Instructor: Leo Goldmakher

Williams College
Department of Mathematics and Statistics

MATH 394 : GALOIS THEORY

Solution Set 6

SOME COMMON MISCONCEPTIONS.

1. If $L = K(\alpha)$ then $\{1, \alpha\}$ is not necessarily a basis of L! However, $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ where $n := \deg m_\alpha$ is a basis.
2. Given $K/\mathbb{Q}$ and some α of degree 3 over $\mathbb{Q}$, it is **not necessarily true** that $[K(\alpha) : K] = 1$ or 3. For example, if $\alpha = \omega\sqrt[3]{2}$ and $K = \mathbb{Q}(\sqrt[3]{2})$ then $[K(\alpha) : K] = 2$.
3. Given some algebraic extension $K/\mathbb{Q}$, there's no canonical minimal polynomial one can associate to generators of K. For example, $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$, but the two minimal polynomials of these elements are completely different: $x^2 + x + 1$ and $x^2 + 3$. The only trait they share (which isn't a coincidence) is their degree.

6.1 Prove that if $2^k + 1$ is prime, then $k = 2^m$. [This came up in our discussion of Fermat primes.]

Given 2^k+1 a prime number, write $k = 2^m\ell$ with ℓ an odd number. Observe that $x+1 \mid x^\ell+1$ (since -1 is root of both), so $2^{2^m} + 1 \mid 2^k + 1$. Since $2^k + 1$ is prime, $2^{2^m} + 1 = 2^k + 1$, whence $k = 2^m$.

6.2 Let $S := \{\sqrt{p} : p \text{ is prime}\}$. Prove that $\mathbb{Q}(S)/\mathbb{Q}$ is algebraic but infinite.

First, observe that any element $\alpha \in \mathbb{Q}(S)$ must live in $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$ for some finite list of primes $p_1, p_2, \ldots, p_n$. Clearly $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})/\mathbb{Q}$ is a finite extension (see below for a precise statement), hence must be algebraic. It follows that α is algebraic over $\mathbb{Q}$.

Next, we prove that $\mathbb{Q}(S)/\mathbb{Q}$ is infinite. It suffices to prove

Claim. *$[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$ for any set of distinct primes $p_1, p_2, \ldots, p_n$.*

Proof. We prove, by induction, that $\sqrt{p} \notin \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$ for any prime $p \notin \{p_1, p_2, \ldots, p_n\}$. The claim instantly follows by Tower Law.

The base case $n = 0$ is simply the assertion that $\sqrt{p}$ is irrational. Now set

$$K := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{n-1}}),$$

and suppose that $\sqrt{p} \in K(\sqrt{p_n})$; in particular,

$$\sqrt{p} = a + b\sqrt{p_n}$$

for some $a, b \in K$. Squaring both sides implies $\sqrt{p_n} \in K$, contradicting our inductive hypothesis that $\sqrt{p_n} \notin K$. □

6.3 Prove that $\mathbb{Q}(\omega\sqrt[3]{2}) \simeq \mathbb{Q}(\omega^2\sqrt[3]{2})$, but $\mathbb{Q}(\omega\sqrt[3]{2}) \neq \mathbb{Q}(\omega^2\sqrt[3]{2})$.

Recall that for any α which is algebraic over K we have

$$K(\alpha) = K[\alpha] \simeq K[t]/(m_\alpha)$$

where m_α denotes the minimal polynomial of α over K.

Observe that all three numbers $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ have the same minimal polynomial over $\mathbb{Q}$: $x^3 - 2$. We deduce that

$$\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}(\omega\sqrt[3]{2}) \simeq \mathbb{Q}(\omega^2\sqrt[3]{2}) \simeq \mathbb{Q}[t]/(t^3-2),$$

which implies the first part of the question.

