1/13

Spring 2025, Howard Math 211

Modern Algebra II (2nd semester graduate algebra)

Instructor: Sam Hopkins, sam.hopkins@howard.edu

Website: samuelfhopkins.com/classes/211.html

Class info:

- Meets MW 11:10am-12:30pm in Annex III - #224
- Office Hrs: T 12-1pm - Annex III - #220
  or by appointment - email me!
- Text: Hungerford "Algebra"
  (email me if you need a copy!)
- Grading: 50% 5 Homeworks
  25% 1 Midterm Exam
  25% Final Project

Collaboration on Hws is encouraged, not on other assessments.
The midterm will be before spring break.
The final project will involve independent research and a presentation, at the end of the semester.
Other than that I expect you to show up to class and participate! :)

What is this class about?

This class is a continuation of the 1st semester of modern algebra, where we learned about groups, rings, and modules. To start the 2nd semester we will study the theory of fields and their extensions. This is also called "Galois theory".

We say L is an extension of K, for K, L fields, if $K \subseteq L$, i.e., K is a subfield of L.

If $K \subseteq L$ is an extension of fields, then the Galois group $\mathrm{Gal}_K(L)$ of L/K is the collection of automorphisms of L that fix K. Under favorable circumstances, the Galois group determines a lot about the structure of the field extension: for example, the subgroup structure of $\mathrm{Gal}_K(L)$ is the same as the "subextension" structure of L/K.

We see how this topic beautifully combines the two major algebraic structures from the 1st semester:

- rings (in the specific case of fields & extensions)
- groups (Galois groups).

Also, we will see connections to very classical topics in mathematics, including:

- the impossibility of certain compass & straightedge constructions,
- the irrationality / transcendence of constants like π and e.

In fact, Galois theory was originally developed in order to understand a very classical problem:

- the "unsolvability" of the quintic equation.

We will of course discuss these connections...

After we finish with Galois / field theory, depending on time we may discuss further topics in algebra, including:

- representation theory of finite groups,
- basic commutative algebra,
- basic algebraic number theory.

The final project at the end of the semester will involve independent research, and a presentation on one of these more advanced topics.

//

Field Extensions § 5.1 of Hungerford

Def'n A field L is an extension of a field K if $K \subseteq L$.
(We often use L/K as a shorthand for an extension.)

Rmk: Recall that a field is a commutative ring in which every nonzero element is a unit, i.e. multiplicatively invertible. In particular, it is an integral domain (no nonzero zero-divisors).

Because every map $\varphi: K \to L$ between fields is an injection, we can equivalently think of a field extension as a pair of fields K, L with a map $\varphi: K \to L$, i.e. in the language we learned at the end of last semester, L is an algebra over K.

In particular, L is a vector space over K, and hence there is some dimension $\dim_K L$ of L over K, the cardinality of any K-basis of L. This dimension is called the degree of the extension L/K and is denoted $[L:K]$. If $[L:K] < \infty$ we say L/K is a finite extension, otherwise we say it is an infinite extension.

E.g. $\mathbb{C}$ is a finite extension of $\mathbb{R}$: a basis of $\mathbb{C}$ over $\mathbb{R}$ is $\{1, i\}$ so $[\mathbb{C}:\mathbb{R}] = 2$.

E.g. Recall that for a field K, $K[x]$ is the ring of polynomials (in formal variable "x") with coefficients in K, and $K(x) = \{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], g(x) \neq 0 \}$ is the field of rational functions over K (= field of fractions of $K[x]$).

$K(x)$ is an infinite extension of K: for example, all of $\{1, x, x^2, x^3, \ldots\}$ are linearly independent.

Rmk: $\{1, x, x^2, x^3, \ldots\}$ is a K-basis of $K[x]$, but not $K(x)$: e.g., also need $x^{-1}, x^{-2}, \ldots, (1+x)^{-1}, \frac{x}{1+x}$, etc. Exercise: write a basis of $K(x)$ over K.

