

Math 6320 Lecture Notes

Lectures by Prof. David Zywina, Notes by Vivian Kuperberg

Disclaimer: Professor David Zywina is responsible for the lectures behind these notes, but has nothing to do with the writing of the notes themselves, and is not responsible for any typos or mistaken proofs. All questions or concerns about the validity of the notes should be sent to Vivian Kuperberg.

Contents

1 January 28th	3
1.1 Galois Theory	3
2 February 2nd	7
2.1 Galois Theory, continued	7
3 February 4th	9
3.1 Proof of the fundamental theorem	9
4 February 9th	12
4.1 More Thoughts on the fundamental theorem	12
4.2 Application: Finite fields	14
5 February 11th	15
5.1 Application: Fundamental Theorem of Algebra	15
5.2 Some General Structure Theorems	16
6 February 18th	19
6.1 Last time	19
6.2 Solving for roots of polynomials of low degree	20
6.2.1 Degree 2	20
6.2.2 Degree 3	20
6.2.3 Degree 4	21
6.2.4 Degree ≥ 5	22
7 February 23rd	23
7.1 Quintics	23

8 February 25th	25
8.1 Solvability and solvability	25
8.2 Galois groups of polynomials of small degree	26
9 March 3rd	28
9.1 Computing Galois groups over \mathbb{Q}	28
10 March 8th	30
10.1 Last Time	30
10.2 Infinite Galois Theory	31
11 March 10th	32
11.1 A New Topic: Representation Theory of finite groups	32
12 March 15th	35
12.1 Last Time	35
12.2 Group Rings	35
13 March 17th	39
13.1 Representations and their Characters	39
13.1.1 Interlude: Constructing New Representations	40
14 March 22nd	43
14.1 Complex Character Theory, continued	43
15 March 24th	46
15.1 Character Tables	46
16 April 5th	50
16.1 The last of the examples	50
16.2 Frobenius Divisibility feat. maybe some Burnside	51
17 April 7th	53
17.1 Loose end	53
17.2 Frobenius and Burnside, cont'd	53
18 April 12th: Transition to Homological Algebra	55
18.1 Hom	55
19 April 14th	58
19.1 Last time	58
19.2 Projective modules	58
19.3 Injective Modules	61

20 April 19th	62
20.1 Some more injective modules	62
20.2 Tensor Products Revisited! D&F§10.4	63
21 April 21st	65
21.1 I'm Getting Tensor Every Day	65
22 April 26th	68
22.1 Homology/Cohomology	68
23 April 28th	70
23.1 Snake Lemma Continued, and More Homological Algebra	70
24 May 3rd	73
24.1 Cohomology Cont: Next Ext and More Tor	73
25 May 5th	78
25.1 Last time	78
26 May 10th	83
26.1 The Cohomology of Groups	83
26.2 Central simple algebras	85

1 January 28th

As review, look at the field theory sections, § 13.1, 13.2, 13.4, 13.5.

1.1 Galois Theory

Let L be a field. Let $\text{Aut}(L)$ be the set of field automorphisms, or structure-preserving bijections $\sigma : L \xrightarrow{\cong} L$. $\text{Aut}(L)$ is a group under composition.

Let L/K be a field extension, i.e. a field $L \supseteq K$. (The book will usually use the notation K/F , but number theorists tend to use L/K .) We can then define a second group $\text{Aut}(L/K)$, the set of automorphisms of L that fix K . $\text{Aut}(L/K)$ is a subgroup of $\text{Aut}(L)$.

The question that Galois theory addresses is, what information does the group $\text{Aut}(L/K)$ encode about the extension L/K ?

Example. 1. $\text{Aut}(\mathbb{Q}) = 1$. $\sigma(1) = 1$, so all integers are fixed because addition is fixed, and then all rationals are fixed.

2. $\text{Aut}(\mathbb{F}_p) = 1$, for a similar reason.

3. $\text{Aut}(\mathbb{C}/\mathbb{R}) = \{1, \tau\}$, where τ is complex conjugation.

4. $\{1, \tau\} \subseteq \text{Aut}(\mathbb{C})$. $\text{Aut}(\mathbb{C})$ has many elements assuming the axiom of choice.

△

Lemma 1.1.1. *Let L/K be an algebraic extension. Take any $\alpha \in L$ and let $f(x) \in K[x]$ be a non-zero polynomial with root α . Then $\sigma(\alpha) \in L$ is a root of f for all $\sigma \in \text{Aut}(L/K)$.*

Proof. $f(x) = \sum_i c_i x^i$, with $c_i \in K$. $0 = f(\alpha) = \sum_i c_i \alpha^i$, so $0 = \sigma(0) = \sum_i \sigma(c_i) \sigma(\alpha)^i = \sum_i c_i \sigma(\alpha)^i = f(\sigma(\alpha))$. □

Example. Look at $\sigma \in \text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, with $\sqrt[3]{2} \in \mathbb{R}$. Then $\sigma(\sqrt[3]{2})$ has to map to a root of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, i.e. to itself, the only real root of $x^3 - 2$. So $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is trivial, because that fixation along with \mathbb{Q} being fixed determines the trivial automorphism.

△

Example. Let $\sigma \in \text{Aut}(\mathbb{F}_p(t)/\mathbb{F}_p(t^p))$. $\sigma(t)$ must be a root of $x^p - t^p = (x - t)^p$, so $\sigma(t) = t$, and thus just as above, this automorphism group is trivial.

△

The first example is boring because there aren't enough roots in our field. The second is boring because the extension is inseparable; the polynomial doesn't have distinct roots when you increase the field. So we avoid both pitfalls by making the following definition.

Definition 1.1.2. An algebraic extension L/K is *Galois* if it is *normal* and *separable*. Recall that an extension is *normal* if it is the splitting field of some polynomials in $K[x]$, and an extension is *separable* if every element is the root of a separable polynomial in $K[x]$, where, again, a separable polynomial is one that has distinct roots in the extension.

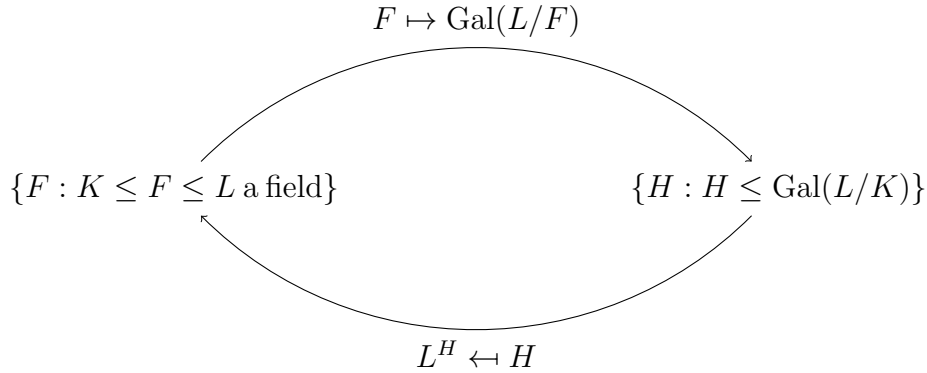
For a Galois extension L/K , we define $\text{Gal}(L/K) = \text{Aut}(L/K)$. The benefit of the new notation is that we call it Gal in the cases where we're sure that it'll be interesting.

Now, fix L/K a finite Galois extension.

1. (Getting a group out of a field) Let $K \subseteq F \subseteq L$ be a subfield. Then the extension L/F is Galois, so there's the group $\text{Gal}(L/F) \leq \text{Gal}(L/K)$.
2. (Getting a field out of a group) Take a subgroup $H \leq \text{Gal}(L/K)$. Then let L^H be the set of $\alpha \in L$ that are fixed by H . Note that this is actually a subfield of L , because fixation is preserved by the field operations. Also, $K \leq L^H$, because $H \leq \text{Gal}(L/K)$.

This is in fact a bijection between subgroups and subfields; it is a bijective correspondence, and the two directions are inverses of each other.

Theorem 1.1.3 (Fundamental Theorem of Galois Theory). *Let L/K be a finite Galois extension. The maps*



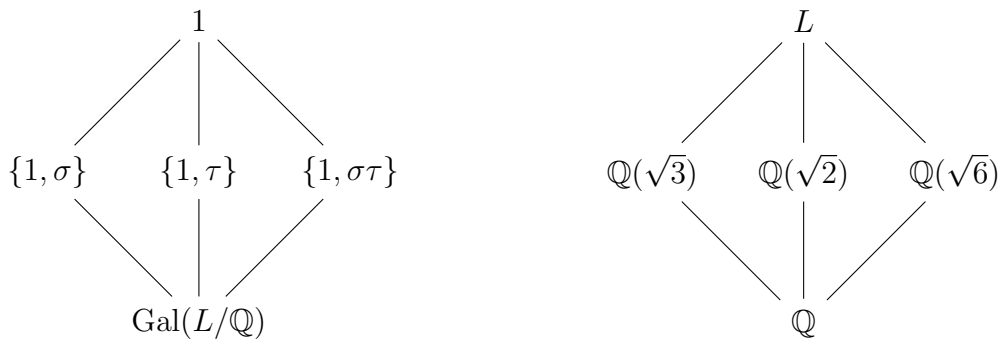
are inverses. The maps are inclusion reversing: $F_1 \supseteq F_2 \Rightarrow \text{Gal}(L/F_1) \subseteq \text{Gal}(L/F_2)$, and $H_1 \supseteq H_2 \Rightarrow L^{H_1} \subseteq L^{H_2}$.

We will see that $|\text{Gal}(L/F)| = [L : F]$, which is the definition of Galois in the book.

Example. We take L/\mathbb{Q} , with $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, the Galois splitting field of $x^2 - 2$ and $x^3 - 3$. $|\text{Gal}(L/\mathbb{Q})|$ should match $[L : \mathbb{Q}] = 4$.

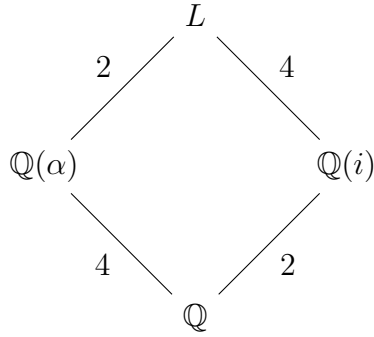
So we know we have $\text{Gal}(L/\mathbb{Q}(\sqrt{3})) \leq \text{Gal}(L/\mathbb{Q})$ which should have order 2, i.e. it should be $\{1, \sigma\}$. $\sigma(\sqrt{3}) = \sqrt{3}$, so $\sigma(\sqrt{2})$ shouldn't be $\sqrt{2}$; thus it sends $\sqrt{2}$ to $-\sqrt{2}$. Similarly, $\text{Gal}(L/\mathbb{Q}(\sqrt{2})) \leq \text{Gal}(L/\mathbb{Q})$ is $\{1, \tau\}$, where $\tau(\sqrt{3}) = -\sqrt{3}$ and $\tau(\sqrt{2}) = \sqrt{2}$. Then the group $\text{Gal}(L/\mathbb{Q})$ is thus $\{1, \sigma, \tau, \sigma\tau\}$. Each of these elements has order 2, so $\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

Okay, so we have this group. What are its subgroups? Well, the correspondence is illustrated by the diagrams below.



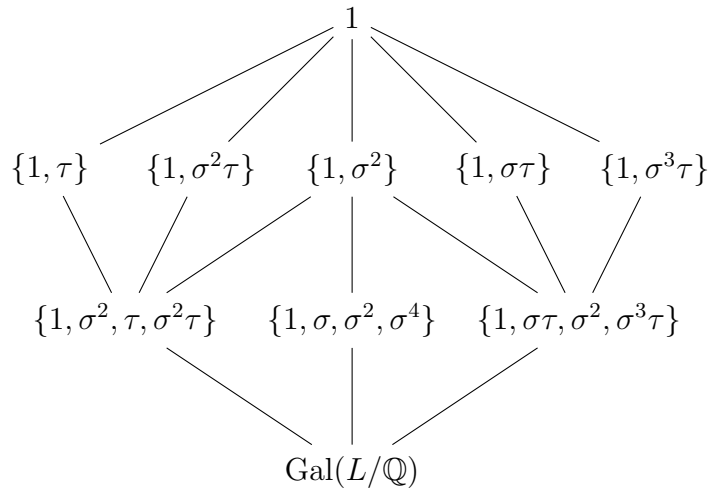
△

Example. Let L/\mathbb{Q} be the splitting field of $x^4 - 2$, in \mathbb{C} . Let $\alpha = \sqrt[4]{2} \in \mathbb{R}$ and let $i = \sqrt{-1}$. Then the roots of $x^4 - 2$ are $\pm\alpha, \pm i\alpha$, so $L = \mathbb{Q}(\alpha, i)$. So there's some lattice of subfields, which we know contains L .

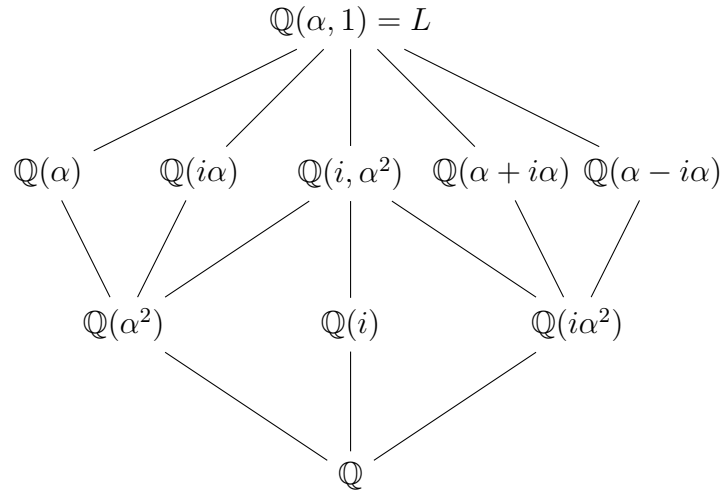


Gal(L/\mathbb{Q}) has order 8, so what are we missing? Well, Gal($L/\mathbb{Q}(\alpha)$) has order 2; it's $\{1, \tau\}$, where $\tau(\alpha) = \alpha$, so $\tau(i) = -i$. Also, Gal($L/\mathbb{Q}(i)$) \subseteq Gal(L/\mathbb{Q}) has order 4, so $\sigma \in$ Gal($L/\mathbb{Q}(i)$) is determined by $\sigma(\alpha)$; there are four options for this. There is a unique $\sigma \in$ Gal(L/\mathbb{Q}) with $\sigma(\alpha) = i\alpha$ and $\sigma(i) = i$. Note that $\sigma(\alpha) = i\alpha$, $\sigma^2(\alpha) = \sigma(i\alpha) = -\alpha$, $\sigma^3(\alpha) = -i\alpha$ and $\sigma^4(\alpha) = \alpha$, so this group is cyclic.

As it turns out, Gal(L/\mathbb{Q}) = $\langle \sigma, \tau \rangle$. One can check that $\tau\sigma\tau^{-1} = \sigma^{-1}$, so Gal(L/\mathbb{Q}) $\cong D_8$, the dihedral group. So we have



which leads to the analogous diagram for fields:



△

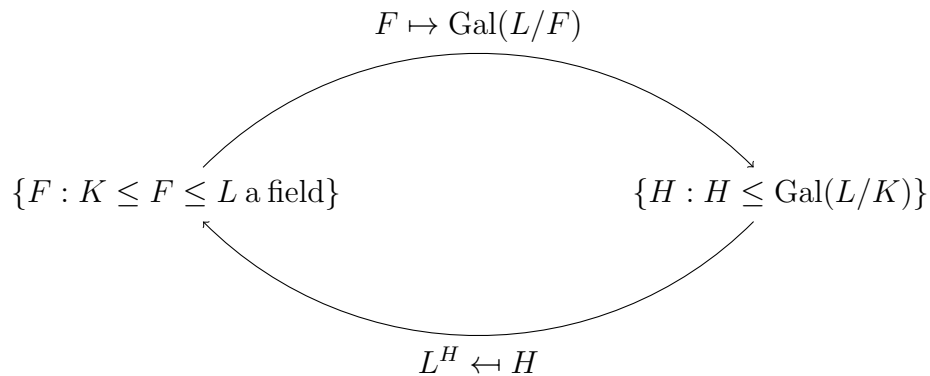
2 February 2nd

HW 1: Dummit and Foote 14.1 # 7,8; 14.2 # 1,3,5,12, 17 & 23, 18 & 21; 14.3 # 8. Due Thursday, February 11th. Recall that there are office hours Wednesday 12:30 - 2:30 in Malott 589.

2.1 Galois Theory, continued

Recall from last time, that we begin with L/K an algebraic field extension. L/K is *Galois* if it is separable and normal, where separable means that for every $\alpha \in L$, α is the root of a separable polynomial $f(x) \in K[x]$ (which automatically happens always in characteristic 0), and normal means that L is obtained from K by adjoining all roots of some polynomials in $K[x]$. In this case we have the Galois group $\text{Gal}(L/K) = \text{Aut}(L/K)$, when L/K is Galois. $\text{Aut}(L/K)$ is the group of field automorphisms of L that fix K . This led us to a Theorem:

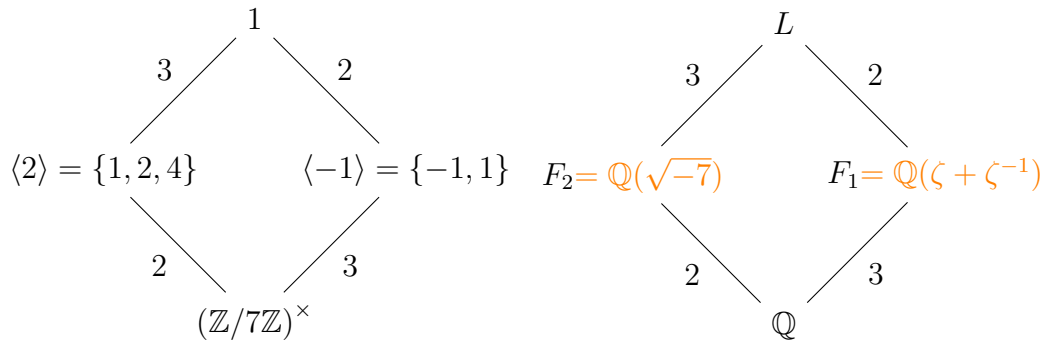
Theorem 2.1.1 (Fundamental Theorem of Galois Theory). *Let L/K be a finite Galois extension. The maps*



are inverses. The maps are inclusion reversing: $F_1 \supseteq F_2 \Rightarrow \text{Gal}(L/F_1) \subseteq \text{Gal}(L/F_2)$, and $H_1 \supseteq H_2 \Rightarrow L^{H_1} \subseteq L^{H_2}$. Also, $|\text{Gal}(L/F)| = [L : F]$. As a special case, $|\text{Gal}(L/K)| = [L : K]$.

Example. $L = \mathbb{Q}(\zeta)$, $K = \mathbb{Q}$, where $\zeta = e^{2\pi i/7}$, a 7th root of unity. What are the fields $F \subseteq L$? Every one of these is going to contain \mathbb{Q} . We're going to solve this by simply computing the Galois group; the subgroups of the Galois group will tell us exactly what these fields are due to the Fundamental Theorem. First, what's $\text{Gal}(L/K)$?

Note that ζ is a root of $\frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, which is irreducible over \mathbb{Q} . (To show that, replace x by $x+1$ and use the Eisenstein criterion). What are the roots? Well, $\zeta^1, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6$. So L/\mathbb{Q} is Galois. But what is it? Well, for $\sigma \in \text{Gal}(L/\mathbb{Q})$, we must have $\sigma(\zeta)$ a root of $\frac{x^7-1}{x-1}$, so $\sigma(\zeta)$ must be one of the six. Also, note that this is the only choice we have, because the image of ζ determines the image of all powers of ζ and thus of all elements. So we have a map $\varphi : \text{Gal}(L/\mathbb{Q}) \rightarrow (\mathbb{Z}/7\mathbb{Z})^\times$, where $\sigma(\zeta) = \zeta^{\varphi(\sigma)}$. This is a homomorphism: $\zeta^{\varphi(\sigma\tau)} = \sigma\tau(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{\varphi(\tau)}) = \zeta^{\varphi(\sigma)\varphi(\tau)}$. But that means it is in fact an isomorphism, since it's injective and these are finite and have the same order. So $\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6$. So we can find all the subgroups! There are four; one of each order 1,2,3, and 6.



And note that $L^1 = L$, $L^{\text{Gal}(L/\mathbb{Q})} = \mathbb{Q}$. Then $F_1 = L^{H_1}$, where $H_1 = \{1, \sigma\}$ and $\sigma(\zeta) = \zeta^{-1}$. Then $\zeta + \zeta^{-1} \in F_1 = L^{\langle \sigma \rangle}$. Note $\zeta + \zeta^{-1} \notin \mathbb{Q}$. Otherwise, ζ is a root of $x^2 - (\zeta + \zeta^{-1})x + 1$, which has coefficients in \mathbb{Q} , but ζ is a root of an irreducible degree 6 polynomial, so this is a problem.

