# Homework 5

Kevin Guillen

MATH 202 — Algebra III — Spring 2022

**Problem 14.2.7** Determine all the subfields of the splitting field of $x^8 - 2$ which are Galois over $\mathbb{Q}$.

*Proof.* Let $K$ refer to the splitting field of the given polynomial. We know by the Fundamental Theorem of Galois Theory that for every subfield $E$ of $K$, there is a corresponding subgroup $H$ of the Galois group which fixes $E$. Which also gives us that $E$ will be Galois over $\mathbb{Q}$ if and only if $H$ is normal. To assist with this problem we can look at the last 2 lattice diagrams given at the end of this section chapter.

We know the subgroups of index 2 are normal and that the normality of subgroups of order 2 can be easily checked,

$$\sigma \left\langle \tau\sigma^{2k} \right\rangle \sigma^{-1} = \left\langle \tau\sigma^{2k+2} \right\rangle \neq \left\langle \tau\sigma^{2k} \right\rangle$$

meaning that these subgroups are not normal, but $\left\langle \sigma^4 \right\rangle$ is the center so it is normal.

Working with the subgroups of order 4 and conjugating them all by $\sigma$,

$$\begin{aligned}
\sigma \left\langle \tau\sigma^3 \right\rangle \sigma^{-1} &= \sigma \left\langle \tau\sigma \right\rangle \sigma^{-1} \\
\sigma \left\langle \tau\sigma \right\rangle \sigma^{-1} &= \sigma \left\langle \tau\sigma^3 \right\rangle \sigma^{-1} \\
\sigma \left\langle \sigma^4, \tau \right\rangle \sigma^{-1} &= \left\langle \sigma^4, \tau\sigma^2 \right\rangle \\
\sigma \left\langle \sigma^4, \tau\sigma^2 \right\rangle \sigma^{-1} &= \left\langle \sigma^4, \tau \right\rangle
\end{aligned}$$

we see that none of them are normal. Giving us that the only subgroup of order 4 that is invariant to conjugation by $\sigma$ is $\left\langle \sigma^2 \right\rangle$. Also note that $\tau\sigma^2\tau = \sigma^6 \in \left\langle \sigma^2 \right\rangle$, therefore $\left\langle \sigma^2 \right\rangle$ is normal.

So in all we have the normal subgroups of the Galois group to be

$$Gal(K/F), 1, \left\langle \sigma^2 \right\rangle, \left\langle \sigma^4 \right\rangle, \left\langle \sigma^2, \tau\sigma^3 \right\rangle, \left\langle \sigma^2, \tau \right\rangle, \text{ and } \left\langle \sigma \right\rangle.$$

Using the lattice diagrams given to us at the end of the chapter we see the corresponding subfields of $K$ which are Galois over $\mathbb{Q}$ are precisely (on the left),

$$\begin{aligned}
\mathbb{Q} &\longleftrightarrow Gal(K/F) \\
K &\longleftrightarrow 1 \\
\mathbb{Q}(i, \sqrt[4]{2}) &\longleftrightarrow \left\langle \sigma^2 \right\rangle \\
\mathbb{Q}(i, \sqrt{2}) &\longleftrightarrow \left\langle \sigma^4 \right\rangle \\
\mathbb{Q}(\sqrt{-2}) &\longleftrightarrow \left\langle \sigma^2, \tau\sigma^3 \right\rangle
\end{aligned}$$

$$\mathbb{Q}(\sqrt{2}) \longleftrightarrow \langle \sigma^2, \tau \rangle$$
$$\mathbb{Q}(i) \longleftrightarrow \langle \sigma \rangle .$$

□

**Problem 14.2.8** Suppose $K$ is Galois extension of $F$ of degree $p^n$ for some prime $p$ and some $n \geqslant 1$. Show there are Galois extensions of $F$ contained in $K$ of degrees $p$ and $p^{n-1}$.

*Proof.* Because $K$ is a Galois extension of $F$ of degree $p^n$ we know that its Galois group will be of order $p^n$. We know from Math 200 / Group Theory, that a group of order $p^n$ will have normal subgroups of order $p^k$ where $k = 0, \ldots, n$. Using this we know then there are normal subgroups of the Galois group of order $p^{n-1}$ and $p$, and by the correspondence given to us from the Fundamental Theorem of Galois Theory, we have that there must exist corresponding subfields of $K$ which are Galois extensions of $F$ and of degree $p$ and $p^{n-1}$. □

**Problem 14.2.13** Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.

*Proof.* Let $p(x) \in \mathbb{Q}[x]$ be of degree 3 (cubic) and for let us assume that is has a complex root. The Galois group has a subgroup generated by complex conjugation due to this complex root. This subgroup is $\mathbb{Z}/2\mathbb{Z}$ which isn't $\mathbb{Z}/3\mathbb{Z}$, meaning then that the Galois group of $p(x)$ can't be $\mathbb{Z}/3\mathbb{Z}$. Therefore if the Galois group is the cyclic group of order 3 then all the roots of $p(x)$ must be real. □

**Problem 14.3.3** Prove that an algebraically closed field must be infinite.

*Proof.* Let $F$ be a finite field. Let us consider a polynomial $p(x) \in F[x]$ specifically,

$$p(x) = 1 + \prod_{\alpha \in F} (x - \alpha).$$

It is clear that this $p(x)$ is indeed in $F[x]$ since all its coefficients are in $F$. We have by Ring Product with zero that $\prod_{\alpha \in F}(x - \alpha) = 0$ for all $x \in F$. Meaning that $p(x) = 1$ for all $x \in F$. Meaning $F$ is not algebraically closed. Therefore an algebraically closed field must be an infinite field.

