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 already 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 $u_1, \ldots, u_n \in L$.
We use $K[u_1, \ldots, u_n]$ to denote the subring of L generated by K and $u_1, \ldots, u_n$, and $K(u_1, \ldots, u_n)$ to denote the subfield of L generated by K and $u_1, \ldots, u_n$.

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

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 $\{1, u, u^2, \ldots, u^{n-1}\}$
4) $L = K(u) \simeq K[x]/(f)$, where again f is the min. poly. of u.

1/22

<u>Pf:</u> 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 <u>field</u>. 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 $\mathbb{Q}$ (<u>exercise</u> 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 $u^4+2u^3+3 = (u+2)(\underbrace{u^3-3u-1}_{0})+(3u^2+7u+5) = 3u^2+7u+5$.

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 $g(x), h(x)$? <u>Euclidean</u> <u>algorithm</u> for <u>GCD</u>!:

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

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

$\Rightarrow g(x) = -7/37\,x + 29/111$ 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. ☒

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. $L = K(u_1, \ldots, u_n)$ with u_i all algebraic.
By induction on n, $[K(u_1, \ldots, u_{n-1}) : K] < \infty$, and by our study of simple extensions $[K(u_1, \ldots, u_{n-1}, u_n) : K(u_1, \ldots, u_{n-1})] = m < \infty$ 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. ☒

Rmk: An algebraic (but not finitely generated!) extension like $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \ldots \sqrt{d}$ 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.