Next we prove that $\mathbb{Q}(\omega\sqrt[3]{2}) \neq \mathbb{Q}(\omega^2\sqrt[3]{2})$. It suffices to prove
Claim. $\omega\sqrt[3]{2} \notin \mathbb{Q}(\omega^2\sqrt[3]{2})$
Proof. Suppose $\omega\sqrt[3]{2} \in \mathbb{Q}(\omega^2\sqrt[3]{2})$. Then

$$\omega = \frac{\omega^2\sqrt[3]{2}}{\omega\sqrt[3]{2}} \in \mathbb{Q}(\omega^2\sqrt[3]{2}) \qquad \Longrightarrow \qquad \sqrt[3]{2} = \frac{\omega^2\sqrt[3]{2}}{\omega^2} \in \mathbb{Q}(\omega^2\sqrt[3]{2}).$$

This implies that $\mathbb{Q}(\omega, \sqrt[3]{2}) \subseteq \mathbb{Q}(\omega^2\sqrt[3]{2})$. But this opposite inclusion is immediate, whence $\mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(\omega^2\sqrt[3]{2})$. But this can't be the case, since (as we showed in class) the field on the left hand side has degree 6 over $\mathbb{Q}$, while the field on the right hand side has degree 3.

6.4 In class we found four fields lying between $\mathbb{Q}$ and $\mathbb{Q}(\omega, \sqrt[3]{2})$. Prove that there are no others.

First we prove a quick
Lemma. Given $F/\mathbb{Q}$ and $\alpha \in \mathbb{C}$ such that $[F:\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}]$. Then $\alpha \in F$ iff $F = \mathbb{Q}(\alpha)$.
Proof. Suppose $\alpha \in F$. Then $\mathbb{Q}(\alpha) \subseteq F$, whence by Tower Law we have

$$[F:\mathbb{Q}] = [F:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}].$$

Our hypothesis implies $[F:\mathbb{Q}(\alpha)] = 1$, whence $F = \mathbb{Q}(\alpha)$. The reverse direction is trivial. $\square$

Continued on next page...

Pick any field F such that $\mathbb{Q} \subsetneq F \subsetneq \mathbb{Q}(\omega, \sqrt[3]{2})$. Since $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$, Tower Law implies that $[F : \mathbb{Q}] = 2$ or 3. We consider two cases:

- F contains some cube root of 2, say, α.

  Then $F \supseteq \mathbb{Q}(\alpha)$, whence $[F : \mathbb{Q}] \geq 3$; we deduce $[F : \mathbb{Q}] = 3$. By our lemma, we conclude that $F = \mathbb{Q}(\alpha)$.

- F doesn't contain any cube root of 2.

  In this case $x^3 - 2$ is irreducible over F, whence $[F(\alpha) : F] = 3$ for any α a cube root of 2. But $F(\alpha) \subseteq \mathbb{Q}(\omega, \sqrt[3]{2})$, so Tower Law implies $[F : \mathbb{Q}] = 2$. We claim that $\omega \in F$. Otherwise, we'd have $[F(\omega) : F] = 2$; this would mean that $[F(\omega) : \mathbb{Q}] = 4$, which would contradict the Tower Law since $F(\omega) \subseteq \mathbb{Q}(\omega, \sqrt[3]{2})$. Thus $\omega \in F$. Our lemma immediately gives $F = \mathbb{Q}(\omega)$.

Putting these two cases together, we conclude that any intermediate field must either be of the form $\mathbb{Q}(\alpha)$ for some α a cube root of 2, or of the form $\mathbb{Q}(\omega)$.

6.5 We imitate the construction of the Galois correspondence from class, but this time with the polynomial $f(x) := x^4 - 4x^2 + 2$. Let $\alpha := \sqrt{2 + \sqrt{2}}$ denote one of the roots of f.

(a) Prove that $\mathbb{Q}(\alpha)$ is a splitting field of f.