Now let $\alpha = \zeta + \zeta^2 + \zeta^4$. $F_2 = L^{H_2}$ with $H_2 = \langle \tau \rangle$, and $\varphi(\tau) = 2$, so $\tau(\zeta) = \zeta^2$. So then $\tau(\alpha) = \tau(\zeta) + \tau(\zeta^2) + \tau(\zeta^4) = \zeta^2 + \zeta^4 + \zeta = \alpha$. So then $\alpha \in F_2$. It turns out $\alpha = \sqrt{-7}$, which can be seen by the fact that

$$\begin{aligned} \alpha^2 &= \zeta^2 + \zeta^4 + \zeta + 2\zeta^3 + 2\zeta^5 + 2\zeta^6 \\ &= 2(\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1) - \alpha - 2 \\ \Rightarrow 0 &= \alpha^2 + \alpha + 2 \\ \Rightarrow \alpha &= \frac{-1 \pm \sqrt{-7}}{2}. \end{aligned}$$

So, $F_2 = \mathbb{Q}(\sqrt{-7})$.

Remark. $\zeta + \zeta^{-1} = 2 \cos(2\pi/7)$, and $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = 3 \neq 2^n$, which ends up meaning as we'll see later that the regular 7-gon is not constructible with straightedge and compass.

△

We will begin the proof of the Fundamental Theorem now.

We'll need the primitive element theorem:

Theorem 2.1.2 (Primitive Element Theorem). *Let L/K be a finite separable extension. Then $L = K(\theta)$ for a "primitive element" $\theta \in L$.*

Idea of proof. • If L is finite, then $L^\times = \langle \theta \rangle$, so $L = K(\theta)$.

- If L is infinite, then the main case is $L = K(\alpha, \beta)$, so show that $\theta = \alpha + c\beta$ works for all but finitely many $c \in K$.

□

We then start with the following lemma.

Lemma 2.1.3. *Let L/K be a finite separable extension. Then $|\text{Aut}(L/K)| \leq [L : K]$. Moreover, L/K is Galois if and only if equality holds; in fact, this is the book's definition of Galois.*

Proof. $L = K(\theta)$, let $f \in K[x]$ be the minimal polynomial of θ (it is separable). Then $\deg(f) = [L : K]$. Choose a field $E \supseteq L$ for which f splits, so that $f = (x - \theta_1) \cdots (x - \theta_n)$, with $\theta_i \in E$. Then there are precisely $[L : K]$ embeddings of $L \hookrightarrow E$ that are the identity on K . Why is this the case? Well, just map $\theta \mapsto \theta_i$. This makes sense, because $K(\theta) = K[x]/(f(x))$.

So now we have the inequality. Each automorphism gives a different embedding, so the number of automorphisms is strictly less than the number of embeddings, so $|\text{Aut}(L/K)| \leq [L : K]$. Equality holds if and only if all embeddings $L \hookrightarrow E$ that fix K have image in L , which will only happen when all θ_i 's are in L itself. Thus if equality holds, the extension is certainly Galois, because $L = K(\theta_1, \dots, \theta_n)$.

Claim. Let L/K be finite and Galois; take $\alpha \in L$ and let $f \in K[x]$ be its minimal polynomial. Then f splits in L . We'll come back to proving this next time. □

3 February 4th

3.1 Proof of the fundamental theorem

Recall that we let L/K be a finite separable extension. Choose $E \supseteq L$ such that E/K is Galois. For today, let $\text{Emb}_K(L, E)$ be the group of field homomorphisms $L \rightarrow E$ that fix K . Then there is a natural map $\text{Aut}(L/K) \hookrightarrow \text{Emb}_K(L, E)$, where $\sigma \mapsto (L \xrightarrow{\sigma} L \subseteq E)$. We showed last time that $\text{Emb}_K(L, E)$ had cardinality $[L : K]$. As a consequence, $\#\text{Aut}(L/K) \leq [L : K]$.

Then we want to determine exactly when we have equality.

Claim. $\#\text{Aut}(L/K) = [L : K] \iff L/K$ is Galois.

\implies : If $L = K(\theta)$, where θ has minimal polynomial $f(x) \in K[x]$ of degree n , then $n = [L : K]$ and $f(x) = (x - \theta_1) \cdots (x - \theta_n)$, for $\theta_i \in E$. There are $[L : K]$ embeddings $L = K(\theta) \rightarrow E$ that fix K , one for each $(\theta \mapsto \theta_i)$. But if the size equality holds, then $\text{Aut}(L/K) \xrightarrow{\sim} \text{Emb}_K(L, E)$, so $\theta_i \in L$ and thus $L = K(\theta_1, \dots, \theta_n)$, which is Galois over K .

\impliedby : If L is Galois, then $L = K(\theta_1, \dots, \theta_n)$, where θ_i are the roots of some separable $f(x) \in K[x]$. So take any embedding $\sigma : L \hookrightarrow E$ that fixes K . Then $\sigma(\theta_i)$ is another root of f in E , so $\sigma(\theta_i) \in L$ already. So $\sigma(L) = \sigma(K(\theta_1, \dots, \theta_n)) \subseteq L$, so $\sigma : L \rightarrow L$, which is an isomorphism since it is an injective homomorphism of finite dimensional K -vector spaces of the same dimension.

OK, so that completed the proof of the lemma from last time. We now complete the proof, using one of Artin's ridiculously slick proofs.

Theorem 3.1.1 (Artin). *Let L be a field. Let G be a finite subgroup of $\text{Aut}(L)$. Then L/L^G is a finite Galois extension and $\text{Gal}(L/L^G) = G$. Moreover, $[L : L^G] = |G|$.*

Before the proof, we give an example.

Example. $L = \mathbb{Q}(t)$. Consider the automorphism $\sigma : L \rightarrow L$ given by $x \mapsto x$ for $x \in \mathbb{Q}$ and $t \mapsto \frac{t-1}{t}$ (check that this is an automorphism). Let $G = \langle \sigma \rangle$. Note that $\sigma^2(t) = \sigma(\sigma(t)) = \sigma(\frac{t-1}{t}) = \frac{-1}{t-1}$; then $\sigma^3(t) = \sigma(\frac{-1}{t-1}) = t$, so $G = \langle \sigma \rangle$ has order 3.

Let $\alpha = t + \sigma(t) + \sigma^2(t)$ (or the trace of G). $\sigma(\alpha) = \alpha$, so $\alpha \in L^G$; as it turns out, $L^G = \mathbb{Q}(\alpha)$. In general, traces and norms are the cheapest way to go from a field to a base field.

△

Proof. Take any $\alpha \in L$. Fix a maximal subset $\{\sigma_1, \dots, \sigma_r\} \subseteq G$ such that $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ are distinct. Define $f(x) = \prod_{i=1}^r (x - \sigma_i(\alpha)) \in L[x]$, which is separable. Then we claim that $f \in L^G[x]$. Take any $\tau \in G$; then

$$\tau(f) = \prod_{i=1}^r (x - \tau(\sigma_i(\alpha))).$$

Note that $\{\sigma_1(\alpha), \dots, \sigma_r(\alpha)\} = \{\tau\sigma_1(\alpha), \dots, \tau\sigma_r(\alpha)\}$; one direction is clear because the set of σ_i 's was maximal. Then the sets have the same size, so they must be the same.

In particular, $\tau(f) = f$. But this holds for each $\tau \in G$, so $f \in L^G[x]$. Also, $f \in L^G[x]$ is irreducible. If it factored, the group would permute the roots of that factor, but it actually acts transitively on all of the roots.

So in particular, L/L^G is Galois. G also fixes L^G , so $G \subseteq \text{Gal}(L/L^G)$. We just need the other inclusion, that $\text{Gal}(L/L^G) \subseteq G$. With α such that $L = L^G(\alpha)$, we have $[L : L^G] = \deg f \leq |G|$, using f from above. We know that $\deg f \leq |G|$, because its roots are indexed by elements of G . So $|G| \leq \#\text{Gal}(L/L^G) \leq [L : L^G] \leq |G|$, and thus $[L : L^G] = |G|$ and $G = \text{Gal}(L/L^G)$. □

Corollary 3.1.2. Fix a finite Galois extension L/K and take any subfield $K \subseteq F \subseteq L$. We have $L^{\text{Gal}(L/F)} = F$.

Proof.

$$\begin{aligned} [L : L^{\text{Gal}(L/F)}] &= |\text{Gal}(L/F)| \\ &= [L : F], \text{ since } L/F \text{ is Galois.} \\ &= [L : L^{\text{Gal}(L/F)}][L^{\text{Gal}(L/F)} : F]. \end{aligned}$$

So $[L^{\text{Gal}(L/F)} : F] = 1$, and thus $F = L^{\text{Gal}(L/F)}$. □

Corollary 3.1.3. Fix a finite Galois extension L/K and let H be a subgroup of $\text{Gal}(L/K)$. We have $\text{Gal}(L/L^H) = H$ and $[L : L^H] = \#H$.

Proof. Use the theorem with $G = H$, □

So these two corollaries give the fundamental theorem, stated again now that it has been proved.

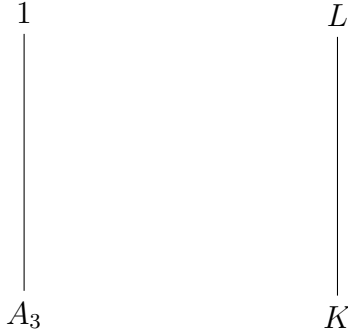
Theorem 3.1.4 (Fundamental Theorem of Galois Theory: short statement version.). *Let L/K be a finite Galois extension. The maps $\{F : K \subseteq F \subseteq L\} \rightarrow \{H : H \text{ subgroup of } \text{Gal}(L/K)\}$ with $F \mapsto \text{Gal}(L/F)$ and $\{H : H \text{ subgroup of } \text{Gal}(L/K)\} \rightarrow \{F : K \subseteq F \subseteq L\}$ with $H \mapsto L^H$ are inverses.*

Proof. Start with F ; then $L^{\text{Gal}(L/F)} = F$. Start with H ; then $\text{Gal}(L/H) = H$. □

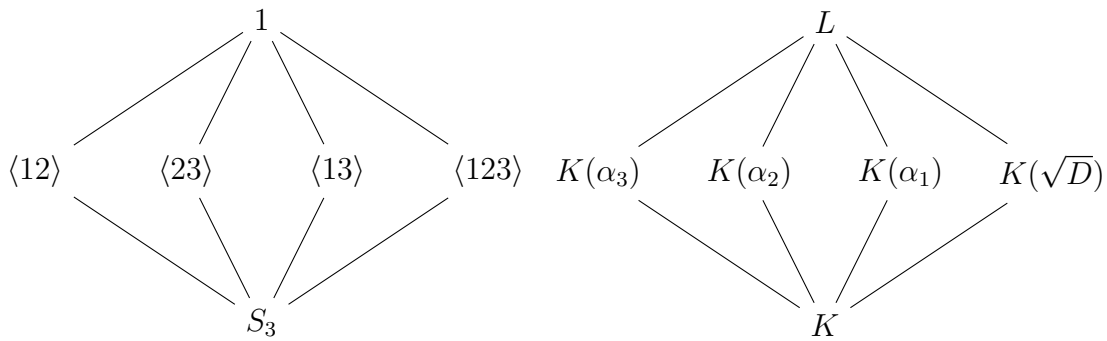
Example. Fix a field K with characteristic not 2 or 3. Fix an irreducible cubic $f(x) \in K[x]$; let L be the splitting field of f over K . $L = K(\alpha_1, \alpha_2, \alpha_3)$, with $\alpha_1, \alpha_2, \alpha_3 \in L$ roots of f . The Galois group $\text{Gal}(L/K)$ acts on $\{\alpha_1, \alpha_2, \alpha_3\}$ via permutations, so there exists $\varphi : \text{Gal}(L/K) \rightarrow S_{\{\alpha_1, \alpha_2, \alpha_3\}} = S_3$. But this map is injective, since $\sigma \in \text{Gal}(L/K)$ is determined by $\sigma(\alpha_1), \sigma(\alpha_2), \sigma(\alpha_3)$. But the permutation action is transitive because f is irreducible, so $\text{Gal}(L/K)$ must be a subgroup of S_3 that acts transitively on the three letters, of which there are two: S_3 and $A_3 = C_3$.

How do we distinguish the two cases? Let $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \in L$. Take $\sigma \in \text{Gal}(L/K)$ with $\varphi(\sigma) = (123)$. Then $\sigma(\delta) = (\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)(\alpha_1 - \alpha_2) = \delta$, i.e. δ is fixed by A_3 . Suppose there exists $\sigma \in \text{Gal}(L/K)$ with $\varphi(\sigma) = (12)$. Then $\sigma(\delta) = (\alpha_2 - \alpha_1)(\alpha_1 - \alpha_3)(\alpha_3 - \alpha_2) = -\delta \neq \delta$ since we're not in characteristic 2. But note that $\sigma(\delta^2) = \delta^2$ still. So $\delta^2 \in L^{\text{Gal}(L/K)} = K$, and $\delta \in K$ if and only if $\varphi(\text{Gal}(L/K)) = A_3$. So $D = \delta^2 \in K$ is the *discriminant* of $f \in K[x]$. $\text{Gal}(L/K) \cong A_3$ if $D \in K$ is a square, and $\text{Gal}(L/K) \cong S_3$ if $D \in K$ is not a square.

In the case where the Galois group is A_3 the subgroup diagram is as follows.



In the case where the Galois group is S_3 , the subgroup diagram is as follows.



△

4 February 9th

4.1 More Thoughts on the fundamental theorem

Recall the fundamental theorem: let L/K be a finite Galois extension. Then the maps

$$\{F : K \subseteq F \subseteq L\} \leftrightarrow \{H \leq \text{Gal}(L/K)\}$$

given by $F \mapsto \text{Gal}(L/F)$ and $H \mapsto L^H$ are inverses.

Here are some extra tidbits:

- The maps are inclusion reversing, and $|\text{Gal}(L/F)| = [L : F]$.
- Take $\sigma \in \text{Gal}(L/K)$, with $K \subseteq \sigma(F) \subseteq L$. If F corresponds to H , then $\sigma(F)$ corresponds to $\sigma H \sigma^{-1}$. $\sigma(F) \sim$ the group of $g \in \text{Gal}(L/K)$ such that $g(x) = x$ for all $x \in \sigma(F)$, or $\text{Gal}(L/\sigma(F))$, which is the same as the group of $g \in \text{Gal}(L/K)$ such that $g\sigma(x) = \sigma x$ for all $x \in F$, so $\sigma^{-1}g\sigma(x) = x$, which happens if and only if $\sigma^{-1}g\sigma \in H$.

- F/K is Galois if and only if $\sigma(F) = F$ for $\sigma \in \text{Gal}(L/K)$, which is true if and only if $\sigma H \sigma^{-1} = H$ for all $\sigma \in \text{Gal}(L/K)$, i.e. F/K is Galois $\iff H \trianglelefteq \text{Gal}(L/K)$. Suppose we're in this situation. Then we have as it turns out a short exact sequence

$$1 \rightarrow \text{Gal}(L/F) \hookrightarrow \text{Gal}(L/K) \twoheadrightarrow \text{Gal}(F/K) \rightarrow 1,$$

where for the third map we have $\sigma \mapsto \sigma|_F$ for $\sigma \in \text{Gal}(L/K)$. Exactness can be checked via finite cardinalities.

- Suppose F_1, F_2 correspond respectively to groups H_1, H_2 , respectively. Then $F_1 \cap F_2$ corresponds to $\langle H_1, H_2 \rangle$, and $F_1 F_2$ corresponds to $H_1 \cap H_2$.

There's more that you can add, but this is the basic fundamental theorem.

Now for some more comments on the theorem of artin from last time. let L/K be a finite Galois extension. Fix $\alpha \in L$, and choose $\{\sigma_1, \dots, \sigma_r\}$ to be a maximal subset of $\text{Gal}(L/K)$ such that $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ are distinct. Then $f(x) = \prod_{i=1}^r (x - \sigma_i(\alpha))$ has coefficients in $L^{\text{Gal}(L/K)} = K$. We also saw that f was irreducible in $K[x]$ and separable, so $f(x) \in K[x]$ is the minimal polynomial of α over K . Note further that f splits completely in L .

Fix a finite separable extension L/K (note: not necessarily Galois). The question is, what are the fields F between K and L , i.e. with $K \subseteq F \subseteq L$? Choose E/K a finite separable Galois extension with $E \supseteq L$. In particular, there is a θ with $L = K(\theta)$, with θ a root of a separable $f(x) \in K[x]$. Let E is the splitting field of f over L . Then we have

$$\{F : K \subseteq F \subseteq L\} \leftrightarrow \{\text{subgroups of } \text{Gal}(E/K) \text{ containing } \text{Gal}(E/L)\}$$

One thing that is appreciable, therefore, is that the set on the left is finite, since the set on the right is as well.

Example (non-example). Let $L = \mathbb{F}_p(x, y)$ and $K = \mathbb{F}_p(x^p, y^p)$, so that L/K is an extension of degree p^2 . But L/K is not separable! So what we just did shouldn't apply. L/K is not separable because $t^p - y^p \in K[t]$ is irreducible, but in the larger field it is $(t - y)^p$. We claim that $L \neq K(\theta)$ for all $\theta \in L$. If $\theta = f(x, y)$, then $\theta^p = f(x, y)^p = f(x^p, y^p) \in K$. So $[K(\theta) : K] \leq p$ (in fact, it's 1 or p), which then can't be all of L .

Claim. There are infinitely many fields F such that $K \subseteq F \subseteq L$. (The part that makes this a non-example is the infinitely many). This claim, which we prove now, gives some appreciation of the fact that we shouldn't have expected the left hand side above to be finite in the first place.

Consider $K(x + cy)$, with $c \in K$. Suppose $F = K(x + cy) = K(x + c'y)$, with $c \neq c'$. Then $(x + cy) - (x + c'y) = (c - c')y \in F$, so $y \in F$, and thus $x \in F$. Thus $F = K(x, y) = L$, so $L = K(x + cy)$, but we already showed that couldn't happen! \square

\triangle

We likely will say nothing about inseparable things ever again.

4.2 Application: Finite fields

Let \mathbb{F} be a finite field. Then there is a ring homomorphism $\mathbb{Z} \rightarrow \mathbb{F}$ mapping $1 \mapsto 1$; then for some prime p , $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{F}$. $\mathbb{Z}/p\mathbb{Z}$ is the finite field of order p . With $n = [\mathbb{F} : \mathbb{F}_p]$, we then have $|\mathbb{F}| = p^n$.

Take any $\alpha \in \mathbb{F}^\times$, a group of order $p^n - 1$. By basic group theory, $\alpha^{p^n - 1} = 1$, so $\alpha^{p^n} = \alpha$ for all $\alpha \in \mathbb{F}$. This is Fermat's Little Theorem. Moreover,

$$x^{p^n} - x = \prod_{\alpha \in \mathbb{F}} (x - \alpha).$$

Then \mathbb{F} is a splitting field of $x^{p^n} - x$ over \mathbb{F}_p . This has the consequence that, up to isomorphism, \mathbb{F} depends only on its size p^n . This also shows that finite fields of order p^n exist; their definition is as this splitting field.

Note that \mathbb{F}/\mathbb{F}_p is a Galois extension of degree n . We will at this point rename \mathbb{F} as \mathbb{F}_{p^n} , for clarity. Then $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ has order n . There is a distinguished automorphism $\sigma_p : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ with $x \mapsto x^p$, known as the Frobenius automorphism. Then the order of σ_p in the Galois group is the smallest $e \geq 1$ such that $\sigma_p^e = 1_{\mathbb{F}_{p^n}}$, i.e. $\alpha^{p^e} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$. $e = n$ certainly does the trick, since $\alpha^{p^n} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$. But, if $\alpha^{p^e} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$, then $p^e \geq p^n$, since $x^{p^e} - x$ is separable with at least p^n roots.

Therefore $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

What are the subgroups of the Galois group? Well, $\langle \sigma_p^d \rangle$, where d divides n . This is a group of order n/d . Each of these d 's corresponds to a field. From a Galois theory perspective, we have:

$$\begin{array}{ccc} \mathbb{F}_{p^n} & & 1 \\ \left| \begin{array}{c} n/d \\ \mathbb{F}_{p^d} \\ \left| \begin{array}{c} d \\ \mathbb{F}_p \end{array} \end{array} \right. & & \left| \begin{array}{c} n/d \\ \langle \sigma_p^d \rangle \\ \left| \begin{array}{c} d \\ \langle \sigma_p \rangle \end{array} \end{array} \right. \end{array}$$

In particular, for each d dividing n , there is a unique subfield \mathbb{F}_{p^d} of order p^d . You can actually start to build this up, depending on the n , doing something like

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^6} \subseteq \mathbb{F}_{p^{30}} \subseteq \cdots \subseteq \mathbb{F}_{p^{n!}} \subseteq \cdots$$

Taking their union, you get $\overline{\mathbb{F}_p}$, an algebraic closure of \mathbb{F}_p . This is no longer finite, though. It actually turns out to be minimal, which will distinguish it up to isomorphism.

