Math 4010/5530 # Galois Correspondence **Oct. 2019**

The goal of this sheet is to thoroughly explore the splitting field of $x^3-2 \in \mathbb{Q}[x]$ and its Galois group.

First, recall that $\omega = e^{2\pi i/3} = \dfrac{-1+\sqrt{3}i}{2}$ is a primitive third root of unity. Of course, so is $\omega^2 = \dfrac{-1-\sqrt{3}i}{2}$. Let $\alpha = \sqrt[3]{2} = 2^{1/3}$ (i.e., the real root of x^3-2). Then since $(\omega\alpha)^3 = \omega^3\alpha^3 = 1\cdot 2 = 2$ and likewise $(\omega^2\alpha)^3 = 2$, we have that $x^3-2 = (x-\alpha)(x-\omega\alpha)(x-\omega^2\alpha)$. Therefore, $\mathbb{E} = \mathbb{Q}[\alpha, \omega\alpha, \omega^2\alpha]$ is the splitting field of x^3-2 (over $\mathbb{Q}$).

While the above description of the splitting field is accurate, it is not the best description for constructing automorphisms. Instead, following our discussion in class, we might first want to attach roots of unity (i.e., ω and ω^2) and then attach a root (and thus all roots) of x^3-2. Further, notice that $\omega = (\omega\alpha)/\alpha \in \mathbb{E}$ so that $\mathbb{Q}[\alpha,\omega] \subseteq \mathbb{E}$. And clearly since $\alpha, \omega\alpha, \omega^2\alpha \in \mathbb{Q}[\alpha,\omega]$, we have that in fact $\mathbb{E} = \mathbb{Q}[\alpha,\omega]$. This suggests the following (radical) tower: $\mathbb{Q} \subseteq \mathbb{Q}[\omega] \subseteq \mathbb{Q}[\alpha,\omega]$. Notice that the first step in the tower is a pure extension of type 2: the minimal polynomial for ω is the cyclotomic polynomial $\Phi_2(x) = x^2+x+1$. The second step in the tower is a pure extension of type 3: the minimal polynomial for $\alpha = \sqrt[3]{2}$ (working over $\mathbb{Q}[\omega]$) still is x^3-2.

This also confirms that $[\mathbb{Q}[\alpha,\omega]:\mathbb{Q}] = [\mathbb{Q}[\alpha,\omega]:\mathbb{Q}[\omega]]\cdot[\mathbb{Q}[\omega]:\mathbb{Q}] = 3\cdot 2 = 6$. In more detail, notice that a basis for the first extension (i.e., $\mathbb{Q}[\omega]/\mathbb{Q}$) is $\{1,\omega\}$ and a basis for the second extension (i.e., $\mathbb{Q}[\alpha,\omega]/\mathbb{Q}[\omega]$) is $\{1,\alpha,\alpha^2\}$. Thus a basis for the full extension (i.e., $\mathbb{Q}[\alpha,\omega]/\mathbb{Q}$) is the product of these bases $\{1,\omega,\alpha,\omega\alpha,\alpha^2,\omega\alpha^2\}$.

Now let's build all of the Galois automorphisms. We start with the identity map on $\mathbb{Q}$: $1_{\mathbb{Q}}$. (*Note*: To build a Galois group, we build up from the identity map, but in this case the identity map also happens to be the *only* automorphism of $\mathbb{Q}$.) Our extension theorem, says the extensions of the identity to $\mathbb{Q}[\omega]$ send ω to any root (i.e., ω or ω^2) of the irreducible polynomial: x^2+x+1 (ω's minimal polynomial). Thus ω must either map to itself or to ω^2. Let's call the resulting isomorphisms φ_1 and φ_2. We have φ_1: $1\mapsto 1$ and $\omega\mapsto\omega$ (the identity on $\mathbb{Q}[\omega]$) as well as φ_2: $1\mapsto 1$ and $\omega\mapsto\omega^2$.