We need to check two things: that all the roots of f lie in $\mathbb{Q}(\alpha)$, and that $\mathbb{Q}(\alpha)$ is the smallest field with this property. The latter claim is clear, since any field in which f splits must contain α. We thus focus on proving the former claim.

Observe that the roots of f are $\pm\sqrt{2 \pm \sqrt{2}}$, so it suffices to prove $\sqrt{2 - \sqrt{2}} \in \mathbb{Q}(\alpha)$. Since $\alpha\sqrt{2 - \sqrt{2}} = \sqrt{2}$, we deduce

$$\sqrt{2 - \sqrt{2}} = \frac{\sqrt{2}}{\alpha} = \frac{\alpha^2 - 2}{\alpha} \in \mathbb{Q}(\alpha).$$

(b) Draw a lattice of all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$, along with the degrees of each extension.

$$\begin{tikzcd} \mathbb{Q}(\alpha) \arrow[d, dash, "2"] \\ \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] \\ \mathbb{Q} \end{tikzcd}$$

Note that f is Eisenstein at 2, so it's irreducible over $\mathbb{Q}$. This implies $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Next, since $\sqrt{2} \in \mathbb{Q}(\alpha)$ but has degree 2 over $\mathbb{Q}$, we have an intermediate field $\mathbb{Q}(\sqrt{2})$.

Claim. There are no other intermediate fields.
Proof. See next page...

Proof. Given an intermediate field $\mathbb{Q} \subsetneq F \subsetneq \mathbb{Q}(\alpha)$. By Tower Law, $[F : \mathbb{Q}] = 2$. If $\sqrt{2} \in F$, then the lemma from problem **6.4** implies $F = \mathbb{Q}(\sqrt{2})$, and we're done. I claim that F must contain $\sqrt{2}$. Indeed, suppose (for the remainder of the proof) that $\sqrt{2} \notin F$. Below we'll construct an element $x \in F$ of degree 4 over $\mathbb{Q}$. Since the degree of any element cannot exceed the degree of its ambient extension, we deduce that $[F : \mathbb{Q}] \geq 4$. But this contradicts our assumption that F is an intermediate extension.

Since $\sqrt{2} \notin F$, we have $[F(\sqrt{2}) : F] = 2$, so Tower Law implies $F(\sqrt{2})$ has degree 4 over $\mathbb{Q}$. On the other hand, $F(\sqrt{2}) \subseteq \mathbb{Q}(\alpha)$, which also has degree 4 over $\mathbb{Q}$, whence $F(\sqrt{2}) = \mathbb{Q}(\alpha)$. In particular, $\alpha \in F(\sqrt{2})$, so

$$\sqrt{2+\sqrt{2}} = x + y\sqrt{2}$$

for some $x, y \in F$. Squaring both sides and simplifying yields

$$(1 - 2xy)\sqrt{2} = x^2 + 2y^2 - 2.$$

Since $x, y \in F$ but $\sqrt{2} \notin F$, the only way this relation could hold is if

$$2xy = 1 \qquad \text{and} \qquad x^2 + 2y^2 = 2.$$

Substitution shows that $2x^4 - 4x^2 + 1 = 0$ which is irreducible over $\mathbb{Q}$ (this can be seen by reduction over $\mathbb{F}_3$, for example). Thus, x has degree 4 over $\mathbb{Q}$. But $x \in F$, which implies F itself must have degree at least 4 over $\mathbb{Q}$. Contradiction! $\square$

(c) Determine $\operatorname{Aut}(\mathbb{Q}(\alpha))$. What familiar group is it isomorphic to?

I claim the automorphism group is the cyclic group of order 4. To see this, first observe that any automorphism $\sigma \in \operatorname{Aut}(\mathbb{Q}(\alpha))$ fixes all rationals, hence is determined by where it sends α. Note that $(\alpha^2 - 2)^2 = 2$; applying σ to both sides and using properties of automorphisms we find

$$\sigma(\alpha) \in \left\{ \pm\sqrt{2 \pm \sqrt{2}} \right\}.$$

Thus we immediately see that the group $\operatorname{Aut}(\mathbb{Q}(\alpha))$ has order 4. But is it the cyclic group or the Klein V group?

