Some Galois Theorem.

We first want to understand when polynomials have repeated roots. If

$$f(x) = \sum_{j=0}^{n} a_j x^j$$

is a polynomial over the fields $\mathbb{F}$, then its ***formal derivative*** (which from now on we will just call the ***derivative***) is just what you expect:

$$f'(x) = \sum_{j=0}^{n} j a_j x^{j-1}.$$

Then the most of the usual rules of calculus hold (i.e. sum rule, product rule, chain rule) and if you have never checked these it is a good idea to do it now. One difference from the usual derivative is that $f'(x) = 0$ does not imply $f(x)$ is constant, at least over fields of prime characteristic. For example if $\mathbb{F} = \mathbb{Z}/\langle p \rangle$ is field with p elements, and

$$f(x) = x^p + 1$$

then $f'(x) = 0$ in $\mathbb{F}[x]$, but $f(x)$ is not a constant in $\mathbb{F}[x]$.

Proposition 1. *Show that if $\mathbb{F}$ is a field of prime characteristic, p, and $f(x) \in \mathbb{F}[x]$ then $f'(x) = 0$ if and only if $f(x) = g(x^p)$ for some polynomial $g(x) \in \mathbb{F}[x]$.*

Problem 1. Prove this. □

Proposition 2. *Let $f \in \mathbb{F}[x]$. Then $f(x)$ has no repeated root in an extension field of $\mathbb{F}$ if and only if $f(x)$ and $f'(x)$ are relatively prime in $\mathbb{F}[x]$.*

Definition 3. Let $\mathbb{F}$ be a field of characteristic $p > 0$. Then the ***Frobenius endomorphism*** is the map $\phi\colon \mathbb{F} \to \mathbb{F}$ give by $\phi(a) = a^p$. □

Proposition 4. *The Frobenius endomorphism injective ring homomorphism $\phi\mathbb{F} \to \mathbb{F}$. Its powers are given by*

$$\phi^k(a) = a^{p^k}.$$

Problem 2. Prove this. □

Proposition 5. *Let $q = p^k$ be a power of a prime and let $\mathbb{F}_q$ be the splitting field of $f_q(x) = x^q - x$ over the field $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle$. Then $\mathbb{F}_q$ has q elements are they are exactly the roots of $f_q(x)$.*

Problem 3. Prove this. *Hint:* There are many many ways to do this. Here is an outline of one way. Let $R \subseteq \mathbb{F}_q$ be the set of roots of f_q. Show that R is closed under sums and products. (One way to do this is to not that a is a root of $f_q(x)$ if and only if $\phi^k(a) = a$ for the Frobenius endomorphism.) Thus R is a subfield of $\mathbb{F}_q$. And as $\mathbb{F}_q$ is the smallest field containing the roots of $f_q(x)$, it follows that $\mathbb{F}_q = R$ and therefore every element of $\mathbb{F}_q$ is a

root of $f_q(x)$. Note $f_q'(x) = -1$ and therefore $f_q(x)$ and $f_q'(x)$ are relatively prime, which implies the roots of $f_q(x)$ are distinct. Use this to conclude $|\mathbb{F}_q| = \deg(f_q(x)) = q$. □

Since splitting fields are unique up to isomorphism, this implies the field of order q is unique up to isomorphism. Also since every polynomial has a splitting field, we see by looking at the splitting field of $f_q(x)$ over $\mathbb{F}_p$ that there exists a field of order $q = P^k$ for every power of a prime.

Theorem 6. *Let $\mathbb{F}_q$ be the field of order $q = p^k$ and $\phi\colon \mathbb{F}_q \to \mathbb{F}_q$ the Frobenius endomorphism. Then the Galois group $\mathrm{Gal}(F_q/\mathbb{F}_p)$ is the cyclic group generalised by ϕ. This group has order k.*

Problem 4. Prove this. □

More generally:

Theorem 7. *Let $q = p^k$ and $r = q^\ell = p^{k\ell}$. Then $\mathrm{Gal}(\mathbb{F}_r/\mathbb{F}_q)$ is the cyclic generated by ϕ^k.* □

Problem 5. Prove this. □

A problem that came up in class was when a Galois group splits as a direct product. Here one criteria for this.