1/15

Just like how in the 1^{st} semester, we mostly stuck to "finite" situations, we will mostly consider finite extensions. First let's note a basic fact about degrees:

<u>Prop:</u> If L/K and M/L are two extensions, then $[M:K] = [M:L][L:K]$.

<u>Pf:</u> We basically proved this last semester when we talked about modules. The idea is that if $\{x_1, \dots, x_\ell\}$ is a K-basis of L and $\{y_1, \dots, y_m\}$ is an L-basis of M, then $\{x_i \cdot y_j : 1 \le i \le \ell, 1 \le j \le m\}$ is a K-basis of M. ☒

We'll see later that this basic multiplicativity of degrees <u>already</u> has interesting consequences. But first...

Even though $K[x]$ and $K(x)$ are ∞-dim'l over K, they are key to understanding extensions over K, including finite dimensional ones.

<u>Def'n</u> Let L/K be an extension and $u \in L$. We say that u is <u>algebraic</u> over K if $f(u) = 0$ for some nonzero $f(x) \in K[x]$, i.e., u is a <u>root</u> of some polynomial with coefficients in K. Otherwise say u is <u>transcendental</u> over K.

<u>E.g.</u> $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since it is a root of the polynomial $x^2 - 2$.

<u>E.g.</u> It is a very nontrivial fact (we may discuss the proofs later) that π and e are transcendental over $\mathbb{Q}$.

Def'n Let L/K be an extension and $u_1, \dots, u_n \in L$.
We use $K[u_1, \dots, u_n]$ to denote the subring of L generated by K and $u_1, \dots, u_n$, and $K(u_1, \dots, u_n)$ to denote the subfield of L generated by K and $u_1, \dots, u_n$.

Rmk: Easy to check $K[u_1, \dots, u_n] = \{ f(u_1, \dots, u_n) : f(x_1, \dots, x_n) \in K[x_1, \dots, x_n] \}$ and $K(u_1, \dots, u_n) = \{ \frac{f(u_1, \dots, u_n)}{g(u_1, \dots, u_n)} : f, g \in K[x_1, \dots, x_n],\ g \neq 0 \}$.

Most important cases are when $n=1$: $K[u]$ and $K(u)$.
We say the extension L/K is simple if $L = K(u)$ for some $u \in K$.
Think: generated by a single element, like a cyclic group/module.

For a simple extension $K(u)$ there are two possibilities: u is transcendental over K, or u is algebraic over K.

Thm Let $L = K(u)$ be a simple extension with u transcendental over K. Then $L \simeq K(x)$, field of rational functions.

Pf: The isomorphism $K(x) \simeq K(u)$ is given by $x \mapsto u$.
The fact that u is not a root of any polynomial implies this is an iso.

Thm Let $L = K(u)$ be a simple ext. with u algebraic over K.
Then:
1) $K(u) = K[u]$
2) there is a unique polynomial $f(x) \in K[x]$, such that $f(u) = 0$, f is monic (leading coeff $= 1$) and f has minimal degree with these properties (f is called the minimal polynomial of u)
3) $[K(u) : K] = n < \infty$ where n is the degree of the minimal polynomial f of u, in particular a basis is given by $\{1, u, u^2, \dots, u^{n-1}\}$
4) $L = K(u) \simeq K[x]/(f)$, where again f is the min. poly. of u.

1/22

Pf: We start by showing $K[u] \simeq K[x]/(f)$ for some irreducible monic polynomial $f(x) \in K[x]$, which will be the min. poly.
Note that there is a surjection $\varphi: K[x] \to K[u]$ of K-algebras determined by $\varphi(x) = u$. What is $\mathrm{Ker}(\varphi)$?
Since u is algebraic, $f(u) = 0$ for some $f(x) \neq 0 \in K[x]$, so $\mathrm{Ker}(\varphi) \neq 0$. But recall that $K[x]$ is a PID, so $\mathrm{Ker}(\varphi)$, an ideal of $K[x]$, must be generated by a single $f \in K[x]$; i.e. $\mathrm{Ker}(\varphi) = (f)$. Suppose this f were reducible: $f = g \cdot h$ for some g, h of strictly lower degree. Then since u is a root of f, it would have to be a root of either g or h, but then $\mathrm{Ker}(\varphi)$ would have to include g or h, i.e., would be strictly bigger than (f).
So indeed f is reducible; and then f is uniquely determined by the requirement that it is monic (we can multiply by inverse of leading coeff. if it's not monic).

