Instructor: Leo Goldmakher

Williams College
Department of Mathematics and Statistics

MATH 394 : GALOIS THEORY

Solution Set 2

2.1 In class, we saw that given one root of a cubic polynomial, we can use the quadratic formula to express the other two roots. The goal of this exercise is to generalize this principle.

(a) Carry out the above for a general (monic) cubic. In other words, given $f(x) = x^3 + a_2x^2 + a_1x + a_0$, and β such that $f(\beta) = 0$, determine the other two roots of $f(x)$ in terms of β (and the a_i's).

Consider the monic cubic polynomial $f(x) = x^3 + a_2x^2 + a_1x + a_0$. Let β be a given root of f, and let α and γ be the other two roots of f. Then we can write

$$f(x) = (x-\alpha)(x-\beta)(x-\gamma) = x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\alpha\gamma+\beta\gamma)x - \alpha\beta\gamma.$$

Matching coefficients with the a_i yields $\alpha+\beta+\gamma = -a_2$ and $\alpha\beta\gamma = -a_0$.

We consider two cases. If $\beta = 0$, then $a_0 = 0$ whence $f(x) = x(x^2 + a_2x + a_1)$. On the other hand,

$$f(x) = (x-\alpha)(x-\beta)(x-\gamma) = x(x-\alpha)(x-\gamma),$$

so α, γ must be the roots of the quadratic polynomial $x^2 + a_2x + a_1$. It follows that

$$\alpha, \gamma = \frac{-a_2 \pm \sqrt{a_2^2 - 4a_1}}{2}.$$

If $\beta \neq 0$ then $\alpha + \gamma = -(\beta + a_2)$ and $\alpha\gamma = -\frac{a_0}{\beta}$ imply that

$$(x-\alpha)(x-\gamma) = x^2 - (\alpha+\gamma) + \alpha\gamma = x^2 + (\beta+a_2)x - \frac{a_0}{\beta}.$$

Thus in this case,

$$\alpha, \gamma = \frac{-(\beta+a_2) \pm \sqrt{(\beta+a_2)^2 + \frac{4a_0}{\beta}}}{2}.$$

(b) Now suppose you're given the polynomial $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, and you happen to know that $f(\beta) = 0$. Write down a cubic polynomial whose roots are precisely the other three roots of $f(x)$.

It will follow from our work in part (c) that

$$x^3 + (a_3 + \beta)x^2 + (a_2 + \beta a_3 + \beta^2)x + (a_1 + \beta a_2 + \beta^2 a_3 + \beta^3)$$

is a cubic polynomial whose three roots are precisely the other three roots of f.

(c) Generalize part (b) to arbitrary monic polynomials f of degree n. [*You should get a polynomial of the form* $\sum_{0\le j\le n-1} q_j(\beta)x^j$ *where the* q_j *are polynomials which are very closely related to* f.]

Proposition. Given a monic polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, denote by $p_k(x)$ the sum of all terms of degree $\le k$, i.e.

$$p_k(x) := a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0.$$

Now set

$$q_k(x) := \frac{p(x) - p_k(x)}{x^{k+1}}.$$

If β is one of the n roots of $p(x)$, then the roots of

$$\hat{p}(x) := x^{n-1} + q_{n-2}(\beta)x^{n-2} + q_{n-3}(\beta)x^{n-3} + \cdots + q_1(\beta)x + q_0(\beta)$$

are precisely the other $n-1$ roots of $p(x)$.

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots (not necessarily distinct) of $p(x)$. Then

$$p(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots \pm s_n$$

where

$$\begin{aligned} s_1 &= \sum_{1\le i\le n} \alpha_i \\ s_2 &= \sum_{1\le i<j\le n} \alpha_i\alpha_j \\ s_3 &= \sum_{1\le i<j<k\le n} \alpha_i\alpha_j\alpha_k \\ &\vdots \\ s_n &= \alpha_1\alpha_2\alpha_3\ldots\alpha_n. \end{aligned}$$

(The s_n are called *symmetric polynomials*, and play an important role in the history of Galois theory.) Comparing these coefficients to those of $p(x)$, we see that

$$s_t = (-1)^t a_{n-t}.$$

Continued on next page...