□

**Problem 14.3.4** Construct the finite field of 16 elements and find a generator for the multiplicative group. How many generators are there?

*Proof.* Consider $\mathbb{F}_2$. We want to find an irreducible polynomial of degree 4 in order to help construct this field of 16 elements. We know polynomials like these though must be factors of $x^{2^4} - x$, giving us $x, x-1$, and $x^2+x+1$ which are degree less than 4. Therefore the polynomial of degree 4 needed can't be divided by the linear polynomials above (0 and 1 are not roots), and must not be divisible by $x^2+x+1$. It is clear a degree 4 polynomial meeting these requirements is

$$p(x) = x^4 + x^3 + x^2 + x + 1$$

, this let's us then construct,

$$\mathbb{F}_{16} \cong \mathbb{F}_2[x]/(p(x))$$

We see that $x$ unfortunately does not generate the multiplicative group of $\mathbb{F}_{16}$ since,

$$(x^5 - 1) = (x+1)(x^4 + x^3 + x^2 + x + 1) = 0$$

giving us that $x^5 = 1$. Let us consider $x+1$ though, we note that,

$$(x+1)^3 = x^3 + x^2 + x + 1 = x^4$$

therefore $\langle x \rangle = \langle x^4 \rangle \subseteq \langle x+1 \rangle$. Now note that $\langle x \rangle = x^k$ for $k = 0, \ldots, 4$, meaning $x+1 \notin \langle x \rangle$, therefore $\langle x+1 \rangle$ is a strictly large subgroup than $\langle x \rangle$, but the only bigger subgroup is $\mathbb{F}_{16}^\times$. Giving us that $x+1$ is a generator of the multiplicative group.

From here we know all the other generators are simply $(x+1)^k$ where $k$ is relatively prime to 15, this is given by the Euler's Totient function, $\varphi(15) = 8$. Meaning we have 8 generators in this multiplicative group. □

**Problem 14.3.8** Determine the splitting field of the polynomial $x^p - x - a$ over $\mathbb{F}_p$ where $a \neq 0$, $a \in \mathbb{F}_p$. Show explicitly that the Galois group is cyclic. [Show $\alpha \mapsto \alpha + 1$ is an automorphism.] Such an extension is called an Artin-Schreier extension.

*Proof.* Let $p(x) = x^p - x - a$, and let $\alpha$ be a root of $p(x)$. Notice now though,

$$\begin{aligned} p(\alpha+1) &= (\alpha+1)^p - (\alpha+1) - a && \text{Apply Prop. 35 from 13.5} \\ &= \alpha^p + 1^p - \alpha - 1 - a \\ &= \alpha^p - \alpha - a \\ &= 0. \end{aligned}$$

Therefore $\alpha + 1$ is also a root. ($\star$) Meaning the $p$ roots of $p(x)$ are just $\alpha + k$ where $k = 1, \ldots, p$. We also have then that $\alpha \notin \mathbb{F}_p$, because if that were the case we would

have $a = 0$ since $a = \alpha^p - \alpha = 0$, which would be a contradiction. So we have that $\mathbb{F}_p(\alpha)$ is the splitting field of the separable polynomial $p(x)$ (we know this from $\star$) over $\mathbb{F}_p$, thus $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is a Galois extension.

Now let us consider

$$\begin{aligned} \sigma : \mathbb{F}_p(\alpha) &\to \mathbb{F}_p(\alpha) \\ \alpha &\mapsto \alpha + 1 \end{aligned}$$

which fixes $\mathbb{F}_p$. Note that $\sigma$ has a two sided inverse defined by $\alpha \mapsto \alpha - 1$ which also fixed $\mathbb{F}_p$ meaning then that $\sigma \in \mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$.

We know by properties of the Galois group, that any other map $\pi$ in $\mathrm{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ must not only fix $\mathbb{F}_p$, but it must send $\alpha$ to a root of $p(x)$, meaning $\pi$ is of the form $\alpha \mapsto \alpha + k$ for some $k \in \mathbb{F}_p$ (which we showed to be the roots from $\star$). Notice though we if we take the powers of $\sigma$ that, $\sigma^k(\alpha) = \alpha + k = \pi(\alpha)$ and fixes $\mathbb{F}_p$, therefore $\sigma^k = \pi$. Meaning every element of the Galois group is simply a power of $\sigma$, and because $\sigma^p = 1$ we have that the Galois group is cyclic.