Notice that if $g(u) = 0$ for any $g \in K[x]$, then $g \in (f)$, i.e. f divides g, which means that indeed f is the minimal polynomial of u.
Since f is irreducible, and $K[x]$ is a PID, (f) is a maximal ideal, which means that $K[x]/(f)$ is a field. So $K[u]$ is a field! But $K[u] \subseteq K(u)$ which is the smallest field containing K and u, so $K(u) = K[u]$.
This proves 1), 2), and 4). For 3): it's easy to see that $\{1, x, x^2, \dots, x^{n-1}\}$ is a K-basis of $K[x]/(f)$ if f has degree n (by polynomial long division), so indeed $\{1, u, u^2, \dots, u^{n-1}\}$ is a K-basis of $K(u)$.

E.g.: $\sqrt{2}$ is algebraic over $\mathbb{Q}$ and its minimal polynomial is x^2-2, which has degree 2. So $\{1, \sqrt{2}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$: i.e. the elements of $\mathbb{Q}(\sqrt{2})$ are of the form $a+b\sqrt{2}$ for $a, b \in \mathbb{Q}$. Let's see how the field operations look in this basis:

- $(a+b\sqrt{2})\cdot(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}$
- $(a+b\sqrt{2})^{-1} = \frac{1}{a^2-2b^2}(a-b\sqrt{2})$ since

$$(a+b\sqrt{2})\cdot\frac{1}{a^2-2b^2}(a-b\sqrt{2}) = 1. \checkmark$$

Q: why is $a^2-2b^2 \neq 0$?

E.g. Let's do a more complicated, degree 3 example.
$f(x) = x^3-3x-1$ is irreducible over $\mathbb{Q}$ (exercise for you) and it has a unique positive real root, call it u.
Thus $\mathbb{Q}(u)$ is a degree 3 extension of $\mathbb{Q}$, and in fact $\mathbb{Q}(u) = \{au^2+bu+c : a, b, c \in \mathbb{Q}\}$.
But how do we concretely work in this field.
For example, $u^4+2u^3+3 \in \mathbb{Q}(u)$ is an element, but how to express it in terms of our basis?
Using polynomial division: $x^4+2x^3+3 = (x+2)(x^3-3x-1) + (3x^2+7x+5)$
So $u^4+2u^3+3 = (u+2)\underbrace{\cancel{(u^3-3u-1)}}_{0} + (3u^2+7u+5) = 3u^2+7u+5$.
How about finding $(3u^2+7u+5)^{-1}$? To do this, let $g(x), h(x)$ be such that $(x^3-3x-1)g(x) + (3x^2+7x+5)h(x) = 1$.
Then $h(u) = (3u^2+7u+5)^{-1}$ since (u^3-3u-1). How to find these $g(x), h(x)$? Euclidean algorithm for GCD!:

$$x^3-3x-1 = \left(\frac{x}{3}-\frac{7}{9}\right)(3x^2+7x+5) + \left(\frac{7x}{9}+\frac{26}{9}\right)$$

$$3x^2+7x+5 = \left(\frac{27x}{7}-\frac{261}{49}\right)\left(\frac{7x}{9}+\frac{26}{9}\right) + \frac{999}{49}$$

$\Rightarrow g(x) = -7/37\, x + 29/111$ and $h(x) = 7/111\, x^2 - 26/111\, x + 28/111$.

