MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney
Homework Sheet 14
Model Solutions

Basic Questions

1. *Which of the following pairs of numbers are conjugate over $\mathbb{Q}$?*

   (a) $\sqrt{2}$ and $\sqrt{6}$.

   These are not conjugate, since $\mathrm{Irr}(\sqrt{2}.\mathbb{Q}) = x^2 - 2$, while $\mathrm{Irr}(\sqrt{6}.\mathbb{Q}) = x^2 - 6$.

   (b) $1+\sqrt{2}$ and $1-\sqrt{2}$.

   These are conjugate, since $\mathrm{Irr}(1+\sqrt{2}.\mathbb{Q}) = x^2 - 2x - 1 = \mathrm{Irr}(1-\sqrt{2}.\mathbb{Q})$.

   (c) $\sqrt[4]{2}$ and $\sqrt{2}$.

   These are not conjugate, since $\mathrm{Irr}(\sqrt{2}.\mathbb{Q}) = x^2 - 2$, while $\mathrm{Irr}(\sqrt[4]{2}.\mathbb{Q}) = x^4 - 2$.

2. *In $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, compute $\psi_{\sqrt{2}+\sqrt{3},\sqrt{2}-\sqrt{3}}(2+\sqrt{2}-\sqrt{6})$.*

   We have that $(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}$, so that $\frac{1}{2}(\sqrt{2}+\sqrt{3})^3 - \frac{9}{2}(\sqrt{2}+\sqrt{3} = \sqrt{2}$, so that $\psi_{\sqrt{2}+\sqrt{3},\sqrt{2}-\sqrt{3}}(\sqrt{2}) = \frac{1}{2}(\sqrt{2}-\sqrt{3})^3 - \frac{9}{2}(\sqrt{2}-\sqrt{3} = \sqrt{2}$. This means that $\psi_{\sqrt{2}+\sqrt{3},\sqrt{2}-\sqrt{3}}(\sqrt{3}) = \psi_{\sqrt{2}+\sqrt{3},\sqrt{2}-\sqrt{3}}(\sqrt{2}+\sqrt{3}) - \psi_{\sqrt{2}+\sqrt{3},\sqrt{2}-\sqrt{3}}(\sqrt{2}) = -\sqrt{3}$. This gives $\psi_{\sqrt{2}+\sqrt{3},\sqrt{2}-\sqrt{3}}(2+\sqrt{2}-\sqrt{6}) = 2+\sqrt{2}-(\sqrt{2}\times -\sqrt{3}) = 2+\sqrt{2}+\sqrt{6}$.

3. *In $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, compute the fixed field of $\{\psi_{\sqrt{2}+\sqrt{3},-\sqrt{2}-\sqrt{3}}\}$.*

   We know that $\psi_{\sqrt{2}+\sqrt{3},-\sqrt{2}-\sqrt{3}}(\sqrt{2}) = -\sqrt{2}$ and $\psi_{\sqrt{2}+\sqrt{3},-\sqrt{2}-\sqrt{3}}(\sqrt{3}) = -\sqrt{3}$, and $\psi_{\sqrt{2}+\sqrt{3},-\sqrt{2}-\sqrt{3}}(\sqrt{6}) = \sqrt{6}$, and we know that $\mathbb{Q}(\sqrt{6})$ is fixed, but $\sqrt{3}$ is not. Since there are no extensions between $\mathbb{Q}(\sqrt{6})$ and $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, the fixed field must be $\mathbb{Q}(\sqrt{6})$.

4. *Let α be a zero of x^3+x^2+x+3 in GF(125).*

   (a) Compute the Frobenius automorphism $\sigma_5(\alpha)$. [Express $\sigma_5(\alpha)$ in the basis $\{1,\alpha,\alpha^2\}$.]

   Since α is a zero of x^3+x^2+x+3, we have that $\alpha^3 = -\alpha^2-\alpha-3 = 4\alpha^2+4\alpha+2$. We know that $\sigma_5(\alpha) = \alpha^5 = \alpha^2(4\alpha^2+4\alpha+2) = 4\alpha^4 + 4\alpha^3+2\alpha^2 = 4\alpha(4\alpha^2+4\alpha+2)+4\alpha^3+2\alpha^2 = 3\alpha^2+3\alpha$.