Proposition 8. *Let $f_1(x), f_2(x) \in \mathbb{Q}[x]$ have positive degree and let $\mathbb{F}_j$ be the splitting field of $f_j(x)$. Assume*

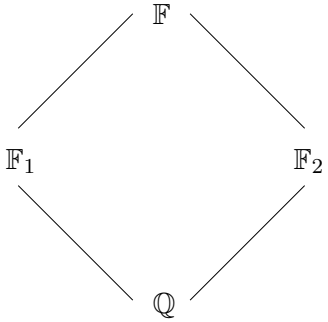
$$\mathbb{F}_1 \cap \mathbb{F}_2 = \mathbb{Q}.$$

Then the Galois group of the product $f(x) = f_1(x)f_2(x)$ is isomorphic to the product of the Galois groups of $f_1(x)$ and $f_2(x)$.

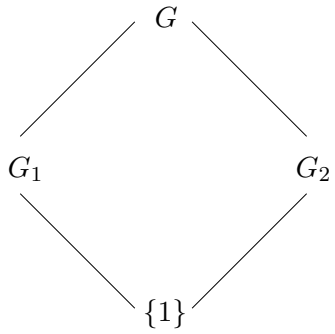
Proof. Consider the field

$$\mathbb{F}_1\mathbb{F}_2 = \text{Span over } \mathbb{Q} \text{ of } \{\alpha\beta : \alpha \in \mathbb{F}_1, \beta \in \mathbb{F}_2\}.$$

This is well known to be the smallest field containing $\mathbb{F}_1$ and $\mathbb{F}_2$ and $\mathbb{F}_1 \cap \mathbb{F}_2 = \mathbb{Q}$ implies $[\mathbb{F} : \mathbb{Q}] = [\mathbb{F}_1, \mathbb{Q}][\mathbb{F}_2, \mathbb{Q}]$. As the splitting field of $f(x)$ most contain both $\mathbb{F}_1$ and $\mathbb{F}_2$ we have $\mathbb{F} \supseteq \mathbb{F}_1\mathbb{F}_2$. But $\mathbb{F}_1\mathbb{F}_2$ contains all the roots of $f(x)$ and therefore $\mathbb{F} \subseteq \mathbb{F}_1\mathbb{F}_2$ and therefore $\mathbb{F} = \mathbb{F}_1\mathbb{F}_2$. This leads to the following lattice of fields:



Therefore if G is the Galois group of $\mathbb{F}$ and G_j is the Galois group of $\mathbb{F}$ this gives the following lattice of groups:



Now to the punchline. The field extensions $\mathbb{F}_1/\mathbb{Q}$ and $\mathbb{F}_2/\mathbb{Q}$ are splitting fields of polynomials and therefore are normal extensions. Therefore G_1 and G_2 are normal subgroups of G be the Galois correspondence. We therefore have $G = G_1G_2$ and $G_1 \cap G_2 = \{1\}$ with G_1 and G_2. It is now a standard group theory exercise (which we have done) to show that $G \approx G_1 \times G_2$. □

Problem 6. Let $f(x) = (x^2 - 2)(x^2 - 3)$. Use Proposition 8 to show the Galois of this polynomial over $\mathbb{Q}$ is $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

Problem 7. For an example that came a few years ago let $f(x) = (x^2 - 2)(x^2-3)(x^2-5)$ we can proceed in steps. First show that $\mathbb{Q}(\sqrt{2})\cap\mathbb{Q}(\sqrt{3}) = \mathbb{Q}$ and then $\mathbb{Q}(\sqrt{2},\sqrt{3})\cap\mathbb{Q}(\sqrt{5}) = \mathbb{Q}$ (and this is the messy step, but so far I don't see a way to avoid it). Then then have (using rather sloppy notation)

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})) &\approx \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{5})) \\ &\approx \mathrm{Gal}(\mathbb{Q}(\sqrt{2})) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{3})) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{5})) \\ &\approx \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.\end{aligned}$$

□