$\Rightarrow (3u^2+7u+5)^{-1} = \frac{7}{111}u^2 - \frac{26}{111}u + \frac{28}{111}$. //

Def'n Let L/K be an extension. We say it is an algebraic extension if every $u \in L$ is algebraic over K, otherwise we say it is a transcendental extension.

Cor If L/K is a transcendental extension, then it is an infinite extension.

Pf: Let $u \in L$ be transcendental. Then $K(u) \cong K(x)$ is an infinite extension of K, and since L is an extension of $K(u)$, L must also be an infinite extension of K. $\boxtimes$

Cor Let L/K be an extension. Then it is a finite extension if and only if it is finitely generated and algebraic.

Pf: First we prove the $\Leftarrow$ direction: so let L/K be finitely generated and algebraic, i.e. $L = K(u_1, \dots, u_n)$ with u_i all algebraic. By induction on n, $[K(u_1, \dots, u_{n-1}) : K] < \infty$, and by our study of simple extensions $[K(u_1, \dots, u_{n-1}, u_n) : K(u_1, \dots, u_{n-1})] = m < \infty$ where m is the degree of the min. poly. of m. Then by the multiplicativity of degree, we are done.
The $\Rightarrow$ direction: If L/K is not algebraic, then by previous corollary it is infinite. Similarly, if it is not finitely generated, it must also be infinite. $\boxtimes$

Rmk: An algebraic (but not finitely generated!) extension like $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \dots \sqrt{d}$ for d square-free$)$ is not a finite extension!

From now on we will study algebraic extensions, especially finite extensions, which have a nice theory.

1/27

Appendix (of § 5.1): Straightedge & compass constructions

Compass and straightedge constructions have been studied at least since the ancient greeks. The idea is that we have as tools a straightedge (ruler) which lets us draw straight lines connecting points, and a compass which lets us draw circles through points. The point is to construct (draw) figures in the plane, or more precisely to understand which figures can be constructed. It turns out that the theory of fields and their extensions leads to a very satisfactory understanding of these!

If K is a subfield of $\mathbb{R}$, the plane of F is the set of all points (x,y) with $x,y\in K$, and a line in F is a line connecting two points P, Q in the plane of F, while a circle in F is the circle whose center is at such a P, containing such a Q.

Lemma Let K be a subfield of R.

i) For two lines L_1, L_2 in K, $L_1 \cap L_2$ is a point in the plane of K or $= \emptyset$.

ii) For a line L_1 in K and a circle C_1 in F, $L_1 \cap C_1 = \emptyset$ or is two points in $K(\sqrt{u})$ for some $u \in K$.

iii) For two circles C_1, C_2 in K, $C_1 \cap C_2 = \emptyset$ or consists of two points in $K(\sqrt{u})$ for some $u \in K$.

Pf: i): Exercise iii): Show that $C_1 \cap C_2$, if nonempty, is the same as $C_1 \cap L_1$ for some line L_1 in K. So reduce to ii).

ii) Write L_1 as $dx + ey + f = 0$ with $d,e,f \in K$ and C_1 as $x^2 + y^2 + ax + by + c = 0$ w/ $a,b,c \in K$. Assume $d \neq 0$ (easy excercise otherwise), so $x = \frac{1}{d}(-ey - f)$. Substitute this into the equation for C_1 to get $Ay^2 + By + C = 0$ for some $A,B,C \in K$. If $A \neq 0$ then divide through to get $y^2 + B'y + C' = 0$, and complete the square to get $(y + B'/2)^2 + (C' - B'^2/4) = 0$. Then either $L_1 \cap C_1 = \emptyset$ or the intersection is two points (x,y) with $x,y \in K(\sqrt{u})$ where $u = -C' + B'^2/4 \geq 0$. ∎

We say a number $c \in \mathbb{R}$ is constructible if the point $(c,0)$ can be constructed in a finite number of steps starting from the integer grid $\mathbb{Z}^2 \subseteq \mathbb{R}^2$ and adding points at the intersections of lines and circles thru points you've constructed so far.
Can show (see HW) that: i) every rational number is constructible,
ii) if $c \geq 0$ is constructible then so is $\sqrt{c}$,
iii) if c,d are constructible then $c \pm d$, cd, and c/d $(d \neq 0)$ are too.
So constructible numbers are a field extension of $\mathbb{Q}$.