□

**Problem 14.3.11** Prove that $(x^p)^n - x + 1$ is irreducible over $\mathbb{F}_p$, only when $n = 1 = p = 2$. [Note that if $\alpha$ is a root, then so is $\alpha + \alpha$ for any $\alpha \in \mathbb{F}_{p^n}$. Show that this implies $\mathbb{F}_p(\alpha)$ contains $\mathbb{F}_{p^n}$ and that $[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] = p$]

*Proof.* Let $p(x) = (x^p)^n - x + 1$. If $\alpha$ is a root of $p(x)$ then so is $\alpha + k$ for any $k \in \mathbb{F}_p$. Therefore $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p(\alpha)$ because if not, the latter would contain all the roots of $x^{p^n} - x + 1$, which would lead to a contradiction. Now any automorphism of the Galois group of $\mathbb{F}_p(\alpha)/\mathbb{F}_{p^n}$ must be defined by $\alpha \mapsto \alpha + k$ for some $k \in \mathbb{F}_{p^n}$, and because they fix $\mathbb{F}_{p^n}$ they are all of order $p$. Because a Galois group of degree $d$ is always cyclic over $\mathbb{F}_p$, with a generator $\sigma_p$, and thus cyclic over $\mathbb{F}_{p^n}$, we have $[\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}] = p$.

So we must have that $p^n = pn$. Now we write $n = p^k$ for $k \geqslant 0$. If we have that $k > 1$, then we have $k + 1 = p^k$, but $p \geqslant 2$, so $k + 1 < 2^k \leqslant p^k$ when $k = 2$ and through induction we have that,

$$(k+1) + 1 < 2^k + 1 \leqslant 2^k + (2^{k+1} - 2^k) = 2^{k+1} \leqslant p^{k+1}$$

$k$ must be 0 and $n = 1$, or $k = 1$ and $n = p$ with $p^2 = p^n$ and $n = p = 2$. Therefore $x^p - x + 1$ is irreducible and we see that $x^4 - x + 1 \in \mathbb{F}_2[x]$ has no roots and is not divisible the only irreducible quadratic over $\mathbb{F}_2[x]$, $x^2 + x + 1$. □

**Problem 14.4.1** Determine the Galois closure of the field $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ over $\mathbb{Q}$.

*Proof.* The Galois closure is simply the splitting field for the minimal polynomial of $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$. We see that the minimal polynomial is just $p(x) = (x^2-1)^2 - 2 = x^4 - 2x^2 - 1$, which has roots,

$$\alpha = \pm i\sqrt{-1+\sqrt{2}} \qquad\qquad \alpha = \pm\sqrt{1+\sqrt{2}}$$

the splitting field is therefore $\mathbb{Q}(i, \sqrt{1+\sqrt{2}})$, which is then the Galois closure. □

**Problem 14.4.2** Find a primitive generator for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$.

*Proof.* A member of the extension is $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$ so we have that $\mathbb{Q}(\alpha)$ is a subset of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. We note that $\alpha$ is not fixed by any of the nontrivial Galois automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ so $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is also a subset of $\mathbb{Q}(\alpha)$. Together we have containment in both directions so, $\alpha$ is a primitive generator of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. □

**Problem 14.4.6** Prove that $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$ is not a simple extension by explicitly exhibiting an infinite number of intermediate subfields.

*Proof.* We see that $x$ is a root of $A^p - x^p$ in $\mathbb{F}_p(x^p, y^p)[A]$ which is a polynomial of degree $p$ in $A$. We have a similar property for $y$ in that it is a root of $A^p - y^p$ in $\mathbb{F}_p(x^p, y^p)[A]$. As indeterminants we have $\mathbb{F}_p(x) \cap \mathbb{F}_p(y) = \mathbb{F}_p$, and therefore $[\mathbb{F}_p(x, y) : \mathbb{F}_p(x^p, y^p)] = p^2$.

Now our goal from here is to show that for every $\delta \in \mathbb{F}_(x^p)$, we have the fields $\mathbb{F}_p(x^p, y^p)(x + \delta y) = \mathbb{F}(x^p, y^p, x + \delta y)$ to be distinct. Now take $\delta$, $\gamma$ from $\mathbb{F}_p(x^p)$ where $\delta \neq \gamma$, and suppose $\mathbb{F}(x^p, y^p, x + \delta y) = \mathbb{F}(x^p, y^p, x + \gamma y)$. We have then that

$$(x + \delta y) - (x + \gamma y) = (\delta - \gamma)y$$

to be in $\mathbb{F}(x^p, y^p, x + \delta y)$, which implies then that both $x$ and $y$ are in our extension. Meaning that $\mathbb{F}_p(x, y) = \mathbb{F}_p(x^p, y^p, x + \delta y)$ is an extension with degree $p^2$ over $\mathbb{F}_p(x^p, y^p)$. Note though that $(x + \delta y)^p = x^p + \delta^p y^p$ (Prop 35 from 13.5), which comes as the solution of $x^p - (x^p + \delta^p y^p)$ which is of degree $p$. This is a contradiction though since we just stated that this is degree $p^2$. All together then, since there is an infinite amount of elements in $\mathbb{F}_p(x^p)$ there is an infinite number of subfields of $\mathbb{F}_p(x, y)$. □