Exercise: How would you build this up for \mathbb{Q} ? For $\mathbb{C}(x, y)$? It's less nice.

5 February 11th

5.1 Application: Fundamental Theorem of Algebra

Theorem 5.1.1 (Fundamental Theorem of Algebra). *The field \mathbb{C} is algebraically closed, i.e. every polynomial in $\mathbb{C}[x]$ splits.*

We say formally that $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$, and that i is the coset of x . For us, formally increasing the field is no big deal. We will use two analytic properties of the real numbers:

- 1) Every polynomial in $\mathbb{R}[x]$ of odd degree has a real root (follows from the Intermediate Value Theorem).
- 2) Positive $x \in \mathbb{R}$ have real square roots.
- 2') Square roots exist in \mathbb{C} . If $a+bi \in \mathbb{C}$ with $a, b \in \mathbb{R}$, take $c, d \in \mathbb{R}$ such that $c^2 = \frac{a+\sqrt{a^2+b^2}}{2}$, $d^2 = \frac{-a+\sqrt{a^2+b^2}}{2}$, with appropriate signs. Then $(c + id)^2 = a \pm bi$, which works for appropriate choice of signs. Note that $c^2 d^2 = \frac{b^2}{4}$.

Okay, now for the proof of the fundamental theorem.

Proof. Take any $f \in \mathbb{C}[x]$. Let L/\mathbb{C} be the splitting field of $f \cdot \bar{f} \in \mathbb{R}[x]$. We want to show that $L = \mathbb{C}$; we'll do this by looking at the Galois group. In particular, $\text{Gal}(L/\mathbb{R})$.

Let H be a 2-Sylow subgroup of $\text{Gal}(L/\mathbb{R})$. This exists, because $\mathbb{R} \leq \mathbb{C} \leq L$, and $[\text{Gal}(L/\mathbb{R}) : H]$ is odd, and $|H| = 2^e$. So we have the following picture:

$$\begin{array}{ccc}
 L & & 1 \\
 | & & | \\
 L^H & & H \\
 | & & | \\
 \mathbb{R} & & \text{Gal}(L/\mathbb{R})
 \end{array}$$

$[L^H : \mathbb{R}] = [\text{Gal}(L/\mathbb{R}) : H]$, which is odd. $L^H = \mathbb{R}(\theta)$; the degree of the minimal polynomial of θ over \mathbb{R} is $[L^H : \mathbb{R}]$, which is odd. So that polynomial has a real root. But the only case in which an irreducible polynomial has a real root is the case in which that polynomial has degree 1, so $[L^H : \mathbb{R}] = 1$, so $L^H = \mathbb{R}$. In particular, $H = \text{Gal}(L/\mathbb{R})$, so $\text{Gal}(L/\mathbb{R})$ is a 2-group.

We claim that if $\text{Gal}(L/\mathbb{C}) \neq 1$, then it has some subgroup of index 2. This follows from last semester's material. If G is a finite p -group, then there exists $H \leq G$ of index p . In particular, $Z(G) \neq 1$. So if $Z(G) \neq G$, replace G by $G/Z(G)$; inductively you can find a subgroup of index p . We need only address the case where $Z(G) = G$. Then by the

structure theorem of finite abelian groups, you can fairly explicitly find the subgroup. Now we (relabel) let H be the subgroup of index 2, so we have

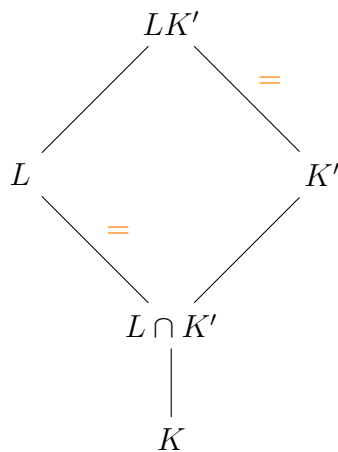
$$\begin{array}{ccc}
 L & & 1 \\
 | & & | \\
 L^H & & H \\
 | & & | \\
 2 & & 2 \\
 | & & | \\
 \mathbb{C} & & \text{Gal}(L/\mathbb{C})
 \end{array}$$

$L^H = \mathbb{C}(\theta)$; the minimal polynomial of θ over \mathbb{C} is of the form $x^2 + ax + b \in \mathbb{C}[x]$. But we can solve for $x \in \mathbb{C}$, since square roots exist in \mathbb{C} ; we know that the minimal polynomial is $(x + a/2)^2 + (b - a^2/4)$, and we can just solve. But this is a contradiction, because $\text{Gal}(L/\mathbb{C}) = 1$. Thus we've arrived at a contradiction no matter what, so $[L : \mathbb{C}] = 1$ and $L = \mathbb{C}$, and we're done. \square

This proof, which is sometimes criticized for being overly slick, is due to Artin. But, Galois theory is super helpful for looking at groups in general.

5.2 Some General Structure Theorems

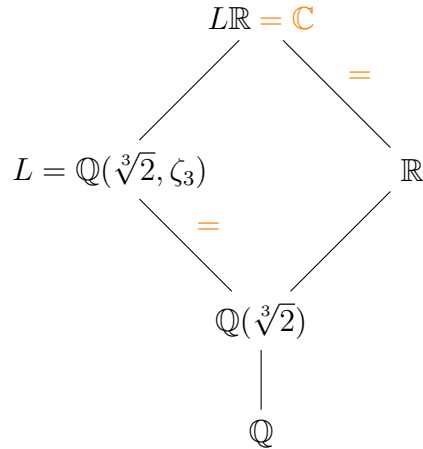
Theorem 5.2.1. *Let L/K be a finite Galois extension and K'/K be an extension (where L and K' lie in some common field), so that we have the following arrangement.*



The extension LK'/K' is Galois. The homomorphism $\text{Gal}(LK'/K') \rightarrow \text{Gal}(L/L \cap K')$ given by $\sigma \mapsto \sigma|_L$ is an isomorphism. In particular, $[LK' : K'] = [L : L \cap K']$ divides $[L : K]$.

Before we prove this, allow us to provide an example.

Example. Let L be the splitting field of $x^3 - 2$ over \mathbb{Q} , let K'/K be \mathbb{R}/\mathbb{Q} , and let's assume that $L \subseteq \mathbb{C}$.



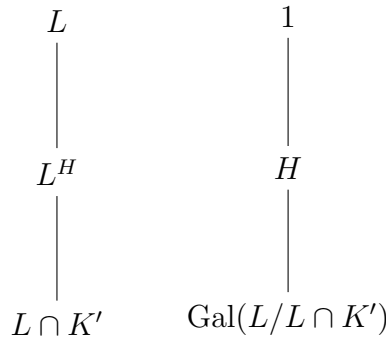
Also, $\text{Gal}(\mathbb{C}/\mathbb{R}) \xrightarrow{\sim} \text{Gal}(L/\mathbb{Q}(\sqrt[3]{2})) \subseteq \text{Gal}(L/\mathbb{Q})$, and both groups in the isomorphism have order 2.

△

Now for the proof!

Proof. Define $\varphi : \text{Gal}(LK'/K') \rightarrow \text{Gal}(L/L \cap K')$ by $\varphi : \sigma \mapsto \sigma|_L$.

φ is injective, which is easy to see by definition. Let $H = \text{im } \varphi$. The appropriate diagram is

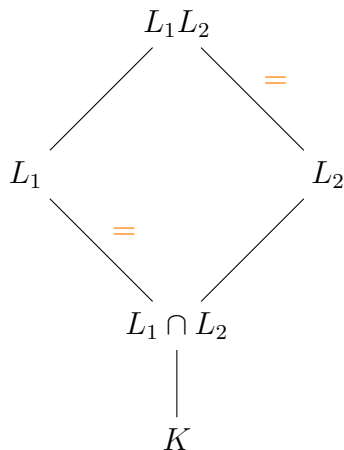


and $L^H K'$ is fixed by $\text{Gal}(LK'/K')$, by definition. $L^H K'$ is an extension of K' , so in fact they have to be equal to each other, because K' is exactly the elements fixed by $\text{Gal}(LK'/K')$. So $L^H \subseteq L \cap K' \subseteq L^H$, so $L^H = L \cap K'$. So then H has index 1 in $\text{Gal}(L/L \cap K')$, and that's the surjectivity. □

Theorem 5.2.2. Let L_1/K and L_2/K be finite Galois extensions, where L_1 and L_2 are in some common field. The extension $L_1 L_2/K$ is Galois, and the map

$$\begin{aligned} \text{Gal}(L_1L_2/K) &\rightarrow \text{Gal}(L_1/K) \times \text{Gal}(L_2/K) \\ \sigma &\mapsto (\sigma|_{L_1}, \sigma|_{L_2}) \end{aligned}$$

is an injective homomorphism. It is an isomorphism when $L_1 \cap L_2 = K$.



Proof.

That φ is injective is clear; knowing how σ acts on L_1 and L_2 is sufficient to know how φ acts on L_1L_2 . Now, assume $L_1 \cap L_2 = K$; $\text{Gal}(L_1L_2/L_2) \cong \text{Gal}(L_1/L_1 \cap L_2)$, so

$$\begin{aligned} [L_1L_2 : K] &= [L_1L_2 : L_2][L_2 : K] \\ &= [L_1 : L_1 \cap L_2][L_2 : K] \\ &= [L_1 : K][L_2 : K]. \end{aligned}$$

So φ is an injective homomorphism between groups of the same size, since $|\text{Gal}(L_1L_2/K)| = [L_1L_2 : K] = [L_1 : K][L_2 : K] = |\text{Gal}(L_1/K) \times \text{Gal}(L_2/K)|$. Since that size is finite, φ is an isomorphism. \square

Remark. • In the general case, $\text{im } \varphi = \{(\sigma, \tau) \in \text{Gal}(L_1/K) \times \text{Gal}(L_2/K) \mid \sigma|_{L_1 \cap L_2} = \tau|_{L_1 \cap L_2}\}$. This is proven in the book, but not here.

• $L_1 \cap L_2$ is Galois.

Example. Let k be a field. Let $n \geq 1$ be an integer, and let $L = k(x_1, \dots, x_n)$. Then $S_n \curvearrowright L$ (or $S_n \hookrightarrow \text{Aut}(L)$), where $\sigma \in S_n$ fixes k and takes x_i to $x_{\sigma(i)}$. Let $K = L^{S_n}$; then $\text{Gal}(L/K) = S_n$.

So what's K ? Well, $x_1x_2 \cdots x_n \in K$, $x_1 + \cdots + x_n \in K$, and so on. These are *elementary symmetric polynomials*:

$$\begin{aligned} s_1 &= x_1 + \cdots + x_n \\ &\dots \\ s_i &= \sum_{J \subseteq [n], |J|=i} \prod_{j \in J} x_j \\ s_n &= x_1x_2 \cdots x_n. \end{aligned}$$

Theorem 5.2.3. $K = k(s_1, \dots, s_n)$, and the s_i are independent variables.

As a proof of independence, consider $(t - x_1)(t - x_2) \cdots (t - x_n)$; this is $t^n - s_1 t^{n-1} + s_2 t^{n-2} - \cdots + (-1)^n s_n \in k(s_1, \dots, s_n)[t] \subseteq K[t]$.

Now for a proof of the theorem. $L/k(s_1, \dots, s_n)$ is the splitting field of f ; then $n! \leq |\text{Gal}(L/K)| \leq |\text{Gal}(L/k(s_1, \dots, s_n))| \leq n!$, so we're done, $K = k(s_1, \dots, s_n)$. △

6 February 18th

6.1 Last time

We saw that $k(x_1, \dots, x_n)^{S_n} = k(s_1, \dots, s_n)$, where $s_1 = x_1 + \cdots + x_n$, $s_2 = x_1 x_2 + \cdots$, $s_i = \sum_{|J|=i} \prod_{j \in J} x_j$, and $s_n = x_1 \cdots x_n$.

This in fact works with polynomials as well, which we didn't show last time. $k[x_1, \dots, x_n]^{S_n} = k[s_1, \dots, s_n]$.

Example.

$$\prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in k[x_1, \dots, x_n]^{S_n} = k[s_1, \dots, s_n].$$

△

Take a polynomial $f \in K[x]$ that is monic of degree $n \geq 1$. Let $\alpha_1, \dots, \alpha_n$ be its roots (in some extension), so that $f = (x - \alpha_1) \cdots (x - \alpha_n)$. Then the *discriminant* of f is

$$D_f = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in K[s_1(\alpha_1, \dots, \alpha_n), \dots, s_n(\alpha_1, \dots, \alpha_n)].$$

But the quantities $s_i(\alpha_1, \dots, \alpha_n)$ are the coefficients of the polynomial up to a sign, so $K[s_1(\alpha_1, \dots, \alpha_n), \dots, s_n(\alpha_1, \dots, \alpha_n)] = K$.

Example. $f(x) = x^2 + bx + c \in K[x]$. This factors into $(x - \alpha_1)(x - \alpha_2)$, and has discriminant $D_f = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c$. △

Example. $f = x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.

Then $f'(x) = 3x^2 + a = (x - \alpha_2)(x - \alpha_3) + (x - \alpha_1)(x - \alpha_3) + (x - \alpha_1)(x - \alpha_2)$. Plugging in different values, we get

$$\begin{aligned}
3\alpha_1^2 + a &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \\
3\alpha_2^2 + a &= -(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3) \\
3\alpha_3^2 + a &= (\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \\
\Rightarrow -D_f &= (3\alpha_1^2 + a)(3\alpha_2^2 + a)(3\alpha_3^2 + a) \\
&= 27(\alpha_1\alpha_2\alpha_3)^2 + 9a(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) + 3a^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + a^3 \\
&= 27b^2 + 9a^3 - 6a^3 + a^3 \\
&= 4a^3 + 27b^2
\end{aligned}$$

$$\Rightarrow D_f = -4a^3 - 27b^2.$$

Note that $\alpha_1 + \alpha_2 + \alpha_3 = 0$, so $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 - (\alpha_1 + \alpha_2 + \alpha_3)^2 = -2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -2a$, and $\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2 = a^2$.

The other ones are nastier still, but nevertheless doable and not so so bad. For $f = x^3 + ax^2 + bx + c$, you can replace evaluation at x by evaluation at $x - \frac{a}{3}$, which will give the same discriminant but turn it into the form seen above.

△

6.2 Solving for roots of polynomials of low degree

For degree 1, this is easy.

6.2.1 Degree 2

$f(x) = x^2 + bx + c \in K[x]$; assume that K does not have characteristic 2. Then $0 = f(x) = (x + b/2)^2 - b^2/4 + c$, so

$$x = -\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2},$$

which is just the familiar quadratic equation.

6.2.2 Degree 3

$f(x) = x^3 + ax^2 + bx + c \in K[x]$, with K not of characteristic 2 or 3. Replace $f(x)$ by $f(x - \frac{a}{3})$. So, assume $f = x^3 + ax + b \in K[x]$.

Vieta's substitution: $x = w - \frac{a}{3w}$. We then solve:

$$\begin{aligned}
w^3 - aw + a^2 \frac{1}{3w} - \frac{a^3}{27w^3} + a(w - a/3w) + b &= 0 \\
\iff w^3 - \frac{a^3}{27w^3} + b &= 0 \\
\iff w^6 + bw^3 - \frac{a^3}{27} &= 0 \\
\iff w^3 &= -\frac{b}{2} \pm \frac{\sqrt{b^2 + 4a^3/27}}{2} \\
&= -\frac{b}{2} \pm \frac{1}{18} \sqrt{-3(-4a^3 - 27b^2)}.
\end{aligned}$$

So w is the cube root of that, which gives roots $x = w - a/3w$ of f . There are six possible choices made here, and any one gives a root of f , with multiplicity.

Example. $f(x) = x^3 + x - 1$. Then $a = 1, b = -1$, and $D_f = -4 - 27 = -31$.

So $w^3 = \frac{1}{2} \pm \frac{1}{18} \sqrt{-3(-31)}$, so choosing the positive one $w = \sqrt[3]{\frac{1}{2} + \frac{1}{18} \sqrt{93}}$; taking $x = w - \frac{1}{3w}$, You Have Successfully Found A Root. Turns out choosing the other value of w^3 would give a different real value of w , but you'd end up with the same real root. There's only one.

△

Example. $f = x^3 - 4x + 1; a = -4, b = 1$. Then $D_f = 229$, so $w^3 = \frac{1}{2} \pm \frac{1}{18} \sqrt{-3 \cdot 229}$. The polynomial has three real roots that you can solve for, but you hit imaginary numbers along the way, which sometimes makes people uncomfortable, especially if you live in Italy in the 1500s. They were initially used as like this mysterious middle ground that would lead to something correct.

△

6.2.3 Degree 4

Let $f(x) = x^4 + ax^3 + \dots \in K[x]$. We assume that our characteristic isn't 2 or 3; by plugging in $x - a/4$ instead, we can get rid of the cubic term. So take $f(x) = x^4 + ax^2 + bx + c \in K[x]$.

For this one it's going to be better to rely on some Galois theory. Assume that f is separable, that it doesn't have repeated roots. Then $f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$, with α_i distinct. So we have a Galois extension $L = K(\alpha_1, \dots, \alpha_4)/K$. Define $\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$, $\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$, and $\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$, which are permuted by $\text{Gal}(L/K)$. From this we can make the *resolvent cubic*, $h(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3) \in L^{\text{Gal}(L/K)}[x] = K[x]$.

The thing about cubic polynomials is we know how to find the roots. So we can find the roots of h like before. Note that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, so $\theta_1 = -(\alpha_1 + \alpha_2)^2$, $\theta_2 = -(\alpha_1 + \alpha_3)^2$, and $\theta_3 = -(\alpha_1 + \alpha_4)^2$.

We then rearrange these equations to get $\alpha_1 + \alpha_2 = \pm\sqrt{-\theta_1}$, $\alpha_1 + \alpha_3 = \pm\sqrt{-\theta_2}$, and $\alpha_1 + \alpha_4 = \pm\sqrt{-\theta_3}$. Add and use that all α_i 's sum to 0 to get that

$$\alpha_1 = \frac{1}{2}(\pm\sqrt{-\theta_1} \pm \sqrt{-\theta_2} \pm \sqrt{-\theta_3})$$

is a root of f . Other roots are acquired by changing signs.

Good news! The resolvent actually has a nice expression. It's not just defined in terms of the roots, which would be a problem. There's some way to write them in terms of a, b, c . And in fact, the resolvent is:

$$h(x) = x^3 - 2ax + (a^2 - 4c)x + b^2.$$

The main takeaway is “fields are pretty, polynomials are ugly. As the degree goes up, of course it gets worse.”

Example. $f = x^4 + x^3 + x^2 + x + 1 \in \mathbb{C}[x]$. The roots are the 5th roots of unity. First you shift to get $f(x - \frac{1}{4}) = x^4 + \frac{5}{8}x^2 + \frac{5}{8}x + \frac{205}{256}$, which leads to the resolvent cubic $h(x) = (x + 5/4)(x^2 - 5/2x + 5/16)$, which happens to factor! The other two roots of h come from the quadratic equation, so all three roots are: $\theta_1 = -\frac{5}{4}$, $\theta_2 = \frac{5}{4} + \frac{\sqrt{5}}{2}$, $\theta_3 = \frac{5}{4} - \frac{\sqrt{5}}{2}$.

Thus a root of $f(x - \frac{1}{4})$ is of the form

$$\frac{1}{2} \left(\pm\sqrt{\frac{5}{4}} \pm \sqrt{-\frac{5}{4} - \frac{\sqrt{5}}{2}} \pm \sqrt{-\frac{5}{4} + \frac{\sqrt{5}}{2}} \right),$$

which leads to the root of f of the form

$$\left(\frac{\sqrt{5}}{2} - \frac{1}{4} \right) + \frac{1}{2} \left(\sqrt{\frac{5}{4} + \frac{\sqrt{5}}{2}} + \sqrt{\frac{5}{4} - \frac{\sqrt{5}}{2}} \right) i,$$

which is in fact a root of f ! It's $e^{2\pi i/5} \in \mathbb{C}$.

A horrible, horrible exercise is to take that expression, forget its gory origin story and its history of bloodshed, and see what happens if you take it to the fifth power! You'll get one.

△

6.2.4 Degree ≥ 5

This is a roadblock. It's not always possible to express the roots in terms of radicals. For example, with the polynomial $x^5 - x - 1$, the roots don't have some nice expression (with e.g. that thing for degree 4 being “nice”). The idea of the proof is going to be to look at the Galois group.

Let K be a field, with characteristic 0, and let $f \in K[x]$. Let $G = \text{Gal}(L/K)$, with L the splitting field of f over K . It turns out that the roots of f can be “expressed in terms of radicals” if and only if G is solvable. It also turns out that S_n for $n \geq 5$ isn't solvable, because for $n \geq 5$, $A_n \trianglelefteq S_n$ is simple and nonabelian.

7 February 23rd

All day today, let K be a field of characteristic 0.

7.1 Quintics

We saw that if $f(x) \in K[x]$ with $\deg f \leq 4$, then its roots can be “expressed by radicals,” a term to be defined later.

