MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney

Homework Sheet 15
Model Solutions

Basic Questions

1. *Find a basis for the splitting field over $\mathbb{Q}$ of x^3-4.*

   The splitting field is $\mathbb{Q}\left(\sqrt[3]{4}, \frac{\sqrt{3}}{2}i\right)$. One basis for this field is $\{1, \sqrt[3]{4}, 2\sqrt[3]{2}, \frac{\sqrt{3}}{2}i, \frac{\sqrt{3}\sqrt[3]{4}}{2}i, \frac{\sqrt{3}\sqrt[3]{2}}{2}i\}$.

2. *(a) What is the order of $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$?*

   Any automorphism of $\mathbb{Q}(\sqrt[3]{2})$ fixing $\mathbb{Q}$, must send $\sqrt[3]{2}$ to a zero of x^3-2. The only zero of this polynomial in $\mathbb{Q}(\sqrt[3]{2})$ is $\sqrt[3]{2}$. Therefore, the isomorphism must fix the whole of $\mathbb{Q}(\sqrt[3]{2})$, so $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is the trivial group, and has order 1.

   (b) What is the order of $G(\mathbb{Q}(\sqrt[3]{2}, \frac{sqrt3}{2}i)/\mathbb{Q}(\sqrt{3}2i))$?

   We know that $[\mathbb{Q}(\sqrt[3]{2}, \frac{sqrt3}{2}i) : \mathbb{Q}(\sqrt{3}2i)] = 3$. Furthermore, the zeros of x^3-2 in $\mathbb{Q}(\sqrt[3]{2}, \frac{sqrt3}{2}i)$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$, where $\omega = \frac{-1+\sqrt{3}i}{2}$ is a complex cube root of unity. We therefore have automorphisms $\psi_{\sqrt[3]{2},\omega^n\sqrt[3]{2}}$ for $n=0,1,2$. This gives at least 3 automorphisms. The number of automorphisms can't be more than 3, so the order of $G(\mathbb{Q}(\sqrt[3]{2}, \frac{sqrt3}{2}i)/\mathbb{Q}(\sqrt{3}2i))$ is 3.

3. *Find an element α such that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbb{Q}(\alpha)$, and express $\sqrt{2}$ and $\sqrt[3]{3}$ as polynomials in this α over $\mathbb{Q}$.*

   One such element is $\alpha = \sqrt{2}+\sqrt[3]{3}$. We see that

$$\begin{aligned}
\alpha &= \sqrt{2}+\sqrt[3]{3}\alpha^2 && = 2+2\sqrt{2}\sqrt[3]{3}+\sqrt[3]{9}\\
\alpha^3 &= 2\sqrt{2}+6\sqrt[3]{3}+3\sqrt{2}\sqrt[3]{9}+3\\
\alpha^4 &= 4+8\sqrt{2}\sqrt[3]{3}+12\sqrt[3]{9}+12\sqrt{2}+3\sqrt[3]{3}\\
\alpha^5 &= 4\sqrt{2}+20\sqrt[3]{3}+20\sqrt{2}\sqrt[3]{9}+60+15\sqrt{2}\sqrt[3]{3}
\end{aligned}$$

   Now we solve these equations for $\sqrt{2}$ and $\sqrt[3]{3}$.

	1	$\sqrt{2}$	$\sqrt[3]{3}$	$\sqrt{2}\sqrt[3]{3}$	$\sqrt[3]{9}$	$\sqrt{2}\sqrt[3]{9}$
1	1	0	0	0	0	0
α	0	1	1	0	0	0
α^2	2	0	0	2	1	0
α^3	3	2	6	0	0	3
α^4	4	12	3	8	12	0
α^5	60	4	20	15	0	20

Solving these by row reduction gives:

$$\sqrt[3]{3} = \frac{1}{791}(1020 - 36\alpha + 540\alpha^2 + 320\alpha^3 - 45\alpha^4 - 48\alpha^5)$$

and therefore

$$\sqrt{2} = \frac{1}{791}(-1020 + 825\alpha - 540\alpha^2 - 320\alpha^3 + 45\alpha^4 + 48\alpha^5)$$

Theoretical Questions

4. *Show that if E is a finite extension of F, and E is a splitting field over F, then E is the splitting field of a single polynomial over F.*

   Pick a basis $\alpha_1, \dots, \alpha_n\}$ for E over F. Let $f_i = \mathrm{Irr}(\alpha_i, F)$. Now it is clear that E is the splitting field for $\{f_1, f_2, \dots, f_n\}$. (This set could have fewer than n elements, since some of the f_i might be repeated.) Now this means that E is the splitting field for the product $f_1 f_2 \cdots f_n$, which is a single polynomial over F.