$$\mathbb{Q}[\alpha,\omega] \overset{\psi_{ij}}{\dashrightarrow} \mathbb{Q}[\alpha,\omega]$$

$$\mathbb{Q}[\omega] \overset{\varphi_i}{\dashrightarrow} \mathbb{Q}[\omega]$$

$$\mathbb{Q} \xrightarrow{1_{\mathbb{Q}}} \mathbb{Q}$$

Next, we extend both φ_1 and φ_2 from $\mathbb{Q}[\omega]$ to $\mathbb{Q}[\alpha,\omega]$. Note the degree of α's minimal polynomial (over $\mathbb{Q}[\omega]$) is $[\mathbb{Q}[\alpha,\omega]:\mathbb{Q}[\omega]] = 3$ and α is a root of $x^3-2 \in \mathbb{Q}[\omega][x]$, so x^3-2 is still α's minimal polynomial over $\mathbb{Q}[\omega]$ (and thus irreducible). Once again, our extension theorem says we can extend any automorphism of $\mathbb{Q}[\omega]$ (i.e., φ_1 or φ_2) to $\mathbb{Q}[\alpha,\omega]$ sending α to any root of x^3-2 (i.e., α, $\omega\alpha$, or $\omega^2\alpha$). So φ_1 can be extended in three ways which we call ψ_{11}, ψ_{12}, and ψ_{23}. Likewise we extend φ_2 and get ψ_{21}, ψ_{22}, and ψ_{23}. The table below summarizes these automorphisms by indicating their action on our basis for $\mathbb{Q}[\alpha,\omega]$:

	ψ_{11}			ψ_{12}			ψ_{13}		
1	$\mapsto$	1	1	$\mapsto$	1	1	$\mapsto$	1
ω	$\mapsto$	ω	ω	$\mapsto$	ω	ω	$\mapsto$	ω
α	$\mapsto$	α	α	$\mapsto$	$\omega\alpha$	α	$\mapsto$	$\omega^2\alpha = -\alpha-\omega\alpha$
$\omega\alpha$	$\mapsto$	$\omega\alpha$	$\omega\alpha$	$\mapsto$	$\omega^2\alpha = -\alpha-\omega\alpha$	$\omega\alpha$	$\mapsto$	α
α^2	$\mapsto$	α^2	α^2	$\mapsto$	$\omega^2\alpha^2 = -\alpha^2-\omega\alpha^2$	α^2	$\mapsto$	$\omega\alpha^2$
$\omega\alpha^2$	$\mapsto$	$\omega\alpha^2$	$\omega\alpha^2$	$\mapsto$	α^2	$\omega\alpha^2$	$\mapsto$	$\omega^2\alpha^2 = -\alpha^2-\omega\alpha^2$

	ψ_{21}			ψ_{22}			ψ_{23}		
1	$\mapsto$	1	1	$\mapsto$	1	1	$\mapsto$	1
ω	$\mapsto$	$\omega^2 = -1-\omega$	ω	$\mapsto$	$\omega^2 = -1-\omega$	ω	$\mapsto$	$\omega^2 = -1-\omega$
α	$\mapsto$	α	α	$\mapsto$	$\omega\alpha$	α	$\mapsto$	$\omega^2\alpha = -\alpha-\omega\alpha$
$\omega\alpha$	$\mapsto$	$\omega^2\alpha = -\alpha-\omega\alpha$	$\omega\alpha$	$\mapsto$	α	$\omega\alpha$	$\mapsto$	$\omega\alpha$
α^2	$\mapsto$	α^2	α^2	$\mapsto$	$\omega^2\alpha^2 = -\alpha^2-\omega\alpha^2$	α^2	$\mapsto$	$\omega\alpha^2$
$\omega\alpha^2$	$\mapsto$	$\omega^2\alpha^2 = -\alpha^2-\omega\alpha^2$	$\omega\alpha^2$	$\mapsto$	$\omega\alpha^2$	$\omega\alpha^2$	$\mapsto$	α^2