Example. The roots of $x^3 - 3x - 1$ in $\mathbb{Q}[x]$ are

$$\sqrt[3]{\frac{1 + \sqrt{-3}}{2}} + \left(\sqrt[3]{\frac{1 + \sqrt{-3}}{2}} \right)^{-1}.$$

△

So what does it mean to be “expressed by radicals”?

Definition 7.1.1. Fix α algebraic over K . Then α can be *expressed by radicals* if α is in a field L such that

$$K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L$$

where $L_{i+1} = L_i(\sqrt[n_i]{a_i})$ for some $a_i \in L_i$, $n_i \geq 1$.

We say that $f \in K[x]$ can be *solved by radicals* if all roots of f can be expressed by radicals.

The *Galois group* of $f(x) \in K[x]$ is the group

$$\text{Gal}(f) = \text{Gal}(L/K),$$

where L is the splitting field of f . This should be thought of as a group of “symmetries.”

Theorem 7.1.2 (due, in spirit at least, to Galois). $f \in K[x]$ can be solved by radicals if and only if $\text{Gal}(f)$ is solvable.

Recall from last semester the definition of solvability; G is *solvable* if and only if there’s a sequence $1 = G_n \subseteq G_{n-1} \subseteq \cdots \subseteq G_2 \subseteq G_1 \subseteq G_0 = G$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian (or cyclic).

Recall that Jordan Hölder tells us that if the quotients are simple, they are unique up to reordering and isomorphism.

This theorem actually motivated most of the definitions in modern abstract algebra; this is what led to people talking about groups and fields. Historically, it’s the very beginning.

Example. Let $f(x) = x^5 - x - 1 \in \mathbb{Q}[x]$. Let $\alpha_1, \dots, \alpha_5 \in \mathbb{C}$ be roots of f ; these are distinct, because $f' = 5x^4 - 1$, which is relatively prime to f .

Let $L = \mathbb{Q}(\alpha_1, \dots, \alpha_5)$. Then $\text{Gal}(L/\mathbb{Q}) \curvearrowright \{\alpha_1, \dots, \alpha_5\}$, so $\text{Gal}(L/\mathbb{Q}) \hookrightarrow S_5$. Here are some relevant observations from group theory:

1. f is irreducible. If it factors, it factors in $\mathbb{Z}[x]$. Then use the fact that $f \pmod{3} \in \mathbb{F}_3[x]$ is irreducible. This implies that the Galois action on the roots is transitive. The converse is true as well. A fact about S_5 is that this means that $\text{Gal}(L/\mathbb{Q})$ has an element of order 5.
2. f has 1 real root. This can be found using calculus. Then let $\tau \in \text{Gal}(L/\mathbb{Q})$ be complex conjugation; τ is not trivial, because if it were, all roots would be real. Also, $\tau^2 = 1$, so our group has an element of order 2.
3. (uncertain) but this probably implies that the subgroup contains A_5 .

A_5 isn't solvable, so this tells us that the polynomial can't be solved by radicals.

△

Example (Key). $f = x^n - a \in K[x]$. We'll show that $\text{Gal}(f)$ is solvable. Fix a root α of f . Let μ_n be the n th roots of unity in some extension of K , which makes it a cyclic group of order n .

Let $L = K(\alpha, \mu_n)$, which is the splitting field of $f = \prod_{\zeta \in \mu_n} (x - \zeta\alpha)$. Note that $K \leq K(\mu_n) \leq L$.

Note that $K(\mu_n)/K$ is Galois, so $\text{Gal}(L/K(\mu_n)) \trianglelefteq \text{Gal}(L/K) \cong \text{Gal}(K(\mu_n)/K)$. We then can simply show that the normal subgroup and the quotient are each solvable, which makes our job easier.

- I) Consider $\sigma \in \text{Gal}(K(\mu_n)/K)$, and let $\mu_n = \langle \zeta \rangle$. σ is then determined by $\sigma(\zeta)$, which has to be another n th root of unity. So $\sigma(\zeta) = \zeta^{\varphi(\sigma)}$, which gives us a well-defined map $\varphi : \text{Gal}(K(\mu_n)/K) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$. This map is an injection, and a homomorphism, which means that $\text{Gal}(K(\mu_n)/K)$ is abelian! Hence, solvable.
- II) Given $\sigma \in \text{Gal}(L/K(\mu_n))$, σ is determined by $\sigma(\alpha)$. $\sigma(\alpha) = \psi(\sigma)\alpha$ for a unique element $\psi(\sigma) \in \mu_n$, giving us an injective map $\psi : \text{Gal}(L/K(\mu_n)) \hookrightarrow \mu_n$. ψ is also a homomorphism: let $\sigma, \tau \in \text{Gal}(L/K(\mu_n))$, and then $\psi(\sigma\tau)\alpha = \sigma\tau(\alpha) = \sigma(\psi(\tau)\alpha) = \psi(\tau)\sigma(\alpha) = \psi(\tau)\psi(\sigma)$. Then $\text{Gal}(L/K(\mu_n))$ is abelian and therefore cyclic.

For this example, we broke up the extension into Galois pieces, and showed that each piece was abelian. This will be important for the proof of the Big Shiny Theorem.

△

Proposition 7.1.3. *Fix a Galois extension L/K of degree n with cyclic Galois group. Suppose $\mu_n \subseteq K$. Then $L = K(\sqrt[n]{a})$ for some $a \in K^\times$.*

This is a hint that “cyclic Galois group” translates to “the extension coming from one radical.” This is a good partial glimpse at what's really going on behind the theorem.

Proof. Let $\mu_n = \langle \zeta \rangle$ and let $\text{Gal}(L/K) = \langle \sigma \rangle$. Recall from homework 1 the norm map $N_{L/K} : L \rightarrow K$ given by

$$\alpha \mapsto \prod_{\tau \in \text{Gal}(L/K)} \tau(\alpha).$$

In this case, this is a product over powers of σ^{n-1} . Consider $N_{L/K}(\zeta^{-1})$. ζ^{-1} is in the base field, so this is just $(\zeta^{-1})^n = 1$.

From the theorem Hilbert 90 in HW 1, if L/K is a Galois extension with cyclic Galois group generated by σ and $\alpha \in L$ has norm 1, then $\alpha = \frac{\beta}{\sigma(\beta)}$ for some $\beta \in L^\times$. (As we'll find out later in the semester, if L/K is Galois, then $H^1(\text{Gal}(L/K), L^\times) = 0$, where H^1 is group cohomology).

So we have an element $\beta \in L^\times$ with $\zeta^{-1} = \frac{\beta}{\sigma(\beta)}$, so $\sigma(\beta) = \zeta\beta$. Inductively, $\sigma^i(\beta) = \zeta^i\beta$. Choose $a = \beta^n$; then $\sigma(a) = (\sigma\beta)^n = (\zeta\beta)^n = \beta^n = a$; since the Galois group is cyclic, every element fixes a , so $a \in K$. Then $\beta = \sqrt[n]{a}$. We have $K(\beta) \subseteq L$. β is not fixed by any $\tau \in \text{Gal}(L/K) \setminus \{1\}$, so $\text{Gal}(L/K(\beta)) = 1 \Rightarrow K(\beta) = L$, and we are done. \square

8 February 25th

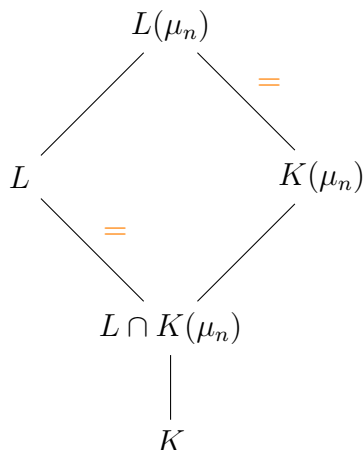
8.1 Solvability and solvability

Again, for all of this section we will say that the characteristic of K is 0.

Recall this theorem, mentioned the past couple times, yet to be proven.

Theorem 8.1.1. $f \in K[x]$ can be solved by radicals if and only if $\text{Gal}(f)$ is solvable.

Proof. (\Leftarrow): Let L be the splitting field of f over K , and let $n = [L : K]$. Let μ_n be the n th roots of unity in some extension of L . So here's a diagram with all the important fields:



We need to show that $L(\mu_n)$ can be obtained from $K(\mu_n)$ by adjoining radicals. $\text{Gal}(L/L \cap K(\mu_n)) \trianglelefteq \text{Gal}(L/K)$, since $L \cap K(\mu_n)/K$ is Galois. Thus $\text{Gal}(L/L \cap K(\mu_n))$ is solvable, since

it is a normal subgroup of a solvable group. Then $\text{Gal}(L(\mu_n)/K(\mu_n)) \cong \text{Gal}(L/L \cap K(\mu_n))$ is solvable as well. Without loss of generality $\mu_n \subseteq K$ (?), so the order divides n .

Since $\text{Gal}(L/K)$ is solvable, $\text{Gal}(L/K) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = 1$, such that G_i/G_{i+1} is cyclic of order dividing n , and $G_{i+1} \trianglelefteq G_i$. Let $L_i = L^{G_i}$. Then $\text{Gal}(L_{i+1}/L_i)$ is cyclic of order d , with $\mu_d \subseteq L_i$. From our proposition last time, then $L_{i+1} = L_i(\sqrt[d]{a_i})$, with $a_i \in L_i$, so we are done.

(\Rightarrow): Let L be the splitting field obtained by radicals of f . Let E be the Galois closure of L/\overline{K} . For all $\sigma \in \text{Gal}(E/K)$, $\sigma(L)$ is the element obtained by radicals over K . So replace L by the composition of all the $\sigma(L)$; without loss of generality L is Galois over K .

Then

$$L = L_m \supseteq L_{m-1} \supseteq \cdots \supseteq L_1 \supseteq L_0 = K,$$

where L_{i+1} is the splitting field over L_i of some $x^{n_i} - a_i \in L_i[x]$. Then

$$1 = G_m \subseteq G_{m-1} \subseteq \cdots \subseteq G_1 \subseteq G_0 = \text{Gal}(L/K),$$

where $G_i = \text{Gal}(L/L_i)$. Since L_{i+1}/L_i is Galois, $G_{i+1} \trianglelefteq G_i$, and $\text{Gal}(L_{i+1}/L_i) \cong G_i/G_{i+1}$, which is solvable as seen last time. Thus $\text{Gal}(L/K)$ is solvable, and there is a surjective homomorphism $\text{Gal}(L/K) \twoheadrightarrow \text{Gal}(f)$, so $\text{Gal}(f)$ is solvable as well. \square

Remark. The theorem is false when $\text{char } K = p > 0$. Let L be the splitting field of $x^p - x - a \in K[x]$. Then $\text{Gal}(L/K)$ is cyclic of order p , but L is not $K(\sqrt[p]{a})$, even though $1 = \mu_p \subseteq K$.

8.2 Galois groups of polynomials of small degree

Let $f \in K[x]$ be monic, separable, and irreducible, with K not of characteristic 2, and let L be the splitting field of f over K . Then $f = \prod_{i=1}^n (x - \alpha_i)$, with $\alpha_i \in L$ and n the degree of f , and $L = K(\alpha_1, \dots, \alpha_n)$. $\text{Gal}(f) = \text{Gal}(L/K)$, and $D_f = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in K$.

We can view $\text{Gal}(f)$ as a subgroup of S_n based on its action on the roots of f , where $\sigma(\alpha_i) = \alpha_{\sigma(i)}$.

Fact 8.2.1. $\text{Gal}(f) \subseteq A_n$ if and only if D_f is a square in K , in which case $\sqrt{D_f} = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$.

Proof. S_n acts on $\mathbb{Z}[x_1, \dots, x_n]$ by permuting the indices. Then for $\sigma \in S_n$,

$$\sigma \left(\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \right) = \varepsilon(\sigma) \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

where $\varepsilon(\sigma) = \pm 1$, and $\varepsilon : S_n \rightarrow \{\pm 1\}$ is a homomorphism. $\varepsilon((12)) = -1$, so ε of any transposition is -1 , so $\ker \varepsilon = A_n$.

Thus $\sigma(\sqrt{D_f}) = \varepsilon(\sigma)\sqrt{D_f}$ for all $\sigma \in \text{Gal}(f)$; if $\text{Gal}(f) \subseteq A_n$ then $\sqrt{D_f} \in L^{\text{Gal}(L/K)} = K$, if not, this is not the case. \square

Now, we plow.

- 1 If $n = 1$, then $\text{Gal}(f) = 1$.
- 2 If $n = 2$, then $\text{Gal}(f) = S_2$.
- 3 If $n = 3$, then $\text{Gal}(f) \cong \begin{cases} A_3 & \text{if } D_f \text{ is a square} \\ S_3 & \text{else} \end{cases}$
- 4 If $n = 4$, then $\text{Gal}(f)$ can be:

- S_4
- A_4
- $C = \langle (1234) \rangle$, and its two conjugates in S_4
- $D_8 = \langle (1234), (13) \rangle$, the dihedral group of order 8, and its conjugates.
- $V_4 = \{1, (12)(34), (13)(24), (14)(23)\} \trianglelefteq A_4 \trianglelefteq S_4$.

Then $S_4/A_4 \cong \{\pm 1\}$, $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$, and $V_4 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, so this is still solvable. If D_f is a square, the Galois group is V_4 or A_4 . If it is not a square, the Galois group is either S_4 or a conjugate to C or D_8 .

We want to finish distinguishing the subcases for polynomials of order 4. For a quartic with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, we can define

$$\begin{aligned}\theta_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ \theta_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\ \theta_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3),\end{aligned}$$

giving us the resolvent cubic $h(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3) \in K[x]$. Let $\sigma \in \text{Gal}(f) \subseteq S_4$.

If $\sigma \in V$, then $\sigma(\theta_1) = \theta_1, \sigma(\theta_2) = \theta_2, \sigma(\theta_3) = \theta_3$.

If $\sigma = (123)$, then $\sigma(\theta_1) = \theta_2, \sigma(\theta_2) = \theta_3, \sigma(\theta_3) = \theta_1$. In the case where D_f is a square, $\text{Gal}(f)$ is V if h has 3 roots in K , and is A_4 if h is irreducible.

It's an important note that h is computable directly from f : if $f = x^4 + ax^2 + bx + c \in K[x]$, then $h = x^3 - 2ax^2 + (a^2 - 4c)x + b^2$.

If D is not a square, then $\text{Gal}(f) = S_3 \Rightarrow h$ is irreducible, and if $\text{Gal}(f)$ is conjugate to C or D_8 , then h has exactly one root in K . So all that's left is distinguishing C and D_8 . $C \cap A_4 = \{1, (13)(24)\}$, and $D_8 \cap A_4 = V$. So look over $K(\sqrt{D_f})$; if $\text{Gal}(f)$ is conjugate to C , then f factors into quadratics in the larger field. If $\text{Gal}(f)$ is conjugate to D_8 , f still doesn't factor.

Example. $f = x^4 + 5x + 5 \in \mathbb{Q}[x]$, which is irreducible. $D_f = 5 \cdot 55^2$, which is not a square! So $\text{Gal}(f)$ is S_4, C , or D_8 . Then $h = x^3 - 20x + 25 = (x + 5)(x^2 - 5x + 5)$, so $\text{Gal}(f) = C$ or D_8 . How does f factor over the bigger field $\mathbb{Q}(\sqrt{5})$? Turns out it factors as $(x^2 + \sqrt{5}x + \frac{5-\sqrt{5}}{2})(x^2 - \sqrt{5}x + \frac{5+\sqrt{5}}{2})$, so the Galois group is C .

△

9 March 3rd

9.1 Computing Galois groups over \mathbb{Q}

We will first discuss conjugacy classes of S_n , which are given by cycle decompositions or cycle type. Given $\sigma \in S_n$, we can assign a tuple $\sigma \mapsto (d_1, \dots, d_r)$ where $1 \leq d_1 \leq \dots \leq d_r$ are integers and $d_1 + \dots + d_r = n$. All that this means is that σ is the product of disjoint cycles of lengths d_1, d_2, \dots, d_r .

For example, given $(123)(45)(78) \in S_n$, we assign the tuple $(1, 2, 2, 3)$.

Theorem 9.1.1. *Fix a separable $f(x) \in \mathbb{Z}[x]$ of degree n . As usual, we can embed $\text{Gal}(f) = \text{Gal}(L/\mathbb{Q}) \hookrightarrow S_n$, where L is the splitting field of f over \mathbb{Q} . Take a prime $p \nmid D_f$. We have $f(x) \equiv f_1(x) \cdots f_r(x) \pmod{p}$, where each $f_i(x)$ is irreducible in $\mathbb{F}_p[x]$. Set d_i to be the degree of f_i , and we can assume that $d_1 \leq \dots \leq d_r$.*

Then $\text{Gal}(f) \hookrightarrow S_n$ contains an element with cycle type (d_1, \dots, d_r) .

Example. Let $f = x^5 - x + 1$; then $D_f = 19 \cdot 151$.

(mod 3): f is irreducible in $\mathbb{F}_3[x]$.

So $\text{Gal}(f) \hookrightarrow S_5$ has a 5-cycle.

(mod 7): $f \equiv (x^2 + x + 3)(x^3 + 6x^2 + 5x + 5) \pmod{7}$, where each term is irreducible.

So $\text{Gal}(f)$ contains an element of cycle type $(2, 3)$. Specifically, it's not contained in the alternating group. Also, this implies that $\text{Gal}(f)$ contains a transposition and a 3-cycle, by taking that element to the second and third powers.

In fact this is enough to show that $\text{Gal}(f) = S_5$. The size of the Galois group is certainly divisible by 2, by 3, and by 5, so it's divisible by 30. By conjugating the transposition by a 5-cycle, maybe multiple times, $\text{Gal}(f)$ contains two disjoint transpositions. These generate a copy of the Klein four group, so the size of $\text{Gal}(f)$ is divisible by 4 and thus by 60. But it's not contained in A_5 , so it must be all of S_5 (its intersection with A_5 has index one or two, but A_5 is simple so it must be index 1, so $A_5 \subset \text{Gal}(f)$, so $\text{Gal}(f) = S_5$).

Note that adding 21 to f does not change the Galois group, because it has the same reduction mod 3 and mod 7.

△

So now we're going to try to compute a bunch of Galois groups.

Example.

f	(1, 1, 1, 1, 1)	(1, 1, 1, 2)	(1, 1, 3)	(1, 4)	(1, 2, 2)	(2, 3)	(5)
$x^5 - x + 1$	0.008	0.083	0.166	0.249	0.124	0.166	0.200
$x^5 + 20x + 16$	0.016	0	0.333	0	0.250	0	0.399
$x^5 - 2$	0.05	0	0	0.5	0.249	0	0.199
$x^5 + x^4 + x^3 - x + 2$	0.082	0.333	0.166	0	0.257	0.166	0

The table is the proportion of primes $p \nmid D_f$ with $p \leq 10^7$ for which $f \pmod{p}$ has a given cycle type.

For example it looks like $\text{Gal}(x^5 + 20x + 16)$ is A_5 , because we haven't seen any odd cycle types, and have seen all the even ones. And, the discriminant is $2^{16}5^6$, which is a square, so

$\text{Gal}(f) \subseteq A_5$. But it contains a 5-cycle, a 3-cycle, and a (2, 2)-cycle. So 30 divides the order; A_5 has no subgroup of index 2, so it must be all of A_5 .

To calculate the others, observe that the transitive subgroups of S_5 (up to conjugation) are $S_5, A_5, C = \langle(12345)\rangle, D_{10} = \langle(12345), (25)(34)\rangle, F_{20} = \langle(12345), (2354)\rangle$. In this case, $|C| = 5, D_{10} = 10,$ and $F_{20} = 20$.

Now consider $f = x^5 - 2$. The Galois group has elements of order 4 and 5, so it's conjugate to F_{20} (although we still haven't ruled out S_5 ; maybe ten million isn't enough). One way of doing this is that it's solvable, so its Galois group isn't S_5 . You could also say that its splitting field has order 20.

Consider $f = x^5 + x^4 + x^3 - x + 2$. Seems pretty reducible based on the number of 5-cycles we found. It looks like the Galois group doesn't act transitively on the roots, so it's probably reducible. Turns out $f = (x^2 + x + 2)(x^3 - x + 1)$. As it turns out, $\text{Gal}(f) \cong S_2 \times S_3$.

The one thing that we haven't looked at is what these numbers mean. That concern is addressed by the following theorem.

△

Theorem 9.1.2 (Chebotarev). *Take f as before, with $\text{Gal}(f) \hookrightarrow S_n$. Fix a cycle type c of S_n . Then the quantity*

$$\frac{|\{p \leq x \mid p \nmid D_f, \text{ factorization of } f \pmod{p} \text{ gives } c\}|}{|\{p \leq x \mid p \nmid D_f\}|},$$

approaches

$$\frac{|\{\sigma \in \text{Gal}(f) \mid \sigma \mapsto c\}|}{|\{\text{Gal}(f)\}|}.$$

as $x \rightarrow +\infty$.

The proof uses complex analysis and is omitted here, so the theorem is a bit of a huge black box thing.

But one can check with the table! The numbers were all kinda predictable.

