M 622 Notes, HW: Voluntary. We'll go over it in class.

Suppose F is a field, and $p(x) \in F[x]$. Recall that an extension K of F

- is said to **split** $p(x)$ if $p(x)$ can be written as a product of linear polynomials in $K[x]$, and
- a field extension S of F is said to be a **splitting field** of $p(x)$ over F if S splits $p(x)$ and no proper subfield T containing F splits $p(x)$.

Given $p(x) \in F[x]$, there is a very straightforward procedure that can be used to construct a splitting field S of $p(x)$:

- Factor $p(x)$ into a product of irreducibles of $F[x]$, say $p(x) = a(x)b(x)\dots z(x)$.
- Form a root of $p(x)$ in an extension field of F, say, F_1. For example, we've shown that $F_1 = F[x]/(a(x))$ has a root of $a(x)$, say, r_1. We also know F_1 is a field since $a(x) \in F[x]$ is irreducible. Needless to say, course r_1 is a root of $p(x)$.
- Continuing, now factor $p(x)$ in $F_1[x]$ as a product $p(x) = (x - r_1)q(x)$, where $q(x) \in F_1[x]$. Of course, $deg(q(x)) = deg(p(x)) - 1$. Factor $q(x)$ into F_1-irreducibles, and repeat the above procedure, adding a root of $q(x)$, say, r_2, in an extension field F_2 of F_1.
- Continue until $p(x)$ is factored as a product of linear polynomials. This procedure terminates in a finite number of steps since $deg(p(x)) = n$ is a finite positive

integer: We have constructed a field in which $p(x)$ can be factored into a product of linear polynomials has been constructed. Let's denote that field S. Note that $S = F(r_1, \dots, r_s)$, where $\{r_1, \dots, r_s\}$ are the roots of $p(x)$ that we found (or constructed).

- If T is any proper subfield of S, then **at least one** of $\{r_1, \dots, r_s\}$ is not in T —this is because S is generated by F and $\{r_1, \dots, r_s\}$. Thus, S is a **splitting field** of $p(x)$ over F.
  - In many instances, less "constructing" is required. One might know (or be able to easily find) the roots $\{r_1, \dots, r_s\}$ of $p(x)$, in which case one can form the splitting field $S = F(r_1, \dots, r_s)$ more directly:
    For example, we formed a splitting field for $p(x) = x^3 - 2 \in \mathbb{Q}$ quite easily: $S = \mathbb{Q}(2^{1/3}, 2^{1/3}\omega, 2^{1/2}\omega^2)$, where $\omega = e^{2\pi i/3}$, a **third root of unity**.
  - But if we have a field F and a polynomial $p(x)$, and we don't have a natural larger field J in which the roots of a polynomial are well known, then we might have to do the root-formation trick repeatedly in order to form a splitting field of $p(x)$. A simple example: As you can verify $x^2+x+1 \in \mathbb{Z}_2[x]$ is irreducible $\mathbb{Z}_2$. We'd like to form a splitting field for x^2+x+1 over $\mathbb{Z}_2$. We can adjoin a root of $p(x)$ in a larger field $F_1 = \mathbb{Z}_2[x]/(x^2+x+1)$. Indeed, $\theta = x + (x^2+x+1)$ is a root of $p(x)$ in F_1. We can now split $x^2+x+1 = p(x)$ in F_1—the other root of $p(x)$ is contained in F_1 and can be found by "long division".

Exercise 0. (A.) Find θ^{-1} in F_1. (B.) Then find $q(x) \in F_1[x]$ such that $(x-\theta)q(x) = x^2+x+1$. (C.) Find the other root of x^2+x+1 in F_1. We'll come back to this little example.

In class, we observed that if $p(x) \in F[x]$ is irreducible over F with degree $n > 1$, then $\mathbb{F}[x]/(p(x))$ is a field, and that $[\mathbb{F}[x]/(p(x)) : F] = n$. Moreover, if K is an extension of F and K contains a root r of $p(x)$, then (*) $F[r] = F(r) \cong F[x]/(p(x))$, so $[F(r) : F] = n$ (where $F(r)$ is the least subfield of K containing F and r).