Corollary If a real number c is constructible, then c is algebraic of degree a power of 2 over $\mathbb{Q}$.

Pf: Easy consequence of previous numbers.

This lets us prove some things cannot be constructed!
For example, we can construct an angle of $60°$ because we can draw an equilateral triangle (exercise), but...

Prop. It is impossible to trisect angle of $60°$ with compass & straightedge.

Pf: If we could, we'd be able to make a right triangle with one angle $20°$, and hence the number $\cos(20°)$ would be constructible.
However, trigonometry says that

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$$

and plugging in $\alpha = 20°$ says that $\cos(20°)$ is a root of $1/2 = 4x^3 - 3x$, i.e. of $8x^3 - 6x - 1$ which is irreducible over $\mathbb{Q}$ (exercise). Hence $\cos(20°)$ has degree 3 over $\mathbb{Q}$, contradicting previous corollary! ∎

One can similarly show that "doubling the cube" and "squaring the circle" are impossible (need that π is transcendental) with straightedge and compass.
However... Origami can let us solve cubic equations and thus construct more points than compass & straightedge.

The Fundamental Theorem of Galois Theory §5.2

So far we have seen how questions about polynomials, especially irreducibility and their roots, are fundamental to understanding extensions of some base field. The next step is to introduce the group of automorphisms of one field over another. Studying this group is the main idea of Galois theory.

Def'n Let L/K be a field extension. We say that a field automorphism $\sigma: L \to L$ is a K-automorphism if $\sigma(k)=k$ for all $k \in K$, i.e., σ fixes all elements of K. (This is equivalent to σ being a K-module homomorphism.) The group of all K-automorphisms of L is called the Galois group of L over K, denoted $\mathrm{Aut}_K(L)$ (or $\mathrm{Gal}_K(L)$).

Why the requirement that the automorphisms fix K? Consider:

Theorem Let L/K and $f(x) \in K[x]$. If $u \in L$ is a root of f, and $\sigma \in \mathrm{Aut}_K(L)$, then $\sigma(u)$ is also a root of f.

Pf: Write $f(x) = \sum_{i=0}^{n} k_i x^i$. Then since $f(u)=0$ we have

$$f(\sigma(u)) = \sum_{i=0}^{n} k_i \sigma(u)^i = \sum_{i=0}^{n} \sigma(k_i)\sigma(u)^i = \sigma\Big(\sum_{i=0}^{n} k_i u^i\Big) = \sigma(f(u)) = 0,$$

where we used $k_i = \sigma(k_i)$ since $k_i \in K$. $\boxtimes$

Consider the case where $L = K(u)$ for some u that is algebraic of degree n over K. Then, since a K-basis of L is $\{1, u, u^2, \ldots, u^{n-1}\}$, any $\sigma \in \mathrm{Aut}_K(L)$ is determined by where it sends u, and by the previous theorem it must send u to another root of the minimal polynomial f of u, so in particular we have in this case that $|\mathrm{Aut}_K(L)| \le n$ (# of choices of where to send u), and we can often work out $\mathrm{Aut}_K(L)$ explicitly...

1/29

E.g. Consider $\mathbb{C}/\mathbb{R}$. Since $\mathbb{C} = \mathbb{R}(i)$, and i has minimal polynomial x^2+1, we know that any $\sigma \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ is determined by where σ sends i, which must be to either i itself or the other root of x^2+1, which is $-i$. So $|\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})| = 2$, in particular $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{1, \sigma\}$ where 1 is the identity automorphism and $\sigma(a+bi) = a-bi$ is complex conjugation. Notice $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) \cong \mathbb{Z}/2\mathbb{Z}$ as a group!