Example. $f = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$. For small p , $f \pmod{p}$ gives cycle types (1, 1, 1, 1, 1) and (5). We expect $\text{Gal}(f) = C$. (But it's not a proof! Based on these calculations, especially since Prof. Zywna checked the first ten million, we would be very very very surprised if the group were not C . But how do we show it?!)

To show that $\text{Gal}(f)$ is small, we define a new polynomial off of the roots $\alpha_1, \dots, \alpha_5$. Define

$$g(x) = \prod_{1 \leq i < j \leq 5} (x - (\alpha_i + \alpha_j)) \in \mathbb{Q}[x].$$

This has degree 10. It's sort of generally a problem that this degree is bigger than 5, which happens because the quintic is unsolvable, and we can't reduce to smaller polynomials.

For this example, if $\text{Gal}(f) = \langle(12345)\rangle$, then $(x - (\alpha_1 + \alpha_2))(x - (\alpha_2 + \alpha_3)) \cdots (x - (\alpha_5 + \alpha_1)) \in \mathbb{Q}[x]$, a degree five factor of $g(x)$. But for the other four cases, there is no factor of $g(x)$ of degree 5. For our f , $g(x) = x^{10} + \cdots + 1 = (x^5 + 2x^4 - 5x^3 - 13x^2 - 7x - 1)(x^5 + 2x^4 - 5x^3 - 2x^2 + 4x - 1)$, so it does factor, so $\text{Gal}(f) = C$.

△

Example. $f = x^7 - 7x + 3$. $D_f = 21^8$, a square, so that's something. It turns out you're missing lots of cycle types. In this case, which is difficult, $\text{Gal}(f)$ has order 168. The proportion of p for which $f \pmod{p}$ splits completely is $\approx 1/168$. The answer ends up being that $\text{Gal}(f) \cong \text{SL}_3(\mathbb{F}_2)$.

△

10 March 8th

Today's notes are courtesy of Oliver Wang.

10.1 Last Time

Example. We discussed at the end of last time the example $f = x^7 - 7x + 3 \in \mathbb{Q}[x]$, known as “Trinks’ Polynomial.” We claim that $\text{Gal}(f) \cong \text{SL}_3(\mathbb{F}_2) \curvearrowright \mathbb{F}_2^3 \setminus \{0\}$. Note that $\mathbb{F}_2^3 \setminus \{0\}$ has 7 elements, so $\text{SL}_3(\mathbb{F}_2) \hookrightarrow S_7$.

The technique is to let $\alpha_1, \dots, \alpha_7$ be roots of f . Then define the resolvent

$$P(x) = \prod_{1 \leq i < j < k \leq 7} (x - (\alpha_i + \alpha_j + \alpha_k)) \in \mathbb{Q}[x].$$

Then, using a computer, one can compute that $P(x) = (x^7 + 14x^6 - 42x^2 - 21x + 9)Q(x)$, where $Q(x)$ is an irreducible polynomial of degree 28, and the degree 7 polynomial is irreducible as well.

So, $\text{Gal}(f) \curvearrowright \{\alpha_1, \dots, \alpha_7\}$ transitively and $\text{Gal}(f) \curvearrowright \{\alpha_i + \alpha_j + \alpha_k \mid 1 \leq i < j < k \leq 7\}$ has two orbits, one of size 7 and one of size 28. Group theoretically, we can then show that $\text{Gal}(f) \leq S_7$ must be isomorphic to $\text{SL}_3(\mathbb{F}_2)$.

△

Example (Malle and Matzat). Let $f(x, t) = x^7 - 56x^6 + 509x^5 + 1190x^4 + 6356x^3 + 4536x^2 - 6804x - 5832 - tx^3(x + 1) \in \mathbb{Q}(t)[x]$. Let L be the splitting field of f over $\mathbb{Q}(t)$; then $\text{Gal}(L/\mathbb{Q}(t)) \cong \text{SL}_3(\mathbb{F}_2)$. One can plug in values for $t \in \mathbb{Q}$ into the polynomial; experimentally, for $a \in \mathbb{Z}$, $|a| \leq 1000$, $a \neq 0$, we have $\text{Gal}(f(x, a)) \cong \text{SL}_3(\mathbb{F}_2)$.

△

This technique corresponds to the following theorem of Hilbert.

Theorem 10.1.1 (Hilbert’s irreducibility theorem, 1892). *Let $K = \mathbb{Q}(t_1, \dots, t_n)$ with $n \geq 1$. Fix a polynomial $f(x, t_1, \dots, t_n) \in K[x]$. Set $G = \text{Gal}(f) = \text{Gal}(L/K)$, with L the splitting field of f over K . Then for infinitely many (in some sense the “most”) $(a_1, \dots, a_n) \in \mathbb{Q}^n$, $f(x, a_1, \dots, a_n) \in \mathbb{Q}[x]$ is well-defined and $\text{Gal}(f(x, a_1, \dots, a_n)) \cong G$.*

Example. Let $L = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ for $n \geq 2$. Then $S_n \curvearrowright L$, and L is an extension of $K = L^{S_n} = \mathbb{Q}(s_1, \dots, s_n)$, where s_i is the elementary symmetric polynomial. L is the splitting field of

$$f(x) = \prod_{i=1}^n (x - \alpha_i) \in K[x],$$

so by Hilbert's irreducibility theorem, for "most" $a_1, \dots, a_n \in \mathbb{Q}$, $\text{Gal}(x^n - a_1x^{n-1} + \dots + (-1)^n a_n) = S_n$.

As a corollary, there exists a Galois extension L/\mathbb{Q} with $\text{Gal}(L/\mathbb{Q}) \cong S_n$.

△

Example. There exists a Galois extension $L/\mathbb{Q}(t)$ with Galois group isomorphic to the monster group, so there exists L/\mathbb{Q} with $\text{Gal}(L/\mathbb{Q})$ congruent to the monster group.

This leads to the inverse Galois problem: does every finite group G occur as the Galois group of some extension of \mathbb{Q} ? this is unknown for $G = \text{SL}_3(\mathbb{F}_8)$, which is simple. However, Shafarevich proved it for solvable groups, and it is known for $\text{SL}_2(\mathbb{F}_p)/\{\pm I\}$.

△

For G a finite group, there exists an n with $G \hookrightarrow S_n$. Then $G \curvearrowright \mathbb{Q}(x_1, \dots, x_n)$ with $\mathbb{Q}(x_1, \dots, x_n)$ an extension of $\mathbb{Q}(x_1, \dots, x_n)^G$. The problem is, that this is not necessarily the same as $\mathbb{Q}(t_1, \dots, t_n)$ with t_i 's independent.

The idea of constructing extensions of $\mathbb{Q}(t)$ is to construct extensions of $\mathbb{C}(t)$ and then "descend." Another technique for a finite group G is to let X be a Riemann surface and let S be a finite set of points, with a cover $\pi : X \rightarrow \mathbb{P}^1(\mathbb{C}) \setminus S$. This can be constructed so that G is the group of automorphisms of the cover π , and $|G| = \deg \pi$, so we get an extension of the function fields $\mathbb{C}(x)/\mathbb{C}(t)$ with Galois group G .

10.2 Infinite Galois Theory

Recall that L/K is *Galois* if it is algebraic, normal, and separable. But if L/K is infinite, then the set $\{H \mid H \leq \text{Gal}(L/K)\}$ may be too big for there to be a bijection

$$\{F \mid K \leq F \leq L\} \leftrightarrow \{H \mid H \leq \text{Gal}(L/K)\},$$

since the sets may have different cardinality.

Example. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots)$ as an extension over \mathbb{Q} . Then $\text{Gal}(L/\mathbb{Q}) \cong \prod_p \{\pm 1\}$, with an isomorphism wherein $\sigma \mapsto (\varepsilon_p)_p$, and $\sigma(\sqrt{p}) = \varepsilon_p \sqrt{p}$.

We don't get bijections here, but if we give $\text{Gal}(L/K)$ a topology and look only at closed subgroups of $\text{Gal}(L/K)$, then we get bijections. So what's the topology? The idea is that for $\sigma, \tau \in \text{Gal}(L/K)$, σ and τ are "close" if $\sigma|_F = \tau|_F$ for a "large" finite extension F/K , $F \subseteq L$.

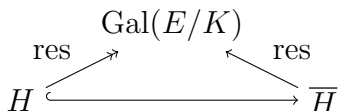
Let $\text{Gal}(L/K)$ be the topological group with the coarsest topology such that $\text{Gal}(L/F)$ with F/K finite are open. (so then $\sigma \text{Gal}(L/F)$ is also open). Then $\sigma\tau^{-1} \in \text{Gal}(L/F)$ if and only if $\sigma|_F = \tau|_F$. This leads us to the following general theorem about this construction.

△

Theorem 10.2.1. *The Fundamental Theorem holds with this topology.*

One issue that arises with this topology is the question of considering a subgroup H as opposed to its closure \overline{H} . This closure is also a subgroup; it turns out that $L^{\overline{H}} = L^H$.

Also, for E/K a finite Galois extension, consider following diagram:



11 March 10th

11.1 A New Topic: Representation Theory of finite groups

Let G be a finite group.

We have been studying the actions of G on fields L , where $G \rightarrow \text{Aut}(L)$ a homomorphism. In this case the extension L/L^G is Galois with Galois group G .

In this section of the course, instead of studying the actions of G on fields, we study the actions of G on vector spaces. Let V be a vector space over a field K (often $K = \mathbb{C}$).

Definition 11.1.1. A *representation* of G on V is a group action that respects the vector space structure.

Equivalently, it is a homomorphism $\rho : G \rightarrow \text{GL}(V)$, with $\text{GL}(V)$ the group of K -linear automorphisms of V .

We will suppress ρ when clear, and simply denote $gv = g \cdot v = \rho(g)v$ for $g \in G$ and $v \in V$. But, we may have to return to the homomorphism notation for clarity if there are multiple representations floating around.

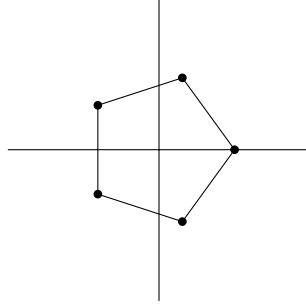
Definition 11.1.2. The *degree* of a representation is $\dim_K V$.

Example. Consider representations of degree 1. In this case, we have $G \rightarrow \text{GL}(V)$, with V one-dimensional, so $\text{GL}(V) = K^\times$.

If $G = S_n$, we have the representation $\rho_1 : S_n \rightarrow K^\times$ with $\rho_1(\sigma) = 1$, the trivial representation. There's also $\rho_2(\sigma) = \varepsilon(\sigma)$, where $\varepsilon(\sigma)$ is multiplication by the sign of σ .

△

Example. If $G = D_{2n} = \langle r, s \mid r^n = s^2 = 1, srs^{-1} = r^{-1} \rangle$ and $K = \mathbb{R}$. Let $V = \mathbb{R}^2$, and consider the regular n -gon (below is $n = 5$) centered at $(0, 0)$. We have $\rho : D_{2n} \rightarrow \text{GL}_2(\mathbb{R})$, where r acts by rotation by $\frac{2\pi}{n}$, and s flips across the x -axis.



In terms of explicit linear transformations, this gives

$$\rho(r) = \begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix}$$

and

$$\rho(r) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

This is a degree 2 representation, which is “irreducible,” i.e. there are no stable one-dimensional subspaces. Up to isomorphism, this is the only degree 2 representation of D_{2n} .

△

Wait, but what kind of isomorphism? What do we mean by the same?

Definition 11.1.3. Consider two representations $\rho : G \rightarrow \text{GL}(V)$ and $\rho' : G \rightarrow \text{GL}(W)$, for V and W vector spaces. Then ρ and ρ' are *isomorphic* (or *equivalent*, or in the world of Dummit and Foote and possibly them alone, *similar*) if there exists an isomorphism $f : V \xrightarrow{\sim} W$ such that the following diagram commutes for all $g \in G$.

$$\begin{array}{ccc} V & \xrightarrow{\sim} & W \\ g \downarrow & & \downarrow g \\ V & \xrightarrow{\sim} & W \end{array}$$

In other words, for all $g \in G$, for all $v \in V$, $f(gv) = gf(v)$, or $f \circ \rho(g) = \rho'(g) \circ f$.

Choose a basis $V \cong K^n$. Then $\rho : G \rightarrow \text{GL}_n(K)$; any two such representations are isomorphic if and only if they are conjugate by a matrix $A \in \text{GL}_n(K)$. We can define the *character* of ρ , which is the map $\chi : G \rightarrow K$ given by $\chi(g) = \text{Tr}(\rho(g))$. Note that χ depends only on the isomorphism class of ρ .

Later we will show that for $K = \mathbb{C}$, a representation is determined up to isomorphism by its character, a very exciting theorem that we will prove next week. This is surprising. It seems like taking the trace would throw away a lot of information. But characters can be really important! For the monster group, people wrote down its characters before they proved it was a group. So it can sometimes be more tractable. (It’s just like a fairy tale. The monster was tamed by the main characters!)

Example. We consider permutation representations. For an action $G \curvearrowright X$, with X a set, let $V = KX$, a formal vector space over K with basis X . In other words, the elements of V are of the form $\sum_{x \in X} a_x \cdot x$, for $a_x \in K$. Then G acts on V via

$$g \left(\sum_{x \in X} a_x \cdot x \right) = \sum_{x \in X} a_x \cdot gx.$$

For example, $S_3 \curvearrowright X = \{1, 2, 3\}$ by permuting. In this case $V = Ke_1 \oplus Ke_2 \oplus Ke_3 = K^3$, so we have a representation $\rho : S_3 \rightarrow \text{GL}_3(K)$ given by permutation matrices, where

$$\rho((12)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho((123)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Are there non-trivial subspaces of V that are stable under this action? Yes. Consider $W = K(e_1 + e_2 + e_3)$. This is a G -invariant subspace. Just as with Galois theory, we denote this by V^G , the subspace of elements of V that are fixed by G .

There is one more fixed subspace, defined by $W' = \{ae_1 + be_2 + ce_3 \mid a, b, c \in K, a + b + c = 0\}$. This is a degree-2 subspace that is closed under the action. We find that $V = W \oplus W'$, if the characteristic of K is not 3.

△

Definition 11.1.4. We say a subspace W of V is G -invariant (or G -stable) if $g(W) \subseteq W$ for all $g \in G$.

The basic starting point in representation theory is then the following theorem.

Theorem 11.1.5 (Maschke). *Let G be a finite group and let V be a representation of G . Assume that $\text{char } K \nmid |G|$. Then for any G -invariant subspace $W \subseteq V$ there is a G -invariant subspace $W' \subseteq V$ such that*

$$V = W \oplus W'.$$

Proof. Fix a projection $f : V \rightarrow V$ of V onto W , so that $f(V) \subseteq W$ and $f(w) = w$ for $w \in W$.

The linear map f need not respect the G -action; we will fix this by “averaging.” Define $F : V \rightarrow W$ given by

$$F(v) = \frac{1}{|G|} \sum_{g \in G} g(f(g^{-1}v)).$$

Note that this is where we use that the characteristic doesn't divide $|G|$. Dividing by zero is unadvisable.

F is a projection onto W :

- For $v \in V$, $f(g^{-1}v) \in W$ for all $g \in G$; then $gf(g^{-1}v) \in W$ because W is G -invariant. Since W is a subspace, then $F(v) \in W$.

- For $w \in W$, $g^{-1}w \in W$ for all $g \in G$, so $f(g^{-1}w) = g^{-1}w$, so for all $g \in G$, $gf(g^{-1}w) = w$. Then $F(w) = \frac{1}{|G|}|G|w = w$.

But F has a new property, that $F(hv) = hF(v)$ for all $v \in V$ and $h \in G$. In other words, F plays nice with the group action. How do we show this? Let $h \in G$ be arbitrary. Then

$$\begin{aligned} F(hv) &= \frac{1}{|G|} \sum_{g \in G} hg \cdot f((hg)^{-1} \cdot hv) \\ &= \frac{1}{|G|} \sum_{g \in G} hg \cdot f(g^{-1}v) \\ &= hF(v). \end{aligned}$$

OK, great. We're pretty much done. Define $W' = \ker F$. Then $V = W \oplus W'$ from linear algebra. All that remains is to show that W' is a G -invariant subspace. For $w \in W'$ and $g \in G$, $F(gw) = gF(w) = g \cdot 0 = 0$, so $gw \in W'$ as well, and we're done. \square

Definition 11.1.6. We say that a representation V of G is *irreducible* (or *simple*) if $V \neq 0$ and the only G -invariant subspaces are 0 and V .

Corollary 11.1.7. If V is finite dimensional over K and $\text{char } K \nmid |G|$, then V breaks up into irreducibles, i.e.

$$V = V_1 \oplus \cdots \oplus V_r,$$

where the V_i are irreducible G -invariant subspaces.

Alternatively, $V \cong V_1^{a_1} \oplus \cdots \oplus V_r^{a_r}$ where V_i are irreducible representations of G and are pairwise non-isomorphic, with $a_i \geq 1$ integers.

Later, we will show that this decomposition is unique up to reordering and replacing V_i by an isomorphic representation.

12 March 15th

12.1 Last Time

Fix a field K . A *representation* of a finite group G on a vector space V over K is a group action of G on V that respects the vector space structure. Equivalently, it is just a homomorphism $\rho : G \rightarrow \text{GL}(V)$.

Now we introduce the same topic from another view, looking at group rings.

12.2 Group Rings

Definition 12.2.1. The *group ring* $KG = K[G]$ of G over K is as an additive group the K vector space with basis G , so that elements are of the form $\sum_{g \in G} a_g \cdot g$, with $a_g \in K$. We

define multiplication by saying that

$$\left(\sum_{g \in G} a_g \cdot g \right) \cdot \left(\sum_{h \in G} b_h \cdot h \right) = \sum_{g, h \in G} a_g b_h \cdot gh.$$

KG is a K -algebra, with KG commutative if and only if G is abelian. Also, KG has zero divisors if G is finite and $G \neq 1$. To see this, take $h \in G - \{1\}$. Then

$$\begin{aligned} (h - 1) \sum_{g \in G} g &= \sum_{g \in G} hg - \sum_{g \in G} g \\ &= \sum_{g \in G} g - \sum_{g \in G} g = 0. \end{aligned}$$

There is a correspondence

$$\{ \text{reps of } G \text{ on } V \} \longleftrightarrow \{ KG\text{-modules} \},$$

where a representation of G on V corresponds to submodule structure given by

$$\left(\sum_{g \in G} a_g g \right) v = \sum_{g \in G} a_g \cdot (gv),$$

and in the other direction, we define the representation where for $g \in G$, $g \cdot v = gv$, using the KG -action.

This correspondence goes pretty far. V is finite dimensional over K if and only if the module is finitely generated. Then we have the following table of correspondences:

Representations	Modules
G -invariant subspaces	KG -submodules
irreducible	simple
isomorphisms	isomorphisms

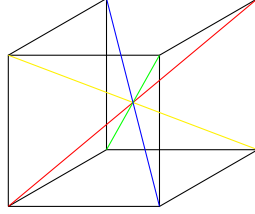
We will later describe the structure of KG for characteristic of K not dividing $|G|$.

Example. Let $G = D_8$, and let $K = \mathbb{C}$. We'll see that $\mathbb{C}G \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$, so D_8 has 5 irreducible representations over \mathbb{C} of degree 1, 1, 1, 1, 2. Also, $|D_8| = \dim_{\mathbb{C}} \mathbb{C}G = 1^2 + 1^2 + 1^2 + 1^2 + 2^2$.

△

Example (Symmetries of a cube). Consider a cube in \mathbb{R}^3 with vertices $(\pm 1, \pm 1, \pm 1)$. By symmetries, we mean physical symmetries, i.e. rotations. No reflecting along some line.

The symmetry group has order 24, and is S_4 , which can be seen by looking at diagonals. The symmetries permute the four long diagonals, colored red, blue, yellow, and green in the picture below:



We then have a representation $\rho : S_4 \hookrightarrow \text{GL}_3(\mathbb{R})$, based on which permutation of the diagonals sends what basis vectors where, with

$$\rho((1234)) = \begin{pmatrix} 0 & -1 & \\ 1 & 0 & \\ & & 1 \end{pmatrix}$$

$$\rho((1243)) = \begin{pmatrix} 0 & -1 & \\ & 1 & \\ 1 & 0 & \end{pmatrix}$$

$$\rho((132)) = \rho((1234)(1243)) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}$$

The image of ρ is the set of signed permutation matrices in $\text{GL}_3(\mathbb{R})$, with determinant 1 (because we're not reflecting). The *character* is the map $\chi = \text{tr} \circ \rho : S_4 \rightarrow \mathbb{R}$, so we can do the following computations of characters of elements:

Conj. class	1	(12)(34)	(12)	(1234)	(123)
χ	3	-1	-1	1	0

We'll see later that χ determines ρ up to isomorphism.