Exercise 1. With p, F, r as in the paragraph above, show that $\{1, r, \ldots, r^{n-1}\}$ is a basis for $F(r)$ over F.

Returning to the splitting field $S = \mathbb{Q}(2^{1/3}, \omega)$ of $x^3 - 2$ over $\mathbb{Q}$, from (*) we have that $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$, and from Exercise 1, we know that $\{1, 2^{1/3}, 2^{2/3}\}$ is a basis for $\mathbb{Q}(2^{1/3})$ over $\mathbb{Q}$. Thus every element of $\mathbb{Q}(2^{1/3})$ is a sum of three real numbers, from we can conclude that $\mathbb{Q}(2^{1/3})$ is contained in $\mathbb{R}$.

It's worth mentioning that $[\mathbb{Q}(2^{1/3}\omega : \mathbb{Q}] = 3 = [\mathbb{Q}(2^{1/3}\omega^2) : \mathbb{Q}]$—that's because both $2^{1/3}\omega$ and $2^{1/3}\omega^2$ are both roots of the degree-three irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$.

Of course $\omega \notin \mathbb{Q}(2^{1/3})$. Observe that $\omega^3 = 1$, and ω is a root of $x^2 + x + 1 \in \mathbb{Q}$.

Exercise 2. Explain why $x^2 + x + 1 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$. What is $[\mathbb{Q}(\omega) : \mathbb{Q}]$? Can you use the Double Extension Lemma to determine $[S : \mathbb{Q}]$, where $S = \mathbb{Q}(2^{1/3}, \omega)$, the splitting field of $x^3 - 2$ over $\mathbb{Q}$?

Terminology.

- If L is an extension of a field F, and K is a subfield of L that contains F, then K is said to be an **in-between field**—the context should be clear in the discussion.
- If K_1, K_2 are between fields $F \leq K_1, K_2 \leq L$, then the least subfield of L containing K_1 and K_2 is denoted K_1K_2.

Further terminology: If K is a field extension of F, then $Aut_F(K) = \{\alpha \in Aut(K) : \forall b \in F \quad \alpha(b) = b\}$. (Later we'll see that under certain circumstances, $Aut_F(K)$ is the so-called *Galois group of* K over F).

Ambitious goals: Describing all between-fields J ($\mathbb{Q} \leq$

$J \le S$) and showing that $Aut_{\mathbb{Q}}(S) \cong S_3$, where S is the splitting field of $x^3 - 2$ over $\mathbb{Q}$, the extension field we've been investigating.

Let's prove a little lemma (as an exercise), and prove another more important lemma (as another exercise).

Exercise 3. Suppose p is a prime, K is an extension of F, and $[K : F] = p$. Prove that if $c \in K - F$, then $F(c) = K$. Suggestion: Use the Double-Extension Lemma.

Exercise 4. *The Roots-to-Roots Lemma*: Suppose $f(x)$ is a polynomial in $F[x]$ having a root r in some extension K of F. Let $H = Aut_F(K) = \{\beta \in Aut(K) : \forall\ b \in F\ \beta(b) = b\}$. Prove that if $\beta \in H$, then $\beta(r)$ is also a root of $f(x)$.

One consequence of the Roots-to-Roots Lemma is this: In the language of the Roots-to-Roots Lemma, the group $H = Aut_F(K)$ **acts** on the roots of $p(x) \in F[x]$. Thus, there is a mapping of H to S_n, where n is $deg(p(x))$.

Exercise 5. *Faithful Action Lemma*: Suppose $p(x)$ is a polynomial in $F[x]$, and S is a splitting field of $p(x)$ over F. Then $H = Aut_F(S)$ acts faithfully on the roots of $p(x)$. (In particular, H can be embedded in S_n, where $n = deg(p(x))$.) **Proof.** Since $S = F(r_1, \ldots, r_k)$, where $\{r_1, \ldots, r_k\}$ are the distinct roots of $p(x)$ (and all are contained in S), if $\alpha \in H$ and α fixes pointwise each r_i, $i = 1, \ldots, n$, then since α fixes F pointwise, and every element in S is a polynomial in $F[r_1, \ldots, r_k]$, it follows that α fixes every element of S. $\square$

We'll continue!