E.g. Consider $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. The minimal poly. of $\sqrt{2}$ is x^2-2, it has another root $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and $\sigma(a+b\sqrt{2}) = a-b\sqrt{2}$ is a nonidentity automorphism, so again $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}/2\mathbb{Z}$.

E.g. With $L = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, the situation is different. Here the min. poly. of $\sqrt[3]{2}$ is x^3-2, whose other two roots are not real, in particular are not in L. So the only element of $\mathrm{Aut}_{\mathbb{Q}}(L)$ is the identity, even though L is a nontrivial extension.

The previous example leads to the following definition.

Def'n We say L/K is a Galois extension if $\{u \in L : \sigma(u) = u \text{ for all } \sigma \in \mathrm{Aut}_K(L)\} = K$, i.e., the subfield of L fixed by all elements of $\mathrm{Aut}_K(L)$ is K itself.

The reason for this definition is the following:

Theorem (Fundamental Theorem of Galois Theory)
If L/K is a finite Galois extension, then there is a one-to-one correspondence between sub-extensions of L (i.e., intermediary subfields of L containing K), and subgroups of the Galois group $\mathrm{Aut}_K(L)$.

...

In fact we can be a little more precise about how this correspondence goes..

<u>Def'n</u> Let L/K be an extension and $G = \mathrm{Aut}_K(L)$ its Galois group. For a subgroup $H \subseteq G$ we define its <u>fixed field</u> to be $H' = \{u \in L : \sigma(u) = u \ \forall \sigma \in H\}$, a subfield of L. (So L/K is Galois if $G' = K$.) Similarly, for F an intermediary field $K \subseteq F \subseteq L$ we define $F' = \{g \in G : g(u) = u \text{ for all } u \in F\}$, a subgroup of G.

<u>Theorem</u> (Fund. Thm. of Galois Theory) If L/K is a finite Galois extension, then there's a 1-to-1 correspondence between sub-extensions $K \subseteq F \subseteq L$ and subgroups $H \subseteq \mathrm{Aut}_K(L)$ given by $F \mapsto F'$ (with inverse $H \mapsto H'$).

Notice that this correspondence is "<u>order</u>-<u>reversing</u>":

$$\begin{array}{lccccccc}
\text{fields} & K & \subseteq & F & \subseteq & E & \subseteq & L \\
 & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\text{groups} & \underset{\text{full group}}{\mathrm{Aut}_K(L) = G} & \supseteq & F' & \supseteq & E' & \supseteq & 1 = \{1\} \text{ trivial subgroup}
\end{array}$$

<u>E.g.</u> Consider $L = \mathbb{Q}(\sqrt{2})$ over $K = \mathbb{Q}$. We have seen that the Galois group is $G = \mathrm{Aut}_K(L) = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$, and there are two subgroups $\{1\}$ and G itself. But similarly, the only sub-extensions are L and K (which can be seen by considering degrees!), and we have $L' = \{1\}$ while $K' = G$.

<u>E.g.</u> With $L = \mathbb{Q}(\sqrt[3]{2})$ and $K = \mathbb{Q}$, we know this is <u>not</u> a <u>Galois</u> <u>extension</u>, indeed $G = \mathrm{Aut}_K(L) = \{1\}$ which has only one subgroup (itself), but there are two sub-extensions: L and K.

E.g. Consider $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbb{Q}$. We have $[L:K] = 4$ and a basis of L over K is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. What does $\mathrm{Aut}_K(L)$ look like? We have two automorphisms:

$$\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$\sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$

i.e. σ_1 sends $\sqrt{2}$ to $-\sqrt{2}$ (and fixes $\sqrt{3}$), and σ_2 sends $\sqrt{3}$ to $-\sqrt{3}$ (and fixes $\sqrt{2}$). Each σ_i satisfies $\sigma_i^2 = 1$ (they are involutions) and their product $\sigma_1\sigma_2 = \sigma_2\sigma_1$ is also an involution, so that

$G = \mathrm{Aut}_K(L) = \{1, \sigma_1, \sigma_2, \sigma_1 \cdot \sigma_2\} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

In particular notice that $G' = K$, so L/K is indeed Galois.