△

For now, note that all vector spaces V are finite dimensional, and the characteristic of K is taken to be not dividing $|G|$. Last time, recall that we saw the following theorem of Mashke:

Theorem 12.2.2. *If V is a representation of G and W is a G -invariant subspace, then there is a G -invariant subspace W' of V such that $V = W \oplus W'$.*

From this it follows that $V = V_1 \oplus \dots \oplus V_r$, with each V_i irreducible. We claim and will see shortly that the V_i are unique up to isomorphism and reordering. This uniqueness ends up being very helpful for using representation theory as a lens to look at modules via a group, or to look at groups via their representations. For the next little bit, we will sweat and toil at the noble altar of uniqueness.

For now, let V, W be representations of G . Then $\text{Hom}_G(V, W) = \text{Hom}_{KG}(V, W)$, where we define $\text{Hom}_G(V, W)$ to be K -linear maps $V \rightarrow W$ that respect the group law, ie. linear maps

f with $f(gv) = gf(v)$. In the special case when $V = W$, we have $\text{Hom}_G(V, V) = \text{End}_G(V)$. (Note that $\text{End}_G(V)$ is a ring with multiplication being composition.) We begin with Schur's Lemma, one of those super-useful results that will always be and has always been a lemma (see also: Zorn, Jordan).

Lemma 12.2.3 (Schur's Lemma). *Let V and W be irreducible representations of G . Let $f : V \rightarrow W$ be a homomorphism of KG -modules. Then*

- a) *either f is an isomorphism or $f = 0$, and*
- b) *$\text{End}_G(V)$ is a division algebra with K in the center, that is finite dimensional over K , and*
- c) *if $V = W$ and K is algebraically closed, then $f = \lambda I$, for $\lambda \in K$.*

Proof. a) $\ker(f)$ is a G -invariant subspace of V , and $\text{im}(f)$ is a G -invariant subspace of W .

Since V and W are irreducible, either $\ker(f) = V$ or $\text{im}(f) = 0$, in which case $f = 0$, or $\ker(f) = 0$ and $\text{im}(f) = W$, in which case f is an isomorphism.

b) $\dim_K \text{End}_G(V) \leq \dim_K \text{End}(V) = (\dim V)^2 < \infty$. This is then a {worthy, straightforward} exercise.

c) Let D be a division algebra with K in its center and of finite dimension over K . We claim that $D = K$. Take any $\alpha \in D$; then $K(\alpha) \subseteq D$. Moreover, $[K(\alpha) : K]$ is finite, and $\alpha \in \text{End}_G(V) \subseteq \text{End}(V) \cong M_n(K)$, so we get $p(\alpha) = 0$ where p is the characteristic polynomial of α . But K is algebraically closed, and $K(\alpha)/K$ is finite, so $K(\alpha) = K$, so $\alpha \in K$. Thus $D = K$, and this completes the proof. □

Example. Let V be irreducible. If $K = \mathbb{C}$, then $\text{End}_G(V) = \mathbb{C}$, and if $K = \mathbb{R}$, then $\text{End}_G(V)$ ends up being \mathbb{R}, \mathbb{C} , or \mathbb{H} . △

Example. Consider the representation $\rho : \mathbb{Z}/3\mathbb{Z} \rightarrow \text{GL}_2(\mathbb{R})$ given by rotation by $\frac{2\pi}{3}$. Explicitly,

$$\rho(1) = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix},$$

and

$$\rho(2) = \rho(1)^2 = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}.$$

ρ is irreducible. But is it irreducible as a representation over \mathbb{C} , with $\rho : \mathbb{Z}/3\mathbb{Z} \rightarrow \text{GL}_2(\mathbb{R}) \subseteq \text{GL}_2(\mathbb{C})$? No. It turns out you can diagonalize, to get eigenvalues ζ_3 and ζ_3^{-1} .

Up to isomorphism, $\rho : \mathbb{Z}/3\mathbb{Z} \rightarrow \mathrm{GL}_2(\mathbb{C})$, with $1 \mapsto \begin{pmatrix} \zeta_3 & \\ & \zeta_3^{-1} \end{pmatrix}$, so it breaks up into two one-dimensional pieces. ρ is the direct sum of two degree 1 representations, given by

$$\begin{aligned} \psi : \mathbb{Z}/3\mathbb{Z} &\rightarrow \mathbb{C}^\times \\ k &\mapsto \zeta_3^k \\ \bar{\psi} : \mathbb{Z}/3\mathbb{Z} &\rightarrow \mathbb{C}^\times \\ k &\mapsto \zeta_3^{-k}. \end{aligned}$$

Over $K = \mathbb{R}$, the endomorphisms of ρ that respect the $\mathbb{Z}/3\mathbb{Z}$ -action are $\mathbb{R} \oplus \mathbb{R} \cdot \rho(1) \cong \mathbb{C}$.

△

Now let V be a representation of G , so that $V = V_1 \oplus \cdots \oplus V_r$. We show that this decomposition is unique up to isomorphism and reordering. Let W be an irreducible representation of G , and consider

$$\mathrm{Hom}_G(W, V) = \bigoplus_{i=1}^r \mathrm{Hom}_G(W, V_i),$$

but since W and V_i are irreducible, each term is 0 if $W \not\cong V_i$. So

$$\mathrm{Hom}_G(W, V) = \bigoplus_{V_i \cong W} \mathrm{Hom}_G(W, V) \cong \bigoplus_{V_i \cong W} \mathrm{End}_G(W).$$

Comparing dimensions, we have $\dim_k \mathrm{Hom}_G(W, V) = |\{i : 1 \leq i \leq r, V_i \cong W\}| \cdot \dim_k \mathrm{End}_G(W)$, so the number of V_i 's that are isomorphic to W is

$$\frac{\dim_k \mathrm{Hom}_G(W, V)}{\dim_k \mathrm{End}_G(W)},$$

which is independent of how we decomposed V into irreducibles. So that's our uniqueness statement.

Characters, seen next time, will be a way of approaching that dimension fraction, of how many V_i 's are isomorphic to W , in a hands-on way.

13 March 17th

13.1 Representations and their Characters

Our set up was and is that K is a field and G is a finite group (with the assumption that the characteristic of K doesn't divide $|G|$), and V is a representation of G with $\dim_k V$ finite. So, there is a homomorphism $\rho : G \rightarrow \mathrm{GL}(V)$, the space of K -linear automorphisms of V .

Then the *character* of ρ is the map $\chi : G \rightarrow K$, where $\chi(g) = \mathrm{tr}(\rho(g))$, which is unique up to isomorphism class. Also, $\chi(hgh^{-1}) = \chi(g)$ for all $g, h \in G$, so χ is what is known as a "class function" of G .

Fact 13.1.1. χ is also a class function of G , on account of how shiny, stylish, and socially adept it is.

Our goal will be to show that if $K = \mathbb{C}$, or has characteristic 0, then χ determines ρ up to isomorphism. This doesn't work in characteristic p , because for a field K , consider the representations of G into K and K^{p+1} with trivial action. Then $\chi(g) = 1$ in the first case, and $\chi(g) = p + 1 = 1$ in the second case, so already this doesn't determine ρ .

For the character of $G \curvearrowright V$, we'll use the notation χ_V , or equivalently χ_ρ .

Let $V \cong V_1 \oplus \cdots \oplus V_r$, where each V_i is irreducible; recall that this decomposition is unique up to isomorphism and reordering, as we discussed last time. For W an irreducible representation of G , we had the formula

$$\#\{i \in \{1, \dots, r\} \mid V_i \cong W\} = \frac{\dim_k \text{Hom}_G(W, V)}{\dim_k \text{End}_G(W)}$$

The questions we're answering now are then "How many irreducible representations are there?," and "What are they/can you find them?"

13.1.1 Interlude: Constructing New Representations

Let V, W be representations of G , with $\rho : G \rightarrow \text{GL}(V)$ and $\rho' : G \rightarrow \text{GL}(W)$.

Direct sum: We have $G \curvearrowright V \oplus W$, with $g(v, w) = (gv, gw)$. In terms of characters, this gives

$$\chi_{V \oplus W} = \chi_V + \chi_W,$$

or "direct sums turn into sums" for characters. This can be understood via the matrices; the image of g in the direct sum is

$$\begin{pmatrix} \rho(g) & 0 \\ 0 & \rho'(g) \end{pmatrix},$$

so the traces add.

Tensor products: $V \otimes W = V \otimes_K W$. If $\{e_i\}$ is a basis of V and $\{f_j\}$ is a basis of W , then $\{e_i \otimes f_j\}$ is a basis of $V \otimes W$, and $\dim V \otimes W = \dim V \cdot \dim W$. There's a group action of G on $V \otimes W$ in the natural manner: for a simple tensor $v \otimes w$, we have $g \cdot (v \otimes w) = gv \otimes gw$, and we extend bilinearly to all of $V \otimes W$.

In terms of characters, we have

$$\chi_{V \otimes W} = \chi_V \cdot \chi_W,$$

or "tensor products turn into products" for characters. To see the idea of why this is true, let $A \in \text{End}(V)$ and let $B \in \text{End}(W)$ be diagonalizable. Then we have v_1, \dots, v_n eigenvectors of A , with $Av_i = \lambda_i v_i$, and w_1, \dots, w_m eigenvectors of B , with $Bw_j = \mu_j w_j$. For $e_i \otimes f_j$ our basis of $V \otimes W$,

$$(A \otimes B)(e_i \otimes f_j) = Ae_i \otimes Bf_j = \lambda_i \mu_j e_i \otimes f_j,$$

so to compute the eigenvalues of $A \otimes B$ we have the sum of all $\lambda_i \mu_j$, which is $(\sum_i \lambda_i) \left(\sum_j \mu_j \right) = \text{tr} A \text{tr} B$.

Remark. This whole exercise is one of the many that can be done to motivate the notation \otimes for tensor products and \oplus for direct sums, along with their naming terminology. Whee!

Duals: Let $V^* = \text{Hom}_K(V, K)$. For $g \in G$, $f \in V^*$, and $f : V \rightarrow K$, we can define

$$(gf)(v) = f(g^{-1}v),$$

which defines a left action $G \curvearrowright V^*$. Let $A \in \text{End}(V)$; then we have the corresponding $A^* \in \text{End}(V^*)$, with $A^*f = f \circ A$. Fixing a basis e_1, \dots, e_n of V , we get the dual basis e_1^*, \dots, e_n^* of V^* , where

$$e_i^*(e_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else} \end{cases} = \delta_{ij}.$$

One can check that with respect to these bases, A^* is the transpose of A . So

$$\chi_{V^*}(g) = \chi_V(g^{-1}).$$

Let's look specifically at the case when $K = \mathbb{C}$. In this case, $\chi_V(g) = \lambda_1 + \dots + \lambda_n$, where the λ_i are eigenvalues of $\rho(g)$, which in fact must be roots of unity because $\rho(g)$ has finite order. Then

$$\begin{aligned} \chi_V(g^{-1}) &= \lambda_1^{-1} + \dots + \lambda_n^{-1} \\ &= \overline{\lambda_1} + \dots + \overline{\lambda_n} \\ &= \overline{\chi_V(g)}. \end{aligned}$$

So if $K = \mathbb{C}$, $\chi_{V^*} = \overline{\chi_V}$.

Hom: We define the action $G \curvearrowright \text{Hom}(V, W)$ by saying that for $g \in G$ and for $f : V \rightarrow W$,

$$\begin{aligned} (g \cdot f)(v) &= g \cdot f(g^{-1}v) \\ &= (\rho'(g) \circ f \circ \rho(g)^{-1})(v). \end{aligned}$$

Observe that there is an isomorphism of K -vectorspaces:

$$\begin{aligned} V^* \otimes W &\xrightarrow{\sim} \text{Hom}(V, W) \\ f \otimes w &\mapsto (v \mapsto f(v)w). \end{aligned}$$

Exercise: Verify that this is an isomorphism, and that defining $G \curvearrowright \text{Hom}(V, W)$ via this isomorphism would give the same result as our definition above.

Then in terms of characters,

$$\begin{aligned} \chi_{\text{Hom}(V, W)}(g) &= \chi_{V^* \otimes W}(g) \\ &= \chi_{V^*}(g) \cdot \chi_W(g) \\ &= \chi_V(g^{-1}) \chi_W(g) \\ &= \overline{\chi_V(g)} \chi_W(g), \text{ when } K = \mathbb{C}. \end{aligned}$$

So, now that we know arguably enough ways to construct representations and what that does to characters, we have the following theorem.

Theorem 13.1.2. *Let V, W be irreducible representations of G with $K = \mathbb{C}$. Then*

$$\frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_W(g)} = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{otherwise.} \end{cases}$$

For generic K , replace $\overline{\chi_W(g)}$ with $\chi_W(g^{-1})$ and replace 1 for the case when $V \cong W$ with $\dim_K \text{End}_G(W)$.

Before we prove this, we will need the following lemma.

Lemma 13.1.3. *Let V be a representation of G . Then*

$$\frac{1}{|G|} \sum_{g \in G} \chi_V(g) = \dim_K V^G,$$

where V^G is the subspace of V fixed by G .

Proof. Define $f : V \rightarrow V$ by

$$f(v) = \frac{1}{|G|} \sum_{g \in G} gv,$$

or $f = \frac{1}{|G|} \sum_{g \in G} \rho(g)$. Then

$$\text{tr}(f) = \frac{1}{|G|} \sum_{g \in G} \text{tr}(\rho(g)) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g).$$

We claim that f is a projection of V onto V^G ; it is a straightforward exercise to show that for $v \in V$, $f(v) \in V^G$, and for $v \in V^G$, $f(v) = v$. So the trace of f is $\dim_K V^G$, since

$$f = \begin{pmatrix} I_{V^G} & 0 \\ 0 & 0 \end{pmatrix},$$

so we're done. □

OK, now we're ready for the theorem.

Proof of theorem.

$$\begin{aligned} \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_W(g)} &= \frac{1}{|G|} \sum_{g \in G} \chi_{\text{Hom}(W, V)}(g) \\ &= \dim_K \text{Hom}(W, V)^G, \text{ by the lemma.} \end{aligned}$$

Our action of G on $\text{Hom}(W, V)$ was $(gf)(v) = gf(g^{-1}v)$. so $f(v) = (gf)(v)$ if and only if $g^{-1}f(v) = f(g^{-1}v)$. So $f \in \text{Hom}(W, V)^G \iff f \in \text{Hom}_G(W, V)$, giving us that

$$\frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_W(g)} = \dim_K \text{Hom}_G(W, V).$$

By Schur's Lemma, for the complex numbers, the RHS is 1 if $V \cong W$ and 0 otherwise, just as desired. □

Let \mathcal{C} be the set of *class functions* of G over \mathbb{C} , or the set $\{f : G \rightarrow \mathbb{C} \mid f(hgh^{-1}) = f(g) \forall g, h \in G\}$. For example, $\chi_V \in \mathcal{C}$. Then \mathcal{C} is a complex vector space. We can assign it with a Hermitian form $\langle \cdot, \cdot \rangle : \mathcal{C} \times \mathcal{C} \rightarrow \mathbb{C}$, where

$$\langle f, f' \rangle = \frac{1}{|G|} \sum_{g \in G} f(g) \overline{f'(g)}.$$

For V_1, \dots, V_m irreducible representations of G over \mathbb{C} up to isomorphism, our theorem tells us that $\chi_{V_1}, \dots, \chi_{V_m}$ are *orthonormal* in \mathcal{C} , i.e. $\langle \chi_{V_i}, \chi_{V_j} \rangle = \delta_{ij}$.

Remark. $\dim_{\mathbb{C}} \mathcal{C}$ is the number of conjugacy classes of G ; call it r . In particular, this means that m , the number of irreducible representations of G over \mathbb{C} , is at most r . We implicitly assumed there were finitely many; it turns out there are only finitely many, and we have an upper bound! Next week, we'll show that the upper bound is exact.

Let V be a (not necessarily irreducible) representation of G (over \mathbb{C}); we now look at $\chi_V : G \rightarrow \mathbb{C}$. $V \cong V_1^{a_1} \oplus \dots \oplus V_m^{a_m}$, where V_i and V_j are distinct, and the integers $a_i \geq 0$ are unique. Then

$$\chi_V = \sum_{i=1}^m a_i \chi_{V_i},$$

and for $1 \leq j \leq m$,

$$\langle \chi_V, \chi_{V_j} \rangle = \sum_{i=1}^m a_i \langle \chi_{V_i}, \chi_{V_j} \rangle = a_j.$$

This is really useful! An easy way to compute the a_i 's. This also gives us a notion of size:

$$\langle \chi_V, \chi_V \rangle = \sum_{i=1}^m \sum_{j=1}^m a_i a_j \langle \chi_{V_i}, \chi_{V_j} \rangle = \sum_{i=1}^m a_i^2.$$

Another consequence is that this is a nice way to check irreducibility.

Corollary 13.1.4. χ_V is irreducible (equivalently, V is irreducible) if and only if $\langle \chi_V, \chi_V \rangle = 1$.

The main use is that this is an easily checkable criterion, which we'll verify next time by checking the criterion for a lot of examples!

14 March 22nd

14.1 Complex Character Theory, continued

Today, all representations of G are finite dimensional vector spaces over $K = \mathbb{C}$, and just like last time G is finite. Given a representation V of G with $\rho : G \rightarrow \text{GL}(V)$, its character is the map $\chi = \chi_V = \chi_\rho : G \rightarrow \mathbb{C}$ with $g \mapsto \text{tr}(\rho(g))$. These characters are examples of class

functions, or maps $G \rightarrow \mathbb{C}$ that only care about conjugacy class. On \mathcal{C} , we have a Hermitian form given by

$$\langle f, f' \rangle = \frac{1}{|G|} \sum_{g \in G} f(g) \overline{f'(g)}.$$

Let V_1, \dots, V_m be the irreducible representations of G , up to isomorphism, and define $\chi_i = \chi_{V_i}$; then we saw that $\langle \chi_i, \chi_j \rangle = \delta_{ij}$. So if $V \cong V_1^{a_1} \oplus \dots \oplus V_m^{a_m}$, with $a_i \geq 0$ integers, then $\chi_V = \sum_{i=1}^m a_i \chi_i$. Furthermore,

$$\langle \chi_V, \chi_j \rangle = \sum_{i=1}^m a_i \langle \chi_i, \chi_j \rangle = a_j,$$

and $\langle \chi, \chi \rangle = \sum_{i=1}^m a_i^2$, so in particular χ is irreducible if and only if $\langle \chi, \chi \rangle = 1$.

If m is the number of irreducible representations of G up to isomorphism, then $m \leq \dim_{\mathbb{C}} \mathcal{C}_G = r$, the number of conjugacy classes of G . We claim that $m = r$, in fact.

Example (Key example: Regular representations.). Let $R = \mathbb{C}G$, the group ring, which acts on itself by left multiplication. Then we have $\rho : G \rightarrow \text{GL}(\mathbb{C}G)$, and we can look at $\chi_{reg} : G \rightarrow \mathbb{C}$. In this case

$$\chi_{reg}(g) = \text{tr}(\rho(g)) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{else} \end{cases},$$

where we know that $\chi_{reg}(g) = 0$ if $g \neq 1$ because g acts on G by left multiplication and fixes no elements; with respect to the basis G , $\rho(g)$ is a permutation matrix with 0's all down the diagonal.

Now let χ_i be an irreducible character. Then

$$\langle \chi_{reg}, \chi_i \rangle = \frac{1}{|G|} \left(\chi_{reg}(1) \overline{\chi_i(1)} + \sum_{g \neq 1} \chi_{reg}(g) \overline{\chi_i(g)} \right) = \chi_i(1),$$

which is the degree of the irreducible representation V_i . In particular, $\chi_{reg} = \sum_{i=1}^m \chi_i(1) \chi_i$, so

$$\mathbb{C}G \cong V_1^{\chi_1(1)} \oplus \dots \oplus V_m^{\chi_m(1)}.$$

In particular, all irreducible representations show up! And each one shows up with the multiplicity equal to the dimension of V_i over \mathbb{C} .

△

Example. Let $G = S_3$; find the irreducible characters. To do this, we draw a character table:

Conj. classes	1	(12)	(123)
sizes	1	3	2
χ_1 (“trivial”)	1	1	1
$\chi_2 = \varepsilon$ (“sign”)	1	-1	1
χ_3	2	0	-1

We can figure out the elusive χ_3 , because $\chi_{reg} = \chi_1 + \chi_2 + 2 \cdot \chi_3$, so we can solve for it in terms of the regular representation and the other characters. We also saw χ_3 before: it appears because $S_3 \cong D_6 \curvearrowright \mathbb{C}^2$.

△

We now proceed to look at the structure of the ring $\mathbb{C}G$. Let $\mathbb{C}G \curvearrowright V_1 \oplus \cdots \oplus V_m$. This is a faithful action, i.e. $\alpha, \beta \in \mathbb{C}G$ act the same if and only if $\alpha = \beta$, because $\mathbb{C}G$ acts faithfully on itself. This gives us a map

$$\mathbb{C}G \hookrightarrow \prod_{i=1}^m \text{End}_{\mathbb{C}}(V_i),$$

an injective \mathbb{C} -algebra homomorphism, which is injective because the action is faithful. The dimension of the LHS is $\dim_{\mathbb{C}} = |G|$, and the dimension of the product on the right is $\sum_{i=1}^m \dim_{\mathbb{C}} \text{End}_{\mathbb{C}}(V_i) = \sum_{i=1}^m (\dim V_i)^2 = |G|$. But since we have an injective map between spaces of the same dimension, it must be an isomorphism, i.e. $\mathbb{C}G \cong \prod_{i=1}^m \text{End}_{\mathbb{C}}(V_i) = \prod_{i=1}^m M_{n_i}(\mathbb{C})$, where $n_i = \dim_{\mathbb{C}} V_i$.