   (b) Describe the fixed field of $\{\sigma_5\}$ in terms of this basis.

   From part (a), we deduce $\sigma_5(\alpha^2) = (3\alpha^2+3\alpha)^2 = 4\alpha^4+3\alpha^3+4\alpha^2 = 4(4\alpha^3+4\alpha^2+2\alpha)+3\alpha^3+4\alpha^2 = 4\alpha^3+3\alpha = 4(4\alpha^2+4\alpha+2)+3\alpha = \alpha^2+4\alpha+3$.

From this it is easy to see that no non-trivial linear combination of α and α^2 is fixed, so the fixed field is just $\mathbb{Z}_5$.

5. *Let $\omega = \frac{-1+\sqrt{3}i}{2}$ (so that $\omega^3 = 1$.) Consider the isomorphism $\psi_{\sqrt[3]{2},\omega\sqrt[3]{2}}$ from $\mathbb{Q}\left(\sqrt[3]{2}\right)$ to $\mathbb{Q}\left(\sqrt[3]{2}\omega\right)$. Compute all ways to extend this isomorphism to an isomorphism mapping $\mathbb{Q}(\sqrt[3]{2},\omega\sqrt[3]{2})$ to a subfield of $\overline{Q}$.*

   We have that $\mathrm{Irr}(\sqrt[3]{2},\mathbb{Q}) = x^3 - 2$. The zeros of this polynomial are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$. Any isomorphism from $\mathbb{Q}(\sqrt[3]{2},\omega\sqrt[3]{2})$ to a subfield of $\overline{Q}$ must send zeros of this polynomial to zeros of this polynomial. An extension σ of $\psi_{\sqrt[3]{2},\omega\sqrt[3]{2}}$ is entirely determined by its value on $\omega\sqrt[3]{2}$ (or equivalently by its value on ω). This must be either $\sqrt[3]{2}$ or $\omega^2\sqrt[3]{2}$ (corresponding to $\sigma(\omega) = \omega^2$ and $\sigma(\omega) = \omega$ respectively). It is straightforward to check that these both lead to automorphisms of $\mathbb{Q}(\sqrt[3]{2},\omega\sqrt[3]{2})$.

Theoretical Questions

6. *Let $F(\alpha_1,\ldots,\alpha_n)$ be an extension field of F. Show that any automorphism σ of $F(\alpha_1,\ldots,\alpha_n)$ leaving F fixed is completely determined by the values $\sigma(\alpha_i)$.*

   Let σ_1 and σ_2 be two automorphisms that leave F fixed, such that for each i, $\sigma_1(\alpha_i) = \sigma_2(\alpha_i)$. We need to show that $\sigma_1 = \sigma_2$. Let $S = \{x \in F(\alpha_1,\ldots,\alpha_n) | \sigma_1(x) = \sigma_2(x)\}$. We need to show that $S = F(\alpha_1,\ldots,\alpha_n)$. We know that S contains $F, \alpha_1,\ldots,\alpha_n$, so we just need to show that S is a subfield. Since σ_1 and σ_2 are homomorphisms, S must be closed under addition and multiplication. Furthermore, since $-1 \in F \subseteq S$, S is closed under additive inverse. We need to show that S is closed under multiplicative inverses. Let $\sigma_1(x) = \sigma_2(x)$. We need to show that $\sigma_1(x^{-1}) = \sigma_2(x^{-1})$. However, we know that $\sigma_1(x)\sigma_1(x^{-1}) = \sigma_1(1) = 1 = \sigma_2(1) = \sigma_2(x)\sigma_2(x^{-1}) = \sigma_1(x)\sigma_1(x^{-1})$. Therefore, multiplying by $(\sigma_1(x))^{-1}$ (which exists because σ_1 is an isomorphism, so its kernel is trivial, so $\sigma_1(x) \neq 0$) we get that $\sigma_1(x^{-1}) = \sigma_2(x^{-1})$. Therefore S is a subfield of $F(\alpha_1,\ldots,\alpha_n)$ containing F and $\{\alpha_1,\ldots,\alpha_n\}$, so it must be the whole of $F(\alpha_1,\ldots,\alpha_n)$.