We're given a root β of $p(x)$; WLOG let's say $\beta = \alpha_1$. The unique monic polynomial of degree $n-1$ with all the other α_i as its roots is

$$\hat{p}(x) = (x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n) = x^{n-1} - \hat{s}_1 x^{n-2} + \hat{s}_2 x^{n-3} - \cdots \pm \hat{s}_{n-1}$$

where

$$\hat{s}_1 = \sum_{2\le i\le n} \alpha_i = s_1 - \beta,$$

$$\hat{s}_2 = \sum_{2\le i<j\le n} \alpha_i\alpha_j = s_2 - \beta\hat{s}_1 = s_2 - \beta s_1 + \beta^2,$$

$$\hat{s}_3 = s_3 - \alpha_1\hat{s}_2 = s_3 - \beta(s_2 - \beta s_1 + \beta^2) = s_3 - \beta s_2 + \beta^2 s_1 - \beta^3,$$

and so on until

$$\hat{s}_{n-1} = s_{n-1} - \beta s_{n-2} + \beta^2 s_{n-3} - \ldots \pm \beta^{n-1}.$$

Applying some elbow grease, we deduce that the coefficient of x^t in $\hat{p}(x)$ is

$$(-1)^{n-1-t}\hat{s}_{n-1-t} = a_{t+1} + a_{t+2}\beta + \cdots + a_{n-2}\beta^{n-3-t} + a_{n-1}\beta^{n-2-t} + \beta^{n-1-t}.$$

Some algebraic manipulation yields the claim. □

2.2 In class we discovered how to find the roots of a specific cubic. Here we explore this further.

(a) Using the method we described in class, derive a formula which always produces a root of x^3+cx+d. [*You should arrive at* $\sqrt[3]{-\frac{d}{2}+\sqrt{\frac{c^3}{27}+\frac{d^2}{4}}}+\sqrt[3]{-\frac{d}{2}-\sqrt{\frac{c^3}{27}+\frac{d^2}{4}}}$]

Straightforward adaptation of our work from class.

(b) Note that 3 is a root of $x^3-3x-18$. What does the formula from part (a) give? Is it obvious that this is equal to 3?

We easily verify that 3 is a root of $p(x) = x^3 - 3x - 18$. Plugging $c = -3$ and $d = -18$ into the formula given in part (a) we produce a root α of $p(x)$:

$$\begin{aligned}\alpha &= \sqrt[3]{-\frac{d}{2}+\sqrt{\frac{c^3}{27}+\frac{d^2}{4}}}+\sqrt[3]{-\frac{d}{2}-\sqrt{\frac{c^3}{27}+\frac{d^2}{4}}}\\ &= \sqrt[3]{9+\sqrt{-1+81}}+\sqrt[3]{9-\sqrt{-1+81}}\\ &= \sqrt[3]{9+4\sqrt{5}}+\sqrt[3]{9-4\sqrt{5}}.\end{aligned}$$

To simplify this further, we need to find x, y such that

$$(x+y\sqrt{5})^3 = 9+4\sqrt{5}.$$

This is equivalent to solving the simultaneous equations

$$\begin{aligned}x^3 + 15xy^2 &= 9\\ 3x^2y + 5y^3 &= 4.\end{aligned}$$

continued on next page...

Solving the first equation for y and plugging it into the second produces, after some intense algebraic manipulations and clever substitutions, the equation $x^3 - 3x - 18 = 0$. We've returned to our original equation! Thus we see that without some divine inspiration, this problem is hopeless. This is why the cubic formula is not usually so helpful.

It turns out that divine inspiration struck some of you, however: you observed that

$$\left(\frac{3}{2} \pm \frac{1}{2}\sqrt{5}\right)^3 = 9 \pm 4\sqrt{5}.$$

This implies that

$$\alpha = \sqrt[3]{9 + 4\sqrt{5}} + \sqrt[3]{9 - 4\sqrt{5}} = \left(\frac{3}{2} + \frac{1}{2}\sqrt{5}\right) + \left(\frac{3}{2} - \frac{1}{2}\sqrt{5}\right) = 3.$$

Mathemagic!