Then $\mathbb{C}G \curvearrowright V_i$ is equivalent to a projection $\prod_{i=1}^m M_{n_i}(\mathbb{C}) \twoheadrightarrow M_{n_i}(\mathbb{C}) \curvearrowright \mathbb{C}^{n_i}$. For example, $\mathbb{C}S_3 \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$.

Now let's prove the claim that $m = r$. We look at the center of $\mathbb{C}G$, the maximal commutative subring of $\mathbb{C}G$, denoted $Z(\mathbb{C}G)$. Then

$$\begin{aligned} Z(\mathbb{C}G) &\cong Z\left(\prod_{i=1}^m M_{n_i}(\mathbb{C})\right) \\ &= \prod_{i=1}^m Z(M_{n_i}(\mathbb{C})) = \prod_{i=1}^m \mathbb{C}I_{n_i}. \end{aligned}$$

In particular, $\dim_{\mathbb{C}} Z(\mathbb{C}G) = m$, the number of irreducible representations of G . Let $\alpha \in \mathbb{C}G$. Then $\alpha = \sum_{g \in G} f(g)g$ for a unique $f : G \rightarrow \mathbb{C}$. So

$$\begin{aligned} \alpha \in Z(\mathbb{C}G) &\iff h\alpha = \alpha h \text{ for all } h \in G \\ &\iff \sum_{g \in G} f(g) \cdot hgh^{-1} = \sum_{g \in G} f(g)g \\ &\iff \sum_{g \in G} f(h^{-1}gh) \cdot g = \sum_{g \in G} f(g)g \\ &\iff f \in \mathcal{C}_G, \end{aligned}$$

the set of class functions. So $\mathcal{C}_G \xrightarrow{\sim} Z(\mathbb{C}G)$ is an isomorphism of \mathbb{C} vector spaces, with $f \mapsto \sum_{g \in G} f(g)g$.

Thus $\dim_{\mathbb{C}} Z(\mathbb{C}G) = \dim_{\mathbb{C}} \mathcal{C}_G = r$, the number of conjugacy classes of G , so $m = r$ just as desired. $\mathbb{C}G$ is a bit of an unusual vector space at this point, because it has two natural bases. They are:

- χ_1, \dots, χ_r
- $f_C, C \subseteq G$ conjugacy classes of G , with $f_C(g)$ being 1 or 0 depending on whether or not $g \in C$.

How are these bases related? One connection is the following, without very much theoretical significance:

$$\chi_i = \sum_C \chi_i(C) \cdot f_C,$$

where C ranges over all conjugacy classes of G and $\chi_i(C) = \chi_i(g)$ for any $g \in C$. A slightly more interesting connection is that

$$\begin{aligned} f_C &= \sum_{i=1}^r \langle f_C, \chi_i \rangle \chi_i \\ &= \sum_{i=1}^r \left(\frac{1}{|G|} \sum_{g \in G} f_C(g) \overline{\chi_i(g)} \right) \chi_i \\ &= \sum_{i=1}^r \frac{1}{|G|} \sum_{g \in C} \overline{\chi_i(g)} \chi_i \\ &= \sum_{i=1}^r \frac{1}{|G|} |C| \overline{\chi_i(C)} \chi_i. \end{aligned}$$

Taking $h \in G$, we get that

$$\sum_{i=1}^r \chi_i(h) \overline{\chi_i(g)} = \begin{cases} |G|/|C| & \text{if } h \in C \\ 0 & \text{if } h \notin C \end{cases},$$

and in the general case with $g, h \in G$,

$$\sum_{i=1}^r \chi_i(h) \overline{\chi_i(g)} = \begin{cases} |G|/|C| & \text{if } g \text{ and } h \text{ are conjugate in } G \\ 0 & \text{otherwise.} \end{cases}$$

In other words, the columns of a characteristic table are orthogonal! This can be checked on the table above. The rows also have orthogonality, with

$$\langle \chi_i, \chi_j \rangle = \frac{1}{|G|} \sum_{C \subseteq G} |C| \chi_i(C) \overline{\chi_j(C)} = 1.$$

15 March 24th

15.1 Character Tables

Today, we recall the set-up from last time, and then we're going to do a bunch of examples. Let G be a finite group with a representation over \mathbb{C} . Let r be the number of conjugacy

classes of G ; let V_1, \dots, V_r be the irreducible representations of G over \mathbb{C} up to isomorphism. Let $\chi_i = \chi_{V_i}$ be the character of the representation V_i , and let $n_i = \dim_{\mathbb{C}} V_i = \chi_i(1)$. Last time we saw that $\sum_{i=1}^r n_i^2 = |G|$.

Example. Let G be abelian. Then $r = |G|$, so $\sum_{i=1}^{|G|} n_i^2 = |G|$, which can only work if each $n_i = 1$. Thus all irreducible representations have degree 1.

△

Today we're gonna compute some character tables, of the form:

	C_1	\dots	C_j	\dots	C_r
χ_1			\vdots		
\vdots			\vdots		
χ_i	\dots	\dots	$\chi_i(C_j)$	\dots	\dots
\vdots					
χ_r					

This table describes all the representations of G . The conditions on the table are:

$$\bullet \sum_{i=1}^r \chi_i(C) \overline{\chi_i(C')} = \begin{cases} \frac{|G|}{|C|}, & C = C' \\ 0 & \text{otherwise} \end{cases}$$

$$\bullet \frac{1}{|G|} \sum_{C \subseteq G} |C| \chi_i(C) \overline{\chi_j(C)} = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}$$

Example. $G = S_4$. First let χ_1 be the trivial character and let χ_2 be the sign function. S_4 acting on \mathbb{C}^4 by permuting basis elements has a character $\chi : S_4 \rightarrow \mathbb{C}$ with $\chi(g)$ being the number of $i \in [4]$ that are fixed by g . This has values across the table of 4,3,1,0,0; then considering what $\chi' = \chi - \chi_1$ is, we actually get

$$\langle \chi', \chi' \rangle = \frac{1}{24} (1 \cdot 3^2 + 6 \cdot 1^2 + 0 + 6 \cdot (-1)^2 + 3 \cdot (-1)^2) = 1,$$

so χ' is irreducible. Thus χ' is our χ_3 .

We then produce $\chi_4 = \chi_3 \chi_2$, a new character which ends up being symmetries of the cube.

So we have one left. Note that it ought to be 0 on the conjugacy class of (12) and that of (1234), because otherwise multiplication with χ_2 would give yet another one, which is not good. We know that $1^2 + 1^2 + 3^2 + 3^2 + n_5^2 = |S_4| = 24$, so $n_5^2 = 4$ and $n_5 = 2$. But using our first bullet point, $\sum_{i=1}^5 \chi_i(C) \overline{\chi_i(1)} = 0$ if $C \neq \{1\}$, so we can use column orthogonality to fill out the rest of the row.

	sizes	1	6	8	6	3
		1	(12)	(123)	(1234)	(12)(34)
(trivial)	χ_1	1	1	1	1	1
(sign)	χ_2	1	-1	1	-1	1
	χ_3	3	1	0	-1	-1
	χ_4	3	-1	0	1	-1
	χ_5	2	0	-1	0	2

So, what's the representation for χ_5 ? We found the character through witchcraft, so we have to think for a bit longer. It's a map $\rho_5 : S_4 \rightarrow \text{GL}_2(\mathbb{C})$. What's its kernel? If $\rho_5(g) = I$, then $\chi_5(g) = \text{tr}(I) = 2$. So products of disjoint transpositions might be in the kernel. In fact, $\chi_5(g) = \zeta_1 + \zeta_2$, with ζ_i a root of unity, the eigenvalues of $\rho_5(g)$. So in fact if $\chi_5(g) = 2$, then $\chi_1 = \chi_2 = 1$, so $\rho_5(g) = I$. Thus the kernel is $\ker(\rho_5) = \{1, (12)(34), (14)(23), (13)(24)\} = V$, the Klein four group. So

$$\rho_5 : S_4 \twoheadrightarrow S_4/V \hookrightarrow \text{GL}_2(\mathbb{C}),$$

where as described last time, $S_4/V \cong S_3$, where elements permute the nontrivial elements of V by conjugation.

△

Example. $G = A_4$. Note that here $A_4/V \cong \mathbb{Z}/3\mathbb{Z}$. So there are representations achieved for free by looking at homomorphisms $A_4/V \rightarrow \mathbb{C}^*$. Taking a generator a , it maps to a cube root of unity $\zeta_3 = e^{2\pi i/3}$, with $i = 0, 1, 2$. You get two characters this way. Then fill in the last line by sum of the image of 1, and orthogonality of the columns.

	sizes	1	4	4	3
		1	(123)	(132)	(12)(34)
(trivial)	χ_1	1	1	1	1
	χ_2	1	ζ_3	ζ_3^2	1
	χ_3	1	ζ_3^2	ζ_3	1
	χ_4	3	0	0	-1

Alternatively, the last one comes from restricting either of the three-dimensional representation of S_4 to A_4 (they restrict to the same thing).

△

With $G \curvearrowright V$, and thus $V \otimes V$ a representation of G , there is a unique isomorphism $\Theta : V \otimes V \xrightarrow{\sim} V \otimes V$, with $v \otimes w \mapsto w \otimes v$. One can then define $\text{Sym}^2(V) = \{v \in V \otimes V \mid \Theta(v) = v\}$, and very similarly $\Lambda^2 V = \text{Alt}^2(V) = \{v \in V \otimes V \mid \Theta(v) = -v\}$. One can check that $V \otimes V = \text{Sym}^2 V \oplus \text{Alt}^2 V$, each of which is a representation of G . Then if χ is the character of V , we get that $\chi(g)^2 = \chi_{V \otimes V}(g)$, so you can derive that

$$\begin{aligned} \chi_{\text{Sym}^2 V}(g) &= \frac{1}{2} (\chi(g)^2 + \chi(g^2)), \\ \chi_{\text{Alt}^2 V}(g) &= \frac{1}{2} (\chi(g)^2 - \chi(g^2)). \end{aligned}$$

The idea is to fix $A \in \text{GL}_n(\mathbb{C})$ diagonalizable and e_1, \dots, e_n eigenvectors of A with $Ae_i = \lambda_i e_i$. $\Lambda^2 V$ has a basis $e_i \otimes e_j - e_j \otimes e_i$, for $1 \leq i < j \leq n$, and $A(e_i \otimes e_j - e_j \otimes e_i) = \lambda_i \lambda_j (e_i \otimes e_j - e_j \otimes e_i)$. So

$$\begin{aligned} \text{tr}(A|\Lambda^2 V) &= \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j \\ &= \frac{1}{2} \sum_{1 \leq i, j \leq n} \lambda_i \lambda_j - \frac{1}{2} \sum_i \lambda_i^2 \\ &= \frac{1}{2} ((\text{tr}(A))^2 - \text{tr}(A^2)). \end{aligned}$$

So taking tensor products is a good way to see new irreducible characters.

Example. $G = S_5$.

S_5 acts on \mathbb{C}^5 by permuting the indices; then $\mathbb{C}^5 = \mathbb{C}(e_1 + \dots + e_5) \oplus \{a \in \mathbb{C}^5 \mid \sum_{i=1}^5 a_i = 0\}$, the latter of which is V_{st} , the so-called standard representation, which becomes χ_3 , so we can compute that row as well.

Then χ_4 is obtained via multiplying χ_3 by χ_2 . We have three left! Then $\chi_5 = \chi_{\Lambda^2 V_{st}}$, which we can compute based on our previous formula.

So for χ_6, χ_7 , we know that $n_6^2 + n_7^2 = 50$, because the sum of the squares of the entries in the first column is 120. So we're missing two, and they're 5-dimensional. Hopefully, $\chi_2 \chi_6 = \chi_7$; but we have to check that we don't have $\chi_2 \chi_6 = \chi_6$. We claim that this works! That $\chi_2 \chi_6 \neq \chi_6$. If not, then $\chi_6((12)) = 0$ and also $\chi_7((12)) = 0$, so that we can't generate an eighth one, and so we should have $\sum_{i=1}^7 \chi_i((12)) \chi_i((12)) = |S_5|/10 = 12$, but we actually have $1^2 + (-1)^2 + 2^2 + (-2)^2 + 0 = 10$, which is bad! So this actually also shows that $\chi_6((12)) = 1$ and $\chi_6((12)) = -1$, without loss of generality, because $10 + (\chi_6((12)))^2 + (-\chi_6((12)))^2 = 12$.

Also, $\langle \chi_6, \chi_i \rangle = 0$ for $1 \leq i \leq 5$. Writing this out, we get linear equations in the missing values $\chi_6((123)), \chi_6((1234)), \chi_6((12345)), \chi_6((12)(34)), \chi_6((12)(345))$. This is 5 equations in 5 unknowns, which we can actually solve, which is how we fill in the last two rows of the table.

	sizes	1	10	20	30	24	15	20
		1	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
(trivial) χ_1		1	1	1	1	1	1	1
(sign) χ_2		1	-1	1	-1	1	1	-1
(standard) χ_3		4	2	1	0	-1	0	-1
$\chi_3 \chi_2 = \chi_4$		4	-2	1	0	-1	0	1
$\chi_{\Lambda^2 V_{st}} = \chi_5$		6	0	0	0	1	-2	0
χ_6		5	1	-1	-1	0	1	1
χ_7		5	-1	-1	1	0	1	-1

△

16 April 5th

16.1 The last of the examples

Example. Let $G = A_5$, the smallest nonabelian simple group. Recall the character table of S_5 :

	sizes	1	10	20	30	24	15	20
		1	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
(trivial) χ_1		1	1	1	1	1	1	1
(sign) χ_2		1	-1	1	-1	1	1	-1
(standard) χ_3		4	2	1	0	-1	0	-1
$\chi_3\chi_2 = \chi_4$		4	-2	1	0	-1	0	1
$\chi_{\Lambda^2 V_{st}} = \chi_5$		6	0	0	0	1	-2	0
χ_6		5	1	-1	-1	0	1	1
χ_7		5	-1	-1	1	0	1	-1

We now turn to A_5 , to fill in its character table. For every irreducible character of S_5 , $\chi_i|_{A_5}$ is a character of A_5 , but it need not be irreducible. So doing that for each of the others, we get that

$$\langle \chi_i|_{A_5}, \chi_i|_{A_5} \rangle = \frac{1}{|A_5|} \sum_{g \in A_5} \chi_i(g) \overline{\chi_i(g)} = \begin{cases} 1 & \text{if } i \neq 5 \\ 2 & \text{if } i = 5 \end{cases},$$

so let $\chi'_1 = \chi_1|_{A_5}$, let $\chi'_2 = \chi_3|_{A_5}$, and let $\chi'_3 = \chi_6|_{A_5}$. This gives us much but not all of our table!

But then also, $\sum_{i=1}^5 \chi'_i(1)^2 = |A_5| = 60$, so $1^2 + 4^2 + 5^2 + n_4^2 + n_5^2 = 60$, so $n_4^2 + n_5^2 = 18$ and $n_4 = n_5 = 3$. Now look at χ_5 ; if $\chi_5|_{A_5} = \sum_{i=1}^5 a_i \chi'_i$, then $2 = \langle \chi_5|_{A_5}, \chi_5|_{A_5} \rangle = \sum_{i=1}^5 a_i^2$, so two of the a_i 's are 1 and the rest 0. $\chi_5(1) = 6$, so either $\chi_5|_{A_5} = \chi'_1 + \chi'_3$ or $\chi_5|_{A_5} = \chi'_4 + \chi'_5$. But $\chi_5|_{A_5}$ can't be $\chi'_1 + \chi'_3$, because $\chi_5((12)(34)) = -2 \neq 2 = \chi'_1((12)(34)) + \chi'_3((12)(34))$. So $\chi_5|_{A_5} = \chi'_4 + \chi'_5$. Great! Let's find those characters and fill in our table.

Let $a = \chi'_4((123))$ and let $b = \chi'_4((12)(34))$. Then

$$\begin{aligned} 0 &= \langle \chi'_4, \chi'_1 + \chi'_2 \rangle \\ &= \frac{1}{60} \sum_{C \subseteq A_5} |C| \chi'_4(C) \overline{(\chi'_1(C) + \chi'_2(C))} \\ &= \frac{1}{60} (1 \cdot 3 \cdot 5 + 20 \cdot a \cdot 2 + 15 \cdot b \cdot 1 + 0 + 0) \\ \Rightarrow 0 &= 15 + 40a + 15b, \text{ and } 0 &= \langle \chi'_4, \chi'_3 \rangle \\ &= \frac{1}{60} (1 \cdot 3 \cdot 5 + 20 \cdot a \cdot (-1) + 15 \cdot b \cdot 1 + 0 + 0) \\ \Rightarrow 0 &= 15 - 20a + 15b, \end{aligned}$$

which we can solve to find that $a = 0$ and $b = -1$. The same argument gives you the same values of χ'_5 .

We then define a new pair of unknowns $x = \chi'_4((12345))$ and $y = \chi'_4((12354))$. Then

$$1 = \langle \chi'_4, \chi'_4 \rangle = \frac{1}{60}(3^2 + 0^2 + (-1)^2 + |x|^2 + |y|^2)$$

$$0 = \langle \chi'_4, \chi'_1 \rangle = \frac{1}{60}(3 - 15 + 12x + 12y),$$

so (assuming the secret assumption that x and y are real), $x^2 + y^2 = 3$ and $x + y = 1$, which can be solved. We know that it's real because they are the rotational symmetries of the dodecahedron and the icosahedron, but that is sort of a deus ex machina in this case (cheating!). Maybe next time we will go over how to see it.

sizes	1	20	15	12	12
	1	(123)	(12)(34)	(12345)	(12354)
χ'_1	1	1	1	1	1
χ'_2	4	1	0	-1	-1
χ'_3	5	-1	1	0	0
χ'_4	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ'_5	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

△

16.2 Frobenius Divisibility feat. maybe some Burnside

The goal of this section, which will be continued in the next lecture, is to prove the following two theorems.

Theorem 16.2.1 (Frobenius Divisibility). *Let G be finite and let χ be an irreducible character over \mathbb{C} . Then $\chi(1)$ divides $|G|$.*

Theorem 16.2.2 (Burnside 1904). *A group G of order $p^a q^b$, with p and q primes, is solvable.*

It'll also be the last section before we start homological algebra, and there might be some blending. We proceed to the proof of Frobenius! And all the definitions that it entails.

Definition 16.2.3. We say that $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is the root of a monic $f(x) \in \mathbb{Z}[x]$.

Example. $\alpha = \frac{1+\sqrt{5}}{2}$, which is the root of $(x - \frac{1+\sqrt{5}}{2})(x - \frac{1-\sqrt{5}}{2}) = x^2 - x - 1$.

△

Let \mathbb{A} be the set of algebraic integers of \mathbb{C} .

Lemma 16.2.4 (Key Fact). *\mathbb{A} is a subring of \mathbb{C} .*

Proof. First, note that $0, 1 \in \mathbb{A}$. Take any $\alpha, \beta \in \mathbb{A}$ and consider the ring $\mathbb{Z}[\alpha, \beta]$. Note $\mathbb{Z}[\alpha, \beta]$ is a finitely generated \mathbb{Z} module; if

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

for $a_i \in \mathbb{Z}$ and

$$\beta^m + b_{m-1}\beta^{m-1} + \cdots + b_0 = 0$$

with $b_i \in \mathbb{Z}$; then for an element $f \in \mathbb{Z}[\alpha, \beta]$, if you see α^n or β^m , you can replace with smaller exponents. so $\mathbb{Z}[\alpha, \beta]$ is generated as a \mathbb{Z} -module by $\alpha^i \beta^j$, for $0 \leq i \leq n$ and $0 \leq j \leq m$. Then let $\gamma \in \{\alpha + \beta, \alpha - \beta, \alpha\beta\}$ act on $\mathbb{Z}[\alpha, \beta]$ by multiplication. γ acts on $\mathbb{Z}[\alpha, \beta] \cong \mathbb{Z}^r$. With respect to a basis, γ acts as a matrix $A \in M_r(\mathbb{Z})$; let $f(x) = \det(xI - A) \in \mathbb{Z}[x]$. By Cayley-Hamilton, $f(A) = 0$, so $f(\gamma)$ acts on $\mathbb{Z}[\alpha, \beta]$ by multiplication as 0. So $f(\gamma) = 0$, and thus $\gamma \in \mathbb{A}$. \square

Another key fact is that $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$. There are similar cases, like $\mathbb{A} \cap \mathbb{Q}(\sqrt{5}) = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, which gives nice alternative notions of integers.