7. *Let E be an extension field of F. Let S be a set of automorphisms of E fixing F. Let H be the subgroup of $G(E/F)$ generated by S. Show that $E_S = E_H$.*

   Clearly $S \subseteq H$, so $E_H \subseteq E_S$. We need to show the converse inclusion that if $x \in E_S$, then $x \in E_H$. Let $G_x = \{\sigma \in G(E/F) | \sigma(x) = x\}$. We know that $S \subseteq G_x$ for any $x \in E_S$, so we just need to show that G_x is a subgroup of $G(E/F)$. It is clear that the identity automorphism fixes x, since it fixes every element of E. Suppose $\sigma(x) = x$ and $\tau(x) = x$. Clearly $\sigma^{-1}(x) = x$, and $(\sigma\tau)(x) = \sigma(\tau(x)) = \sigma(x) = x$, so we have that G_x is a subgroup of $G(E/F)$. Since H is the subgroup generated by S, we have that $H \subseteq G_x$ for all $x \in E_s$. This is equivalent to saying $x \in E_H$, so we have $E_S \subseteq E_H$ as required.

8. *(a) Show that if F is an algebraically closed field, then any isomorphism σ of F to a subfield of F such that F is algebraic over $\sigma(F)$, is an automorphism of F. [Hint, since $\sigma(F)$ is isomorphic to F, it must be algebraically closed.]*

   Since $\sigma(F)$ is isomorphic to F, it must be algebraically closed. [We can extend σ to an isomorphism $\sigma[x] : F[x] \longrightarrow (\sigma(F))[x]$, and it is straightforward to see that for any $f \in F[x]$, any $\alpha \in F$ is a zero of f if and only if $\sigma(\alpha)$ is a zero of $\sigma[x](f)$.] We have that F is algebraic over the algebraically closed field $\sigma(F)$. This means that for any $\alpha \in F$, we have $\mathrm{Irr}(\alpha, \sigma(F)) \in \sigma(F)[x]$. However, we know that all zeros of $\mathrm{Irr}(\alpha, \sigma(F))$ are in $\sigma(F)$ (since $\sigma(F)$ is algebraically closed), so we must have $\alpha \in \sigma(F)$. Thus we have $F \subseteq \sigma(F)$, so σ is an automorphism of F.

   (b) Let E be an algebraic extension of F. Show that any isomorphism of E onto a subfield of $\overline{F}$ that fixes F can be extended to an automorphism of $\overline{F}$.

   We know that any isomorphism of E onto a subfield of $\overline{F}$ that fixes F extends to an isomorphism τ from $\overline{F}$ to a subfield of $\overline{F}$. However, τ fixes F, so $F \subseteq \tau(\overline{F})$. Since $\overline{F}$ is algebraic over F, it is algebraic over $\tau(\overline{F})$. Therefore, by part (a), τ is an automorphism of $\overline{F}$.

9. *Let E be an algebraic extension of F. Show that there is an isomorphism of $\overline{F}$ to $\overline{E}$ fixing all elements of F.*

   The inclusion from F to E is an isomorphism from F to a subfield of E. By the extension theorem, we can extend it to an isomorphism σ from $\overline{F}$ to a subfield of $\overline{E}$. The image $\sigma(\overline{F})$ is algebraically closed, and contains F, over which $\overline{E}$ is algebraic. Therefore, $\overline{E}$ is algebraic over the algebraically closed field $\sigma(\overline{F})$. Therefore, $\sigma(\overline{F}) = \overline{E}$, so σ is an isomorphism from $\overline{F}$ to $\overline{E}$.