(c) Consider the cubic $(x-1)(x-2)(x+3)$ with roots 1, 2, -3. Can you determine, without calculator or computer, which of these three roots the cubic formula from part (a) produces? [*This type of phenomenon forced people to recognize the existence—or at least, the utility!—of imaginary numbers.*]

Consider the cubic equation $p(x) = (x-1)(x-2)(x+3) = x^3 - 7x + 6$. Plugging in the values $c = -7, d = 6$ into the formula from part (a) we see that some root of this equation is given by

$$\begin{aligned}
\alpha &= \sqrt[3]{-\frac{d}{2} + \sqrt{\frac{c^3}{27} + \frac{d^2}{4}}} + \sqrt[3]{-\frac{d}{2} - \sqrt{\frac{c^3}{27} + \frac{d^2}{4}}} \\
&= \sqrt[3]{-3 + \sqrt{-\frac{343}{27} + 9}} + \sqrt[3]{-3 - \sqrt{-\frac{343}{27} + 9}} \\
&= \sqrt[3]{-3 + \sqrt{-\frac{100}{27}}} + \sqrt[3]{-3 - \sqrt{-\frac{100}{27}}} \\
&= \sqrt[3]{-3 + \frac{10}{27}\sqrt{-27}} + \sqrt[3]{-3 - \frac{10}{27}\sqrt{-27}}.
\end{aligned}$$

In order to evaluate this sum, we need to find a cube root of $-3 + \frac{10}{27}\sqrt{-27}$ in $\mathbb{C}$. For any $a, b \in \mathbb{Q}$ we have that

$$(a + b\sqrt{-27})^3 = a^3 + 3a^2b\sqrt{-27} - 81ab^2 - 27b^3\sqrt{-27} = (a^3 - 81ab^2) + (3a^2b - 27b^3)\sqrt{-27}$$

$$\implies (a - b\sqrt{-27})^3 = (a^3 - 81ab^2) - (3a^2b - 27b^3)\sqrt{-27}.$$

Therefore, in order to find such a cube root we need to find $a, b \in \mathbb{Q}$ such that $a^3 - 81ab^2 = -3$ and $3a^2b - 27b^3 = \frac{10}{27}$. As in part (b), this is a totally hopeless problem without divine inspiration.

continued on next page...

However, some of you were inspired. It turns out there are three such pairs (a, b), namely $(\frac{1}{2}, -\frac{5}{18}), (1, \frac{2}{9})$, and $(-\frac{3}{2}, \frac{1}{18})$. These correspond to the three different roots $1, 2$, and -3 of $p(x)$ since choosing them in turn yields

$$\alpha_1 = \sqrt[3]{-3 + \frac{10}{27}\sqrt{-27}} + \sqrt[3]{-3 - \frac{10}{27}\sqrt{-27}} = \left(\frac{1}{2} - \frac{5}{18}\sqrt{-27}\right) + \left(\frac{1}{2} + \frac{5}{18}\sqrt{-27}\right) = 1,$$

$$\alpha_2 = \sqrt[3]{-3 + \frac{10}{27}\sqrt{-27}} + \sqrt[3]{-3 - \frac{10}{27}\sqrt{-27}} = \left(1 + \frac{2}{9}\sqrt{-27}\right) + \left(1 - \frac{2}{9}\sqrt{-27}\right) = 2,$$

$$\alpha_3 = \sqrt[3]{-3 + \frac{10}{27}\sqrt{-27}} + \sqrt[3]{-3 - \frac{10}{27}\sqrt{-27}} = \left(-\frac{3}{2} + \frac{1}{18}\sqrt{-27}\right) + \left(-\frac{3}{2} - \frac{1}{18}\sqrt{-27}\right) = -3.$$

This is rather suspicious: the formula is supposed to produce one of the roots, not all three! It's also worth pointing out that without being able to extract square roots of negative numbers, the formula would immediately fail, whereas if we allow imaginary numbers then it's at least hypothetically possible to use the formula to find the roots. Examples like this led to the invention of imaginary numbers.

