As $t, 1$ generate $k[t]$, by exercise 14.1 #1 above, the action of φ on $k[t]$ is determined entirely by its action on t and 1. That is, $k[t] = (t, 1)$, the ideal generated by t and 1. By hypothesis, $\varphi(1) = 1$.

If the degree of $\varphi(t) = 0$, then $\varphi(k[t]) = k$, which is not an automorphism. Moreover, the degree of every element in $\varphi(k[t])$ is divisible by the degree of $\varphi(t)$, so if that degree is bigger than 1, then there are no linear polynomials in $\varphi(k[t])$. Thus, $\varphi(t)$ must be a linear polynomial, i.e., $\varphi(t) = at + b$ for $a, b \in k$, $a \neq 0$. □

$\sqrt{2}$ Make explicit using the Theorem of the Primitive Element that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Proof. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has 4 distinct $\mathbb{Q}$-embeddings into $\overline{\mathbb{Q}}$, which are:

$$\begin{aligned}
\sigma_1 &: \sqrt{2} \mapsto \sqrt{2}, && \sqrt{3} \mapsto \sqrt{3};\\
\sigma_2 &: \sqrt{2} \mapsto -\sqrt{2}, && \sqrt{3} \mapsto \sqrt{3};\\
\sigma_3 &: \sqrt{2} \mapsto \sqrt{2}, && \sqrt{3} \mapsto -\sqrt{3};\\
\sigma_4 &: \sqrt{2} \mapsto -\sqrt{2}, && \sqrt{3} \mapsto -\sqrt{3}.
\end{aligned}$$

By the Theorem of the Primitive Element, it is sufficient to show that $\{\sigma_i(\sqrt{2} + \sqrt{3}) \mid i = 1, \ldots, 4\}$ contains 4 distinct elements. So, observe that

$$\begin{aligned}
\sigma_1(\sqrt{2} + \sqrt{3}) &= \sqrt{2} + \sqrt{3}\\
\sigma_2(\sqrt{2} + \sqrt{3}) &= -\sqrt{2} + \sqrt{3}\\
\sigma_3(\sqrt{2} + \sqrt{3}) &= \sqrt{2} - \sqrt{3}\\
\sigma_4(\sqrt{2} + \sqrt{3}) &= -\sqrt{2} - \sqrt{3},
\end{aligned}$$

✓ Good

which are 4 distinct elements. Thus, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. □

Better wording: If the degree of $\varphi(t) > 1$, then $t \notin \mathrm{Im}(\varphi)$.