5. *Show that if E is a splitting field over F, then for any element $\alpha \in E$, E contains all conjugates of α over F.*

   Let $\alpha \in E$, and let $\alpha' \in \overline{F}$ be a conjugate of α. Then we have the isomorphism $\psi_{\alpha,\alpha'}$ from E to a subfield of $\overline{F}$. This extends to an automorphism of $\overline{F}$ leaving F fixed. Since E is a splitting field, this induces an automorphism of E. This means that $\psi_{\alpha,\alpha'}(\alpha) = \alpha'$ is in E.

6. *Let E be a splitting field of an irreducible polynomial $f(x)$ over F. Let σ be an automorphism of E that leaves F fixed.*

   (a) Show that σ induces a permutation of the zeros of $f(x)$.

   We know that if α is a zero of $f(x)$ and $\sigma(\alpha) = \alpha'$, then $f(\alpha') = \sigma(f(\alpha)) = \sigma(0) = 0$, so α' must be a zero of f. Therefore, restricting σ to zeros of f gives a function from zeros of f to zeros of f. This function is one-to-one, since σ is, and since the set of zeros of f is finite, this function must also be onto, so it must be a permutation of the zeros of f.

   (b) Show that if σ' is another automorphism of E that leaves f fixed and induces the same permutation on the zeros of $f(x)$ as σ, then $\sigma' = \sigma$.

Consider the subset $S = \{x \in E | \sigma(x) = \sigma'(x)\}$. This set contains F and all the zeros of f. We now want to show that it is a subfield. Since E is the smallest field that contains F and all zeros of f, this will prove that $S = E$. It is clear that if $\sigma(x) = \sigma'(x)$ and $\sigma(y) = \sigma'(y)$, then we must have $\sigma(x+y) = \sigma(x) + \sigma(y) = \sigma'(x) + \sigma'(y) = \sigma'(x+y)$, and similarly $\sigma(xy) = \sigma(x)\sigma(y) = \sigma'(x)\sigma'(y) = \sigma'(xy)$. We need to check that if $x \neq 0$, then $\sigma(x^{-1}) = \sigma'(x^{-1})$. However, we know that $\sigma(x^{-1}) = \sigma(x)^{-1} = \sigma'(x)^{-1} = \sigma'(x^{-1})$.

7. *Show that if E is an algebraic extension of a perfect field F, then E is perfect.*

   Suppose E is not perfect, and that E' is a finite extension of E which is not separable over E. There must be some $\alpha \in E'$ which is not separable over E. Now let $f = \mathrm{Irr}(\alpha, F)$ (this exists because E is algebraic over f, and α is algebraic over E), and let $g = \mathrm{Irr}(\alpha, E)$. Now clearly f is also a polynomial in $E[x]$, and α is a zero of f, so f is divisible by g in $E[x]$. However, in $E'[x]$, g is divisible by $(x-\alpha)^2$, so f must also be divisible by $(x-\alpha)^2$, so α is not separable over F. This means that $F(\alpha)$ is a finite, but not separable extension of F. This contradicts our assumption that F is perfect.

8. *Let K be a field extension of F, and let L be a field extension of K. Let $\alpha \in L$ be algebraic over F. Show that $[K(\alpha) : K] \leqslant [F(\alpha) : F]$.*

   We know that $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is a basis for $K(\alpha)$ over K, for some n. Now if $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ are not independent elements over F, then α is a zero of some polynomial f of degree at most n over F. Now f is also a polynomial over K, and α is still a zero of f over K, so $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ are not linearly independent over K, contradicting our assumption that they are a basis for $K(\alpha)$ over K.

Bonus Questions

9. *For an infinite algebraic field extension, we will say that the extension is separable if every element of the larger field is separable over the smaller field. Show that if E is a separable extension of F and K is a separable extension of E, then K is a separable extension of F.*

   Let $\alpha \in K$. We need to show that α is separable over F. However, we know that α is separable over E, and E is separable over F. We will show that $F(\alpha)$ is separable over F. Let $f = \mathrm{Irr}(\alpha, F)$ and $g = \mathrm{Irr}(\alpha, E)$. Since f is a polynomial in $E[x]$, and α is a zero of f, we must have that g divides f, so $f = gh$ for some $h \in E[x]$. Since $(x-\alpha)^2$ divides f in $K[x]$, but does not divide g, we must have that $(x-\alpha)$ divides h. Since g is the smallest polynomial that has α as a zero, we must have that g divides h, so $h = gk$, and $f = g^2k$. Now consider the splitting field L for f over F, and consider $L \cap E$. Clearly, $g \in L[x]$, so we must have $g \in (L \cap E)[x]$. Since E is a separable extension of F, we must have that $(L \cap E)$ is a separable extension of F. Furthermore, since every element of L is separable over E, and L is a splitting field over $(L \cap E)$, for any $\beta \in L$, we must have $\mathrm{Irr}(\beta, E) \in L[x]$, since this polynomial is a product of the linear factors $(x - \beta_i)$, all of which are in $L[x]$. Therefore, $g \in (L \cap E)[x]$, and since g has no repeated zeros, we have shown that L is separable over $L \cap E$. Therefore, L is separable over F, so α is separable over F.