Summarizing parts (b) and (c), we see that the cubic formula is rubbish when it comes to actually determining the roots of a cubic. On the other hand, it does reduce solving an arbitrary cubic to solving some simpler equations... a point we'll return to later in the course.

(d) Use the cubic formula to explicitly determine one solution of the equation $x^3 - 6x^2 + 21x - 22 = 0$.

We first complete the cube. Noting that $(x-2)^3 = x^3 - 6x^2 + 12x - 8$, we have

$$x^3 - 6x^2 + 21x - 22 = (x-2)^3 + 9x - 14 = (x-2)^3 + 9(x-2) + 4.$$

We've therefore reduced the problem to finding a root of the auxiliary cubic $f(x) = x^3 + 9x + 4$. Using the formula in part (a) with $c = 9$, $d = 4$ produces a root of f:

$$\begin{aligned}\sqrt[3]{-\frac{d}{2} + \sqrt{\frac{c^3}{27} + \frac{d^2}{4}}} + \sqrt[3]{-\frac{d}{2} - \sqrt{\frac{c^3}{27} + \frac{d^2}{4}}} &= \sqrt[3]{-2 + \sqrt{27+4}} + \sqrt[3]{-2 - \sqrt{27+4}} \\ &= \sqrt[3]{-2 + \sqrt{31}} + \sqrt[3]{-2 - \sqrt{31}}\end{aligned}$$

It immediately follows that

$$2 + \sqrt[3]{-2 + \sqrt{31}} + \sqrt[3]{-2 - \sqrt{31}}$$

is a root of the given cubic.

2.3 The goal of this exercise is to review and develop some nice properties of symmetric groups.

(a) Prove that the collection of adjacent transpositions

$$\{(k\ k+1) : 1 \leq k < n\}$$

generates all of S_n.

Observe that $(n\ n+m) = (n\ n+1)(n+1\ n+m)(n\ n+1)$. The claim follows by a straightforward induction on m.

(b) Prove that the transposition $(1\ 2)$ and the n-cycle $(1\ 2\ \cdots\ n)$ generate all of S_n. [*Hint: use part (a).*]

Observe that $(k+1\ k+2) = (1\ 2\ \ldots\ n)(k\ k+1)(1\ 2\ \ldots\ n)^{-1}$ for all $1 \leq k < n-1$. Thus we can generate all adjacent transpositions. By part (a), we can then generate all of S_n.

(c) Prove that given a prime p, any transposition and any p-cycle generate all of S_p. [*Hint: relabel elements to put yourself in a position to use part (b).*]

Without loss of generality, relabel the p-cycle as $(0\ 1\ \ldots\ p-1)$ and the transposition as $(0\ j)$. A similar argument as in part (b) allows us to generate all transpositions $(a\ b)$ such that $b - a \equiv j \pmod{p}$. Since p is prime, j is a generator of the index set $\mathbb{Z}_p$. Thus, we can relabel each transposition of the form $(kj\ (k+1)j)$ as $(k\ k+1)$. Then we can generate all of S_p by part (a).

(d) Show by example that primality is a necessary condition in part (c). In other words, find an integer n, as well as a transposition and an n-cycle in S_n, which do *not* generate S_n.

I claim $(1\ 3)$ and $(1\ 2\ 3\ 4)$ do not generate S_4. To see this, let $r := (1\ 3)$ and $f := (1\ 2\ 3\ 4)$, and observe that we have the relations

$$r^2 = () = f^4 \qquad \text{and} \qquad fr = rf^3.$$

Thus r and f generate the dihedral group D_8 inside of S_4.