Let's unpack where the formula for ψ_{22} comes from. Recall that ψ_{22} extends φ_2. So we send $\psi_{22}(\omega) = \varphi_2(\omega) = \omega^2$. Also, recall $0 = \Psi_2(\omega) = \omega^2+\omega+1$, so $\omega^2 = -\omega-1$. Thus $\psi_{22}(\omega) = -\omega-1$. Next, ψ_{22} is the second extension of φ_2 so $\psi_{22}(\alpha) = \omega\alpha$. All the rest of the values of ψ_{22} follow from these values. For example, any automorphism must map $\psi_{22}(1) = 1$, but we could also note $\psi_{22}(1) = \psi_{22}(\omega^3) = (\psi_{22}(\omega))^3 = (\omega^2)^3 = \omega^6 = 1$ where we pull an exponent out of our automorphism. Next, $\psi_{22}(\omega\alpha) = \psi_{22}(\omega)\psi_{22}(\alpha) = \omega^2\cdot\omega\alpha = \omega^3\alpha = \alpha$ and $\psi_{22}(\alpha^2) = (\psi_{22}(\alpha))^2 = (\omega\alpha)^2 = \omega^2\alpha^2 = -\alpha^2-\omega\alpha^2$. Finally, $\psi_{22}(\omega\alpha^2) = \psi_{22}(\omega)\psi_{22}(\alpha^2) = \omega^2\cdot\omega^2\alpha^2 = \omega\alpha^2$. In general, (for $a,b,c,d,e,f \in \mathbb{Q}$):

$$\begin{aligned}\psi_{22}(a+b\omega+c\alpha+d\omega\alpha+e\alpha^2+f\omega\alpha^2) &= a+b(-1-\omega)+c\omega\alpha+d\alpha+e(-\alpha^2-\omega\alpha^2)+f\omega\alpha^2\\ &= (a-b)-b\omega+d\alpha+c\omega\alpha-e\alpha^2+(f-e)\omega\alpha^2\end{aligned}$$

Notice that we **do not** permute the basis elements. On the other hand, these maps **do permute the roots** of x^3-2. For example, $\psi_{22}(\alpha) = \omega\alpha$, $\psi_{22}(\omega\alpha) = \alpha$, and $\psi_{22}(\omega^2\alpha) = \omega^4\cdot\omega\alpha = \omega^2\alpha$.

Side note: One might ask why we didn't just define the automorphisms in terms of permutations to begin with?! Well, we could have. For this particular example, our Galois group is isomorphic to S_3, so every permutation corresponds with an automorphism. However, if this were not the case, figuring out which permutations are *valid* permutations can be very difficult. If you pick a random splitting field and randomly shuffle roots around, it's possible that such a shuffling cannot be extended to a mapping on the whole field that preserves addition and multiplication. In other words, a permutation of generators for a field does not generally extend to an automorphism.

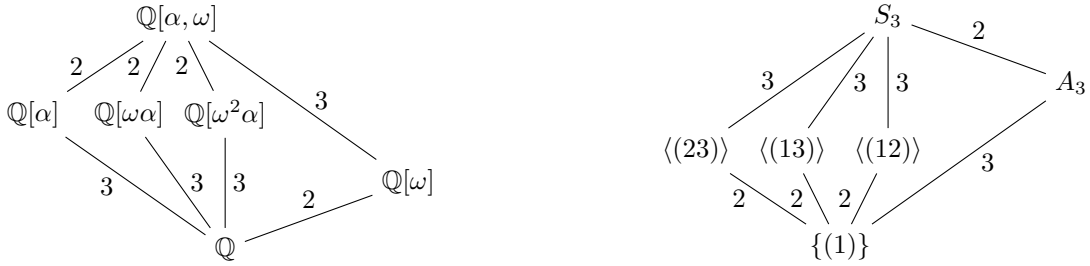
If we label the roots $\alpha \leftrightarrow 1$, $\omega\alpha \leftrightarrow 2$, and $\omega^2\alpha \leftrightarrow 3$, then ψ_{22} is the permutation (12) (swap 1 and 2 while fixing 3). This leads to an explicit isomorphism $F : \mathrm{Gal}(\mathbb{Q}[\alpha,\omega]/\mathbb{Q}) \to S_3$ where $F(\psi_{11}) = (1)$, $F(\psi_{12}) = (123)$, $F(\psi_{13}) = (132)$, $F(\psi_{21}) = (23)$, $F(\psi_{22}) = (12)$, and $F(\psi_{23}) = (13)$.