Consider the automorphism $\tau \in \operatorname{Aut}(\mathbb{Q}(\alpha))$ defined by

$$\tau(\alpha) := \sqrt{2 - \sqrt{2}}.$$

Algebraic manipulation implies that $\tau(\sqrt{2}) = -\sqrt{2}$, from which we deduce

$$\tau^2(\alpha) = \tau\left(\sqrt{2-\sqrt{2}}\right) = \tau\left(\frac{\sqrt{2}}{\alpha}\right) = \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} = -\alpha.$$

We immediately derive

$$\tau^3(\alpha) = \tau(-\alpha) = -\sqrt{2-\sqrt{2}} \qquad \text{and} \qquad \tau^4(\alpha) = \tau^2(-\alpha) = \alpha.$$

Thus all of $\tau, \tau^2, \tau^3, \tau^4$ are distinct automorphisms. We conclude that
$$\operatorname{Aut}(\mathbb{Q}(\alpha)) = \{e, \tau, \tau^2, \tau^3\}.$$

(d) Draw a lattice of all subgroups of $\mathrm{Aut}\big(\mathbb{Q}(\alpha)\big)$, labelling all the connecting edges by the index of one group inside the other.

$$\begin{tikzcd}
\{e, \tau, \tau^2, \tau^3\} \arrow[d, dash, "2"] \\
\{e, \tau^2\} \arrow[d, dash, "2"] \\
\{e\}
\end{tikzcd}$$

6.6 Another Galois correspondence, this time for the polynomial $g(x) := x^4 - 12x^2 + 35$.

(a) Determine a splitting field K of g. (Write it in the form $\mathbb{Q}(\beta_1, \beta_2)$.)

It's $\mathbb{Q}(\sqrt{5}, \sqrt{7})$.

(b) Draw a lattice of all intermediate fields between $\mathbb{Q}$ and K, along with the degrees of each extension.

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{5}, \sqrt{7}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{5}) \arrow[dr, dash, "2"] & \mathbb{Q}(\sqrt{35}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{7}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

As above, verifying that all the fields appearing here are distinct isn't terribly difficult. Most of the work goes into proving this is a complete list. But similar games to the ones in the previous problem work here as well.

(c) Determine $\mathrm{Aut}(K)$. What familiar group is it isomorphic to?

Any automorphism is determined by where it sends $\sqrt{5}$ and $\sqrt{7}$, from which we quickly deduce that the order of the automorphism group is 4. Is it the cyclic group of the Klein group? I claim the latter.

Consider the automorphisms defined by

$$\sigma(\sqrt{5}) = -\sqrt{5} \qquad \tau(\sqrt{5}) = \sqrt{5}$$
$$\sigma(\sqrt{7}) = \sqrt{7} \qquad \tau(\sqrt{7}) = -\sqrt{7}.$$

It's straightforward to verify that $\sigma^2 = \tau^2 = e$ and that σ, τ, and $\sigma\tau$ are all distinct nontrivial automorphisms. Thus the automorphism group must be the Klein V group $\{e, \sigma, \tau, \sigma\tau\}$.

(d) Draw a lattice of all subgroups of $\mathrm{Aut}(K)$, labelling all the connecting edges by the index of one group inside the other.

$$\begin{tikzcd}
& \{e,\sigma,\tau,\sigma\tau\} \arrow[dl, no head, "2"'] \arrow[d, no head, "2"] \arrow[dr, no head, "2"] & \\
\{e,\sigma\} \arrow[dr, no head, "2"] & \{e,\sigma\tau\} \arrow[d, no head, "2"] & \{e,\tau\} \arrow[dl, no head, "2"] \\
& \{e\} &
\end{tikzcd}$$