(e) Suppose $\varphi : S_n \to \{\pm 1\}$ is a nontrivial homomorphism. Prove that φ is the sign function on S_n. [*Hint: start by proving that $\varphi(\sigma) = \varphi\big((1\ 2)\big)$ for any transposition $\sigma \in S_n$.*]

Lemma. $\varphi(\sigma) = \varphi\big((1\ 2)\big)$ for any transposition $\sigma \in S_n$.

Proof. Observe that any nontrivial transposition $(m\ n)$ is conjugate to $(1\ 2)$:

$$(m\ n) = (1\ m)(2\ n)(1\ 2)(2\ n)(1\ m).$$

Since φ is a homomorphism and $\{\pm 1\}$ is abelian, we deduce that $\varphi\big((m\ n)\big) = \varphi\big((1\ 2)\big)$. □

There are therefore two cases to consider:

- $\varphi\big((1\ 2)\big) = 1$. Then the lemma implies $\varphi(\sigma) = 1$ for all transpositions $\sigma \in S_n$. Since S_n is generated by transpositions, we deduce that φ is the trivial homomorphism.
- $\varphi\big((1\ 2)\big) = -1$. Then the lemma implies $\varphi(\sigma) = -1$ for all transpositions $\sigma \in S_n$. Since σ agrees with sgn on a set of generators of S_n, we deduce that $\sigma = \operatorname{sgn}$ on all of S_n.

Combining these two cases concludes the proof. □

(f) Suppose $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct complex numbers, and $\sigma \in S_n$. What is the relationship between

$$\prod_{i<j}(\alpha_i - \alpha_j) \qquad \text{and} \qquad \prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$$

in terms of σ? Prove your assertion. [*Hint: use part (e).*]

Claim. $\prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = \operatorname{sgn}(\sigma) \prod_{i<j}(\alpha_i - \alpha_j)$.

Proof. Define $\varphi : S_n \to \{\pm 1\}$ by

$$\varphi(\sigma) := \prod_{i<j} \frac{\alpha_{\sigma(i)} - \alpha_{\sigma(j)}}{\alpha_i - \alpha_j}.$$

Observe that φ is a homomorphism, since

$$\varphi(\sigma\tau) = \prod_{i<j} \frac{\alpha_{\sigma\tau(i)} - \alpha_{\sigma\tau(j)}}{\alpha_i - \alpha_j} = \prod_{i<j} \frac{\alpha_{\sigma\tau(i)} - \alpha_{\sigma\tau(j)}}{\alpha_{\tau(i)} - \alpha_{\tau(j)}} \cdot \frac{\alpha_{\tau(i)} - \alpha_{\tau(j)}}{\alpha_i - \alpha_j} = \varphi(\sigma)\varphi(\tau).$$

Moreover, φ isn't the trivial homomorphism, since $\varphi\big((1\ 2)\big) = -1$. Part (e) immediately implies that $\varphi = \operatorname{sgn}$ as claimed. □

2.4 The goal of this exercise is to calculate the Galois group of $f(x) := x^4 - 2$. Denote the roots of f as follows:

$$\alpha_1 := \sqrt[4]{2} \quad \alpha_2 := i\sqrt[4]{2} \quad \alpha_3 := -\sqrt[4]{2} \quad \alpha_4 := -i\sqrt[4]{2}$$

(a) Explain why (1 2) isn't an element of $\operatorname{Gal}(f)$. [*Find a rational relation which isn't invariant under this permutation.*]

The transposition (1 2) does not preserve the rational relation $\alpha_1 + \alpha_3 = 0$.

(b) List all elements of $\operatorname{Gal}(f)$.

Writing $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$ and expanding, we deduce four equations

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$$
$$\sum_{i<j} \alpha_i\alpha_j = 0$$
$$\sum_{i<j<k} \alpha_i\alpha_j\alpha_k = 0$$
$$\alpha_1\alpha_2\alpha_3\alpha_4 = -2$$

Four equations, four variables—it seems like we're done! But these aren't a great set of relations, because they are too generic; they imply that the α_i are completely symmetric, which is not the case. For example, $\alpha_1 + \alpha_3 = 0$ but $\alpha_1 + \alpha_2 \neq 0$, but good luck deducing this from the above!

continued on next page...