Using this isomorphism to identify the Galois group and S_3 (e.g., $\langle(23)\rangle = \{(1),(23)\} = \{\psi_{11},\psi_{21}\}$), we can identify all of the fixed fields: $(\mathbb{Q}[\alpha,\omega])^{(1)} = \mathbb{Q}[\alpha,\omega]$, $(\mathbb{Q}[\alpha,\omega])^{\langle(23)\rangle} = \mathbb{Q}[\alpha]$, $(\mathbb{Q}[\alpha,\omega])^{\langle(13)\rangle} = \mathbb{Q}[\omega\alpha]$, $(\mathbb{Q}[\alpha,\omega])^{\langle(12)\rangle} = \mathbb{Q}[\omega^2\alpha]$, $(\mathbb{Q}[\alpha,\omega])^{A_3} = \mathbb{Q}[\omega]$, and $(\mathbb{Q}[\alpha,\omega])^{S_3} = \mathbb{Q}$.

Explicitly calculating fixed fields can be tricky. However, using the fundamental theorem of Galois theory (identifying the dualized subgroup lattice with a subfield lattice) makes the determination fairly straight forward. For example, obviously, $\langle(12)\rangle$ fixes $3 \leftrightarrow \omega^2\alpha$, so $(\mathbb{Q}[\alpha,\omega])^{\langle(12)\rangle} = \mathbb{Q}[\omega^2\alpha]$.

Notice that ω is fixed by ψ_{11}, ψ_{12}, and ψ_{13} (i.e., $A_3 = \{(1),(123),(132)\}$). Another way to see that this subgroup and intermediate field go together, notice that $[\mathbb{Q}[\omega] : \mathbb{Q}] = 2$ and the only subgroup of index $2 = [S_3 : A_3]$ is A_3. So these must go together: $\mathbb{Q}[\alpha,\omega]^{A_3} = \mathbb{Q}[\omega]$.

The lattice of intermediate fields of $\mathbb{Q}[\alpha,\omega]/\mathbb{Q}$ and subgroup lattice of S_3 are shown below. The numbers on the edges indicate degrees in the case of fields and indices in the case of subgroups.



Now $\{(1)\}$, A_3, and S_3 are normal subgroups of S_3. This means that $\mathbb{Q}[\alpha,\omega]$, $\mathbb{Q}[\omega]$, and $\mathbb{Q}$ are all Galois extensions of $\mathbb{Q}$. In fact, they are splitting fields of x^3-2, x^2+x+1, and 1 respectively. Alternatively, $\mathbb{Q}[\alpha,\omega]^{\mathrm{Gal}(\mathbb{Q}[\alpha,\omega]/\mathbb{Q})} = \mathbb{Q}[\alpha,\omega]^{S_3} = \mathbb{Q}$, $\mathbb{Q}[\omega]^{\mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})} = \mathbb{Q}[\omega]^{\{1,\mathrm{conjugation}\}} = \mathbb{Q}$, and $\mathbb{Q}^{\mathrm{Gal}(\mathbb{Q}/\mathbb{Q})} = \mathbb{Q}^{\{1\}} = \mathbb{Q}$ (thus they are Galois extensions).