The structure of sub-extensions of L and subgroups of G is:

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\quad \xrightarrow{F \mapsto F'} \quad
\begin{tikzcd}[column sep=small]
 & \{1\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{1, \sigma_2\} \arrow[dr, dash] & \{1, \sigma_1\} \arrow[d, dash] & \{1, \sigma_1 \cdot \sigma_2\} \arrow[dl, dash] \\
 & G &
\end{tikzcd}$$

The proof of the fund. thm. is rather involved. To start, we need:

<u>Def'n</u> Let L/K be an extension, and $G = \mathrm{Aut}_K(L)$. For a sub-extension $K \subseteq F \subseteq L$, we say F is <u>closed</u> if $(F')' = F$. Similarly, for a subgroup $H \subseteq G$, we say H is <u>closed</u> if $(H')' = H$.

<u>Thm</u> There is a correspondence between closed sub-extensions $K \subseteq F \subseteq L$ and closed subgroups, given by $F \mapsto F'$.

<u>Pf</u>: Exercise, the inverse is given by $H \mapsto H'$. ∎

So the main task is to show that if L/K is a finite Galois extension, then all intermediary fields, and all subgroups of the Galois group, are closed...

Our proof of the fund. thm. will rely on keeping track of more numerical info about sub-extensions of L/K & subgroups of $\mathrm{Aut}_K(L)$. To that end, if E, F are intermediary fields $K \subseteq E \subseteq F \subseteq L$ we define their <u>relative degree</u> to be $[F:E]$, and if I, H are subgroups $\{1\} \subseteq I \subseteq H \subseteq G := \mathrm{Aut}_K(L)$, we define their <u>relative index</u> to be $[H:I]$.

<u>Thm</u> (Fund. Thm, Refined) Let L/K be a finite Galois extension. Under the correspondence $F \mapsto F'$ (with inverse $H \mapsto H'$) between sub-extensions of L/k and subgroups of $G := \mathrm{Aut}_K(L)$:

for two intermediary fields $k \subseteq E \subseteq F \subseteq L$, their relative degree is the relative index of the corresponding subgroups $E' \supseteq F'$.
(In particular, $|\mathrm{Aut}_K(L)|$ is $[L:K]$ in this case.)

<u>Thm</u> (Fund. Thm, Cont'd) Also, for any intermediary field $K \subseteq F \subseteq L$, L is always a Galois extension of F, but F is a Galois extension of K $\Leftrightarrow$ the subgroup F' is <u>normal</u> in G, in which case $\mathrm{Aut}_K(F) \simeq G/F'$ is its Galois group.

We will sketch a proof of the first part, see book for 2^{nd} part.

<u>E.g.</u>: In our previous example of $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $K = \mathbb{Q}$, for any of the intermediary fields $F = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$, or $\mathbb{Q}(\sqrt{6})$ we have $F' \simeq \mathbb{Z}/2\mathbb{Z}$, and indeed relative index $[F:K] = 2$ $= [\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} : \mathbb{Z}/2\mathbb{Z}]$ (recalling that $K' = G \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$). Also, all these subgroups are normal, and indeed F/K is Galois.

<u>E.g.</u> On the homework you will consider $L = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$, where $\omega = e^{\frac{2\pi i}{3}}$ is a primitive cube root of unity, over $K = \mathbb{Q}$. This L/K is Galois, however $G = \mathrm{Aut}_K(L) \simeq S_3$, the symmetric group, which has <u>non-normal</u> subgroups. And indeed recall that $F = \mathbb{Q}(\sqrt[3]{2})$ over $K = \mathbb{Q}$ is <u>not</u> Galois. //

The main technical lemmas we will use involve inequalities for the relative degree and relative index of subfields/subgroups.