Some playing around should convince you that the four rational relations

$$\begin{aligned}\alpha_1 + \alpha_3 &= 0\\ \alpha_2 + \alpha_4 &= 0\\ \alpha_1\alpha_3 + \alpha_2\alpha_4 &= 0\\ \alpha_1\alpha_2\alpha_3\alpha_4 &= -2\end{aligned}$$

suffice to generate all rational relations among the roots. This yields the following Galois group:

$$\mathrm{Gal}(f) = \{(), (1\ 3), (2\ 4), (1\ 3)(2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\}.$$

NOTES. You might have started to wonder when exactly you can be sure you have derived all the symmetry constraints. You were not expected to be able to show this rigorously when solving this problem. As you will see, when we approach this more abstractly, we will be able to use our knowledge of the subgroup structure of symmetry groups (along with other group-theoretic information) to narrow down the possible subgroup candidates for the Galois group. But even in the more sophisticated approach, there is no simple mechanical algorithm.

(c) $\mathrm{Gal}(f)$ is isomorphic to a familiar group. Which one?

$\mathrm{Gal}(f) \simeq D_8$, the dihedral group of order 8. (See problem **2.3**(d) above.)

(d) Denote $G_0 := \mathrm{Gal}(f)$, and set $G_i := [G_{i-1}, G_{i-1}]$ for all i. Does this sequence terminate? Explain why the Galois theoretic prediction agrees with what you know about the shape of the roots.

Write $D_8 = \langle r, f : r^4 = f^2 = e, fr = r^3 f\rangle$. Then we have $G_1 := [D_8, D_8] = \{e, r^2\}$. Since this is abelian, it follows that $G_2 := [G_1, G_1]$ is trivial. Galois theory therefore predicts that the roots should have one radical nested inside another, which is consistent with what we know about the roots: they are all of the form $\sqrt[4]{q} = \sqrt{\sqrt{q}}$ for some $q \in \mathbb{Q}$.

2.5 The goal of this exercise is to prove

Cayley's Theorem. *Every finite group can be embedded in a symmetric group.*

Suppose G is a finite group. For each $g \in G$, define the function

$$\begin{aligned}\phi_g : G &\longrightarrow G\\ a &\longmapsto ga\end{aligned}$$

(a) Prove that $\phi_g \in S_G$ for every $g \in G$. Here S_G denotes the symmetric group of G.

Note that ϕ_g is an injection, since if $ga = \phi_g(a) = \phi_g(b) = gb$ then $a = b$. Since any injection from a finite set to itself must be a bijection, we deduce that ϕ_g is bijective. It follows that $\phi_g \in S_G$.

(b) Let $\phi : G \to S_G$ be the function defined by $\phi(g) = \phi_g$. Prove that ϕ is an injective homomorphism.

First we show that ϕ is a homomorphism. Note that for any $x, g, h \in G$ we have

$$(\phi_g \circ \phi_h)(x) = ghx = \phi_{gh}(x)$$

by associativity. Thus, $\phi(gh) = \phi_{gh} = \phi_g \circ \phi_h = \phi(g) \circ \phi(h)$, which shows that ϕ is a homomorphism.

Next we show that ϕ is injective. Suppose $\phi(g) = \phi(h)$. Then $\phi_g(x) = \phi_h(x)$ for all $x \in G$, whence $gx = hx$. But this implies $g = h$. Thus ϕ is injective.

(c) Prove that if G has order n, then it is isomorphic to a subgroup of S_n.

Since $\phi : G \to S_G$ is an injective homomorphism, we deduce that $G \simeq \text{im } \phi$, which is a subgroup of S_G. Finally, $S_G \simeq S_n$, whence im ϕ is isomorphic to a subgroup of S_n.

Extra Credit. Find (with proof!) a minimal set of rational relations among the roots of $f(x) = x^4 - 5x^2 + 6$ that generate all rational relations. (In other words, find a set of rational relations such that (a) none of them can be derived from the others, and (b) every rational relation can be derived from them.)