Notice that $(123)\langle(23)\rangle(123)^{-1} = \{(123)(1)(123)^{-1},(123)(23)(123)^{-1}\} = \{(1),(123)(23)(132)\} = \{(1),(13)\} = \langle(13)\rangle$. Likewise, $(123)\langle(13)\rangle(123)^{-1} = \langle(12)\rangle$ and $(123)\langle(12)\rangle(123)^{-1} = \langle(23)\rangle$ (these subgroups are conjugate to each other). This means that these subgroups are not normal subgroups (normal subgroups are self-conjugate). Therefore, the corresponding intermediate fields are conjugate subfields and also those fields fail to be Galois subfields (i.e., they are not Galois extensions of $\mathbb{Q}$). In particular, $\mathbb{Q}[\alpha]$ corresponds with $\langle(12)\rangle$, $\mathbb{Q}[\omega\alpha]$ corresponds with $\langle(13)\rangle$, and $\mathbb{Q}[\omega^2\alpha]$ corresponds with $\langle(12)\rangle$. In addition, (123) is the automorphism ψ_{12}. We have $\psi_{12}(\mathbb{Q}[\alpha]) = \mathbb{Q}[\omega\alpha]$, $\psi_{12}(\mathbb{Q}[\omega\alpha]) = \mathbb{Q}[\omega^2\alpha]$, and $\psi_{12}(\mathbb{Q}[\omega^2\alpha]) = \mathbb{Q}[\alpha]$.

We could also see directly that these are not Galois extensions (of $\mathbb{Q}$). For example, $\mathbb{Q}[\alpha]$ is a degree 3 extension of $\mathbb{Q}$ (α is a root of the irreducible *cubic* polynomial x^3-2). Thus $\{1,\alpha,\alpha^2\}$ is a basis for $\mathbb{Q}[\alpha]$ (working over $\mathbb{Q}$). Suppose $\varphi \in \mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$. We always have $\varphi(1) = 1$. Next, φ must send roots (of polynomials in $\mathbb{Q}[x]$) to roots. Since α is a root of $x^3-2 \in \mathbb{Q}[x]$, we must have that $\varphi(\alpha)$ is a root of x^3-2. However, the roots of x^3-2 are α, $\omega\alpha$, and $\omega^2\alpha$. Notice that neither $\omega\alpha$ nor $\omega^2\alpha$ belong to $\mathbb{Q}[\alpha]$. Therefore, $\varphi(\alpha) = \alpha$ and since it's an automorphism, we also have $\varphi(\alpha^2) = \varphi(\alpha)^2 = \alpha^2$. This means that φ is the identity map! Thus $\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q}) = \{1\}$ so that $\mathbb{Q}[\alpha]^{\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})} = \mathbb{Q}[\alpha]^{\{1\}} = \mathbb{Q}[\alpha] \neq \mathbb{Q}$ (this is not a Galois extension). Likewise, for $\mathbb{Q}[\alpha]$'s conjugate fields.

Of course this makes sense. If $\mathbb{Q}[\alpha]$ were Galois, it would split any irreducible (over $\mathbb{Q}$) where one of the roots is in $\mathbb{Q}[\alpha]$. However, it has the root α of x^3-2 but not the other two roots. In some sense, Galois extensions have a *completeness* to them. $\mathbb{Q}[\alpha]$ isn't complete because it's missing $\omega\alpha$ and $\omega^2\alpha$ (the *conjugates* of α). A nice/complete subfield should contain whole sets of "conjugate" elements.

One final note: Since we are working over $\mathbb{Q}$ (the prime subfield of any field of characteristic 0) and since all automorphisms automatically fix their prime subfields, any Galois group of an extension over $\mathbb{Q}$ is just the automorphism group of that extension field. For example, $S_3 \cong \mathrm{Gal}(\mathbb{Q}[\alpha,\omega]/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}[\alpha,\omega])$ and $\mathrm{Aut}(\mathbb{Q}[\alpha]) = \mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q}) = \{1\}$.