10. *Let E be a finite extension of F. Show that $\{E : F\} \leqslant [E : F]$. [You may assume the result for simple extensions.]*

    We know that any finite extension can be expressed as a tower of simple extensions:

$$\begin{tikzcd}
E = F(\alpha_1, \dots, \alpha_n) \arrow[d, dash] \\
F(\alpha_1, \dots, \alpha_{n-1}) \arrow[d, dotted, dash] \\
F(\alpha_1) \arrow[d, dash] \\
F
\end{tikzcd}$$

This gives

$$\begin{aligned}
\{E : F\} &= \{E : F(\alpha_1, \dots, \alpha_{n-1})\}\{F(\alpha_1, \dots, \alpha_{n-1}), F(\alpha_1, \dots, \alpha_{n-2})\} \cdots \{F(\alpha_1) : F\} \\
&\leqslant [E : F(\alpha_1, \dots, \alpha_{n-1})][F(\alpha_1, \dots, \alpha_{n-1}), F(\alpha_1, \dots, \alpha_{n-2})] \cdots [F(\alpha_1) : F] \\
&= [E : F]
\end{aligned}$$

Bonus Questions

11. *Show that if α and β are both transcendental over F, then there is an isomorphism of $F(\alpha)$ and $F(\beta)$ sending α to β.*

    We define the isomorphism in the obvious way — elements of $F(\alpha)$ are of the form $\frac{f(\alpha)}{g(\alpha)}$ for $f, g \in F[x]$, with no common divisor, such that g is monic (coefficient of the largest power of x is 1). We define $\sigma : F(\alpha) \xrightarrow{F} (\beta)$ by $\sigma\left(\frac{f(\alpha)}{g(\alpha)}\right) = \frac{f(\beta)}{g(\beta)}$. We need to show that this is an isomorphism. It is straightforward to see that it is a homomorphism (assuming it is well-defined), so we just need to show that it is well-defined, that its kernel is zero, and that it is onto. To show that it is well-defined, we need to show that we can't represent the same element of $F(\alpha)$ in more than one way subject to the condition that g is monic, and f and g have no non-trivial common divisor. Suppose we have $\frac{f(\alpha)}{g(\alpha)} = \frac{h(\alpha)}{k(\alpha)}$. Multiplying through gives $f(\alpha)k(\alpha) - g(\alpha)h(\alpha) = 0$. Since α is transcendental over F, this means that $fk - gh$ is the zero polynomial, i.e. $fk = gh$. Now since f and g have no common factor, this means we must have that g is a divisor of k, and similarly, h is a divisor of f. Furthermore, since g and k are both monic, this must give $g = k$ and $f = h$. We also need to show that $\frac{f(\beta)}{g(\beta)}$ is an expression of the required form in $F(\beta)$, i.e. that f and g have no non-trivial common factor, and g is monic, but this is true. Next we need to check that σ is onto: given $\gamma = \frac{f(\beta)}{g(\beta)} \in F(\beta)$, we see that $\gamma = \sigma\left(\frac{f(\alpha)}{g(\alpha)}\right)$ is in the image of σ, so σ is onto. Finally, if $\frac{f(\alpha)}{g(\alpha)}$ is in the kernel of σ, then we have $\frac{f(\beta)}{g(\beta)} = 0$, and therefore, $f(\beta) = 0$. Since β is transcendental over F, this means that f is the zero polynomial, so that $\frac{f(\alpha)}{g(\alpha)} = 0$. Therefore, σ is an isomorphism between $F(\alpha)$ and $F(\beta)$.

12. *Show that the only automorphism of $\mathbb{R}$ is the identity. [Hint: show that any automorphism preserves positive numbers (since these are the squares of real numbers) and therefore preserves the order on real numbers.]*

Let σ be an automorphism of $\mathbb{R}$. Any non-negative real number x satisfies $x = y^2$ for some $y \in \mathbb{R}$, so we must have $\sigma(x) = \sigma(y)^2$. Therefore, $\sigma(x)$ is also non-negative. Now for any $x \leqslant y \in \mathbb{R}$, we have $y - x$ is non-negative, so $\sigma(y) - \sigma(x)$ is also non-negative. Therefore, $\sigma(x) \leqslant \sigma(y)$. We also know that σ must preserve the prime field $\mathbb{Q}$. Now for any $x \in \mathbb{R}$, we consider $L = \{q \in \mathbb{Q} | q \leqslant x\}$ and $U = \{q \in \mathbb{Q} | x \leqslant q\}$. We know that σ fixes all elements of L and U. However, we also know that $\sigma(x) \leqslant \sigma(u) = u$ for all $u \in U$ and $l = \sigma(l) \leqslant \sigma(x)$ for all $l \in L$. The only possible value of $\sigma(x)$ satisfying these constraints is x, so σ is the identity automorphism.