Lemma(1) Let L/K be a finite extension and $K \subseteq E \subseteq F \subseteq L$ intermediary fields. Then $[E' : F'] \leq [F : E]$.

Lemma(2) Let L/K be a finite extension and $\{1\} \subseteq I \subseteq H \subseteq G$ subgroups of $G = \mathrm{Aut}_K(L)$. Then $[I' : H'] \leq [H : I]$.

Let us see how these Lemmas let us prove the fund. thm. in the case when L/K is Galois...

Pf: (of Fund. Thm) Since L/K is Galois, K is closed. We will show in fact that all intermediary fields, and all subgroups of $G = \mathrm{Aut}_K(L)$ are closed. Let $K \subseteq F \subseteq L$ be an intermediary field. Then

$$\underbrace{[F:K] \leq [F'':K'']}_{\text{since } F \subseteq F''} = \underbrace{[F'':K]}_{\text{since } K = K''} \underbrace{\leq [K' : F']}_{\text{By 2nd Lem. above}} \underbrace{\leq [F:K]}_{\text{By 1st Lem. above}},$$

which means that $F'' = F$, i.e. that F is closed. The same basic chain of inequalities shows that any subgroup of G is closed, establishing the 1-to-1 correspondence in the fund. thm, and then the fact that relative degree of intermediary fields = relative index of subgroups also follows easily by the same inequalities. ☒

To prove the key technical lemmas relating relative degree and relative index, we play around with cosets of subgroups of finite groups of automorphisms and do some basic linear algebra (over the intermediary fields...).

Pf sketch of lem. 1: By an induction argument (see book), we can reduce to the case when $F = E(u)$ for some $u \in F$ algebraic over E, of degree n say. Let $f(x) \in E[x]$ be the min. poly. of u. We will construct an injection from the set of left cosets of F' in E' to the roots of $f(x)$. The map is given by $\sigma F' \mapsto \sigma(u)$, which can be checked easily to be well-defined and injective. ☒

Pf sketch of lem. 2: Let $[H:I] = n$ and suppose $[I':H'] > n$. So let $u_1, u_2, \ldots, u_{n+1} \in I'$ be linearly independent over H', and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be a complete set of coset representatives of I in H. Consider this system of equations:

$$\begin{aligned}
\sigma_1(u_1)x_1 + \sigma_1(u_2)x_2 + \cdots &+ \sigma_1(u_{n+1})x_{n+1} = 0\\
\sigma_2(u_1)x_1 + \cdots &+ \sigma_2(u_{n+1})x_{n+1} = 0\\
&\vdots\\
\sigma_n(u_1)x_1 + \cdots &+ \sigma_n(u_{n+1})x_{n+1} = 0
\end{aligned}$$

Because of the dimensions of this system, it always has a nontrivial solution (i.e., one with not all $x_i = 0$). Choose such a solution, where the number of nonzero x_i's is minimal. By rearranging, assume $x_1 = a_1$, $x_2 = a_2, \ldots, x_r = a_r$ with all these nonzero, and $x_{r+1} = \cdots = x_{n+1} = 0$. Can also assume $a_1 = 1$ by multiplying by a_1^{-1}. We will show there is a $\tau \in H$ s.t. $x_i = \tau a_i$ $\forall i$ is also a solution, with $\tau a_2 \neq a_2$, which contradicts minimality of our solution since subtracting it from our solution gives a smaller one. To show such a $\tau \in H$ exists, first note that some σ_i, say σ_1, is in I, so that $u_1 a_1 + \cdots + u_r a_r = 0$. That the u_i are linearly independent over H' means some a_i, say a_2, is not in H'. So choose a $\tau \in H$ with $\tau(a_2) \neq a_2$. Then it can be checked that this τ works, i.e., $x_i = \tau a_i$ is a solution too! ☒