The idea behind the proof of Frobenius divisibility is to show that $|G|/\chi(1) \in \mathbb{A}$, which because we know that $|G|/\chi(1) \in \mathbb{Q}$ shows that $|G|/\chi(1) \in \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$, which suffices. For G a finite group with C_1, \dots, C_r conjugacy classes and χ_1, \dots, χ_r irreducible characters, for all i, j , $\chi_i(C_j)$ is an algebraic integer. This is because it is a sum of eigenvalues of $\rho_i(g)$, all of which are roots of unity, and roots of unity are algebraic integers.

Lemma 16.2.5.

$$\frac{|C_j|\chi_i(C_j)}{\chi_i(1)} \in \mathbb{A}.$$

In the interest of time, this lemma will be proved next time. Assume that lemma, here is the proof of Frobenius divisibility:

Proof.

$$\begin{aligned} |G| &= |G|\langle \chi_i, \chi_i \rangle \\ &= \sum_{g \in G} \chi_i(g) \overline{\chi_i(g)} \\ &= \sum_{j=1}^r |C_j| \chi_i(C_j) \overline{\chi_i(C_j)} \\ \Rightarrow \frac{|G|}{\chi_i(1)} &= \sum_{j=1}^r \underbrace{\frac{|C_j|\chi_i(C_j)}{\chi_i(1)}}_{\in \mathbb{A}} \underbrace{\overline{\chi_i(C_j)}}_{\in \mathbb{A}} \in \mathbb{A}. \end{aligned}$$

But then $\frac{|G|}{\chi_i(1)} \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$. \square

Example. If $|G| = p^2$, then $p^2 = |G| = \sum_{i=1}^r \chi_i(1)^2$, so each $\chi_i(1)$ cannot be p or p^2 , despite dividing p , so $\chi_i(1) = 1$ for all i , and thus G is abelian. \triangle

17 April 7th

17.1 Loose end

Let $g \in A_5$ be a 5-cycle. Then g and g^{-1} are conjugate in A_5 ! So for all characters χ of A_5 , $\chi(g) = \chi(g^{-1}) = \overline{\chi(g)}$, so $\chi(g) \in \mathbb{R}$.

17.2 Frobenius and Burnside, cont'd

Recall that \mathbb{A} is the set of algebraic integers in \mathbb{C} , i.e. $\alpha \in \mathbb{C}$ that are roots of monic $f(x) \in \mathbb{Z}[x]$. Also \mathbb{A} is a subring of \mathbb{C} , and $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Example. Let $f(x) \in \mathbb{Z}[x]$ be monic of degree 4, and let $\theta_1, \theta_2, \theta_3, \theta_4 \in \mathbb{C}$ be roots of f . Then there's a resolvent cubic

$$g(x) = (x - (\theta_1 + \theta_2)(\theta_3 + \theta_4))(x - (\theta_1 + \theta_3)(\theta_2 + \theta_4))(x - (\theta_1 + \theta_4)(\theta_2 + \theta_3)).$$

Note $g(x)$ has coefficients in \mathbb{A} and has coefficients in \mathbb{Q} via Galois theory, so $g(x) \in \mathbb{Z}[x]$.

△

For G a finite group with conjugacy classes C_1, \dots, C_r and irreducible characters χ_1, \dots, χ_r , we have $\chi_i(C_j) \in \mathbb{A}$.

From last time, we had as a step in the proof that $\frac{|G|}{\chi_i(1)} = \sum_{j=1}^r \left(\frac{|C_j| \chi_i(C_j)}{\chi_i(1)} \right) \overline{\chi_i(C_j)}$, and we needed one last lemma to use this to complete the proof of Frobenius divisibility.

Lemma 17.2.1.

$$\frac{|C_j| \chi_i(C_j)}{\chi_i(1)} \in \mathbb{A}.$$

Proof. Set $\chi = \chi_i$ and $C = C_j$. Define $\alpha = \sum_{g \in C} g \in \mathbb{C}G$; then for all $h \in G$, $h\alpha h^{-1} = \alpha$, so $h\alpha = \alpha h$. Let V be an irreducible representation corresponding to χ ; Consider $T : V \rightarrow V$ given by $v \mapsto \alpha v = \sum_{g \in C} gv$. Then for $h \in G$ and $v \in V$, $T(hv) = \sum_{g \in C} g(hv) = \alpha hv = h\alpha v = hT(v)$, so T is a homomorphism of $\mathbb{C}G$ -modules.

Then by Schur's Lemma, since V is irreducible and T is a linear map that respects the group actions, T acts on V as multiplication by a scalar $\lambda \in \mathbb{C}$. The trace $\text{tr}(T) = \lambda \cdot \dim V = \lambda \chi(1) = \sum_{g \in C} \text{tr}(g|V) = \sum_{g \in C} \chi(g) = |C| \chi(C)$. Thus $\lambda = \frac{|C| \chi(C)}{\chi(1)}$, so our question boils down to whether or not λ is in \mathbb{A} .

Let α act on $\mathbb{Z}G \subseteq \mathbb{C}G$ by multiplication. $\mathbb{Z}G$ is a free \mathbb{Z} -module with respect to some basis. α acts as a matrix $A \in M_{|G|}(\mathbb{Z})$. Let $f(x) = \det(xI - A) \in \mathbb{Z}[x]$; by Cayley-Hamilton, $f(A) = 0$. So $f(\alpha)$ acting on $\mathbb{Z}G$ by multiplication acts as 0. Then $f(\alpha)$ must be 0, so $f(T) = 0$, so since λ is an eigenvalue of T , $f(\lambda) = 0$. Then $\lambda \in \mathbb{A}$, since it's the root of a monic polynomial, so we're done. □

So Frobenius divisibility holds! Yay.

Theorem 17.2.2 (Burnside). *A group G of order $p^a q^b$, with p, q primes, is solvable.*

To prove it, we'll use a quick lemma:

Lemma 17.2.3. *Let V be an irreducible representation of G with character χ , and let C be a conjugacy class of G . Suppose $|C|$ and $\chi(1)$ are relatively prime. Then for any $g \in C$, either $\chi(g) = 0$ or g acts on V by a scalar.*

Proof. Fix $g \in C$. Let ζ_1, \dots, ζ_n be the eigenvalues of g on V , and let $n = \chi(1)$. Then $\chi(g) = \zeta_1 + \dots + \zeta_n \in \mathbb{A}$. By the previous lemma, $\frac{|C|\chi(C)}{\chi(1)} \in \mathbb{A}$. $\chi(1)$ and $|C|$ are relatively prime, so there exists $a, b \in \mathbb{Z}$ with $a|C| + b\chi(1) = 1$. Then $a\frac{|C|\chi(C)}{\chi(1)} \in \mathbb{A}$, and this is equal to $(1 - b\chi(1))\frac{\chi(C)}{\chi(1)} = \frac{\chi(C)}{\chi(1)} - b\chi(C)$, with $b\chi(C) \in \mathbb{A}$. Thus $\frac{\chi(C)}{\chi(1)} \in \mathbb{A}$, so $\alpha = \frac{\zeta_1 + \dots + \zeta_n}{n} \in \mathbb{A}$. Suppose $\alpha \neq 0$, or equivalently that $\chi(C) = \chi(g) \neq 0$. Take a finite Galois extension L/\mathbb{Q} containing $\zeta_1 + \dots + \zeta_n$; then $\alpha \in L$. Then

$$N_{L/\mathbb{Q}}(\alpha) = \prod_{\sigma \in \text{Gal}(L/\mathbb{Q})} \sigma(\alpha) \in \mathbb{Q} \cap \mathbb{A}.$$

$\sigma(\alpha)$ lies in \mathbb{A} , because $f(\alpha) = 0$ implies that $f(\sigma(\alpha)) = 0$. So $N_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and isn't zero, because $\alpha \neq 0$. Thus

$$\begin{aligned} 1 \leq |N_{L/\mathbb{Q}}(\alpha)| &= \prod_{\sigma} |\sigma(\alpha)|, \text{ where} \\ |\sigma(\alpha)| &= \left| \frac{\sigma(\zeta_1) + \dots + \sigma(\zeta_n)}{n} \right| \\ &\leq \frac{1}{n} \sum_{i=1}^n |\sigma(\zeta_i)| = \frac{n \cdot 1}{n} = 1. \end{aligned}$$

So $|\sigma(\alpha)| = 1$ for all σ , so $\left| \frac{\zeta_1 + \dots + \zeta_n}{n} \right| = 1$, so $\zeta_1 = \dots = \zeta_n$, so g acts by multiplication by ζ_1 on V . □

This leads us to the following zany theorem!

Theorem 17.2.4. *Let G be a finite group and suppose C is a conjugacy class of G of cardinality p^e , with p a prime and $e \geq 1$. Then G is not simple.*

Proof. Let $C \neq \{1\}$. Then

$$\begin{aligned} &\sum_{\chi \text{ irred.}} \chi(C)\overline{\chi(1)} = 0 \\ \Rightarrow 1 + \sum_{\chi \neq 1, p \mid \chi(1)} \chi(1)\chi(C) + \sum_{\chi \neq 1, p \nmid \chi(1)} \chi(1)\chi(C) &= 0. \end{aligned}$$

We claim that there exists an irreducible $\chi \neq 1$ with $p \nmid \chi(1)$ and $\chi(C) \neq 0$. If not, then

$$0 = 1 + p \cdot \sum_{\chi \neq 1, p \nmid \chi(1)} \frac{\chi(1)}{p} \chi(C)$$

$$\Rightarrow -\frac{1}{p} \in \mathbb{A}, \text{ which is a contradiction.}$$

So take $g \in C$. We have $\chi(g) = \chi(C) \neq 0$ and $p \nmid \chi(1)$ and $|C| = p^e$. By the previous lemma, g acts on V by a scalar λ . Taking $g' \in C$ with $g \neq g'$, g' also acts on V via multiplication by λ . So $g(g')^{-1} \neq 1$ but acts on V as the identity. so $\rho : G \rightarrow \text{GL}(V)$ has nontrivial kernel, and $\ker \rho \neq G$, since $\chi \neq 1$, so we've found a normal subgroup $\ker \rho \trianglelefteq G$. \square

Now we're ready for the proof of Burnside's Theorem.

Proof. Recall that $|G| = p^a \cdot q^b$. Suppose the theorem fails. Then there is a simple nonabelian group with cardinality $p^a q^b$; without loss of generality G is simple and nonabelian, and we will prove a contradiction. Let $C \neq \{1\}$ be a conjugacy class. Then $|C| = |G|/|\text{Cent}_G(g)|$ for a fixed $g \in C$, due to the bijection $G/\text{Cent}_G(g) \xrightarrow{\sim} C$ given by $h \mapsto hgh^{-1}$. So $|C|$ divides $|G|$; by the previous theorem, $|C| \neq p^e$ or q^e . So $|C| \equiv 0 \pmod{pq}$, and in particular $|C| \equiv 0 \pmod{q}$, unless $C = \{1\}$. Thus

$$0 \equiv p^a q^b \equiv |G| = \sum_{C \subseteq G} |C| \equiv 1 \pmod{q},$$

so $0 \equiv 1 \pmod{q}$, a contradiction. \square

18 April 12th: Transition to Homological Algebra

18.1 Hom

Fix a ring R with identity (but not necessarily commutative). We will work with the category of (left) R -modules, $R\text{-Mod}$. Its objects are R -modules M , and its morphisms are R -module homomorphisms $f : M \rightarrow N$. Then $\text{Hom}_R(M, N)$ is the set of such f . We can give $\text{Hom}_R(M, N)$ an additive group structure via $(f + f')(m) = f(m) + f'(m)$. If R is commutative, then we can also make $\text{Hom}_R(M, N)$ an R -module, via $(rf)(m) = r \cdot f(m)$. But this might not work for the noncommutative case.

Now for functors! Let $F : R\text{-Mod} \rightarrow \mathbf{Ab}$ (the category of abelian groups) be a functor. On objects, a module M is mapped to $F(M)$ an abelian group, and on morphisms $M \xrightarrow{f} N$ gives a morphism $F(M) \xrightarrow{F(f)=f_*} F(N)$. For morphisms f, g , we have $F(gf) = F(g) \cdot F(f)$, and we have that $F(\text{id}_M) = \text{id}_{F(M)}$.

Examples. 0. $F : R\text{-Mod} \rightarrow \mathbf{Ab}$ a forgetful functor, with $M \mapsto M$, forgetting the R -action.

1. Fix an R -module M , and consider the function $\text{Hom}_R(M, -) : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$. For objects, we have $N \mapsto \text{Hom}_R(M, N)$, and for morphisms $A \xrightarrow{f} B$ an R -module homomorphism, we have $\text{Hom}_R(M, A) \xrightarrow{f_*} \text{Hom}_R(M, B)$, where $\varphi \mapsto f \circ \varphi$. It can be checked that composition of maps can be done before or after applying the functor.

Remark. The functor $\text{Hom}_R(M, -)$ up to equivalence determines M up to isomorphism. This is known as Yoneda's Lemma, and can be looked up.

But our examples above, and our definition, were actually covariant functors. With arrow reversed, i.e. $M \xrightarrow{f} N$ corresponding to $F(N) \xrightarrow{f^*} F(M)$, we have what's known as a contravariant functor.

2. Fix an R -module N . Consider the functor $\text{Hom}_R(-, N) : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$, with $M \mapsto \text{Hom}_R(M, N)$. Given $A \xrightarrow{f} B$, we then have $\text{Hom}_R(B, N) \xrightarrow{f^*} \text{Hom}_R(A, N)$, with $\varphi \mapsto \varphi \circ f$, composing on the other side.
3. Fix a right R -module M . Given a left R -module N , we can define $M \otimes_R N$ an abelian group. We'll discuss this next time; it is the familiar definition of tensor products for the case of abelian groups.
4. Let $R = \mathbb{Z}G$ for G a finite group. There is then a covariant functor $\mathbf{R-Mod} \rightarrow \mathbf{Ab}$, with $M \mapsto M^G = \{m \in M \mid gm = m \forall g \in G\}$. Then given $f : M \rightarrow N$, we have $f_* : M^G \rightarrow N^G$ with $m \mapsto f(m)$.

Looking at the group ring, we actually have a special case of example 1, given by $\text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M) \xrightarrow{\sim} M^G$, with $\varphi \mapsto \varphi(1)$.

Later we'll associate "derived functors." Examples 1 and 2 will lead to $\text{Ext}_R^n(M, N)$, example 3 to $\text{Tor}_n^R(M, N)$, and 4 to $H^n(G, M)$, the group cohomology.

Definition 18.1.1. A pair $A \xrightarrow{f} B \xrightarrow{g} C$ of R -modules is *exact* at B if $\text{im } f = \ker g$.

A sequence of homomorphisms

$$\cdots \rightarrow A_{n+1} \rightarrow A_n \rightarrow A_{n-1} \rightarrow \cdots$$

is *exact* if it is exact at every A_n .

Example. $0 \rightarrow A \xrightarrow{f} B$ is exact if and only if $0 = \ker f$, or if and only if f is injective. Similarly, $B \xrightarrow{g} C \rightarrow 0$ is exact if and only if $\text{im } g = C$, i.e. g is surjective.

Combining them, $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ is exact if and only if f is injective, g is surjective, and $\text{im } f = \ker g$. In this case, it is called a short exact sequence or SES.

△

Take a covariant functor $F : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$ and a SES $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$, and apply F to get $0 \rightarrow F(A) \rightarrow F(B) \rightarrow F(C) \rightarrow 0$. There is an interesting and useful question of whether or not exactness is preserved.

Example. Let $R = \mathbb{Z}$, and consider the SES $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$. Let $M = \mathbb{Z}/2\mathbb{Z}$ and consider the $\text{Hom}_{\mathbb{Z}}(M, -)$ functor. We then get

$$0 \rightarrow \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z}) \rightarrow \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}) \rightarrow \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}) \rightarrow 0,$$

where \mathbb{Q} and \mathbb{Z} have no torsion elements, so the first two terms are 0, but the third term is the group of order 2. However, we can salvage exactness by erasing the last 0.

Now let $N = \mathbb{Z}$ and consider the functor $\text{Hom}_{\mathbb{Z}}(-, N)$, getting the sequence

$$0 \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, N) \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Q}, N) \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \rightarrow 0.$$

In this case the last term is \mathbb{Z} , the middle term is 0, and the first term is 0. But we can again cheat by erasing the final 0, and we still have exactness for the first part.

△

Example. Let $G = \text{Gal}(\mathbb{C}/\mathbb{R})$, and consider the sequence

$$1 \rightarrow \{\pm 1\} \rightarrow \mathbb{C}^{\times} \rightarrow \mathbb{C}^{\times} \rightarrow 1.$$

Letting $R = \mathbb{Z}G$ and taking the fourth functor above, this gives the sequence

$$1 \rightarrow \{\pm 1\} \rightarrow \mathbb{R}^{\times} \rightarrow \mathbb{R}^{\times} \rightarrow 1.$$

Again, this isn't exact, but it becomes exact if we erase the last term. So this begins to beg the question, if it's not zero at the end, what comes next? What can we naturally add on to the sequence?

△

Proposition 18.1.2. *Take a SES $0 \rightarrow A \xrightarrow{\psi} B \xrightarrow{\varphi} C \rightarrow 0$.*

a) *Then*

$$0 \rightarrow \text{Hom}_R(M, A) \xrightarrow{\psi_*} \text{Hom}_R(M, B) \xrightarrow{\varphi_*} \text{Hom}_R(M, C)$$

is exact for all R -modules M , and

b)

$$0 \rightarrow \text{Hom}_R(C, N) \rightarrow \text{Hom}_R(B, N) \rightarrow \text{Hom}_R(A, N)$$

is exact for all R -modules N .

$\text{Hom}_R(M, -)$ and $\text{Hom}_R(-, N)$ are called left exact because of this property.

Proof. We'll just prove a, and b will be very similar. Take any $f : M \rightarrow A$ such that $\psi_* f = 0$. Then $\psi \circ f = 0$, so $f = 0$, because ψ is injective, and we're done.

Now for exactness at $\text{Hom}_R(M, B)$. Since $\varphi \circ \psi = 0$, $\varphi_* \circ \psi_* = 0$, so $\text{im } \psi_* \subseteq \ker \varphi_*$. But are they equal? Let $f \in \ker \varphi_*$, i.e. any $f : M \rightarrow B$ with $\varphi \circ f = 0$. $\text{im } f \subseteq \ker \varphi = \text{im } \psi$ by exactness of the sequence, so $M \xrightarrow{f} \text{im } (f) \subseteq \text{im } \psi$. But since ψ is injective, $\text{im } \psi \cong A$, so we have the composition g mapping $M \rightarrow A$. And $\psi_*(g) = \psi \circ g = f$, so $f \in \text{im } \psi_*$, so exactness holds. □

There is also a notion of *right exact*, which loses exactness on the left but keeps it on the right, and of a functor being *exact*, where exactness is preserved on both sides, i.e. short exact sequences are taken to short exact sequences.

Definition 18.1.3. An R -module M is *projective* if $\text{Hom}_R(M, -)$ is exact.

An R -module N is *injective* if $\text{Hom}_R(-, N)$ is exact.

Example. Free R -modules are projective.

If R is a PID, then M is injective if and only if $rM = M$ for all nonzero $r \in R$. For example, if $R = \mathbb{Z}$, then $M = \mathbb{Q}$ is an injective module.

△

For M an R -module, we'll see that we can construct $F_0 \twoheadrightarrow M$, a surjective homomorphism, where F_0 is a free R -module. In fact, one can continue, making an exact sequence

$$\cdots \rightarrow F_2 \rightarrow F_1 \rightarrow F_0 \rightarrow M \rightarrow 0,$$

with F_i a free (or projective) R -module. This is the idea of a free resolution, as we'll see later.

19 April 14th

19.1 Last time

Let R be a ring. Then:

- For M an R -module, $\text{Hom}_R(M, -) : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$ with $N \mapsto \text{Hom}_R(M, N)$ and for $f : A \rightarrow B$, $f_* : \text{Hom}_R(M, A) \rightarrow \text{Hom}_R(M, B)$ given by $\varphi \mapsto f \circ \varphi$, is a covariant left exact functor.
- For N an R -module, $\text{Hom}_R(-, N) : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$ with $M \mapsto \text{Hom}_R(M, N)$ is a contravariant left exact functor.

19.2 Projective modules

Recall that an R -module P is *projective* if $\text{Hom}_R(P, -)$ is exact.

Recall an R -module M is *free* if there is a subset $A \subseteq M$ such that every $m \in M$ has a unique expression $m = \sum_{a \in A} r_a \cdot a$ for $r_a \in R$ and $r_a = 0$ for all but finitely many $a \in A$. Given a set A , we define $F(A) = \bigoplus_{a \in A} R$, the free module with basis A , where $a \in A$ embeds by mapping a to δ_a , which is 1 at a and 0 elsewhere.

Proposition 19.2.1. *Let P be an R -module. TFAE:*

- a) P is projective, i.e. $\text{Hom}_R(P, -)$ is exact.

b) For a surjective homomorphism $\varphi : M \rightarrow N$ of R -modules and any $f : P \rightarrow N$, there exists a homomorphism $g : P \rightarrow M$ such that $\varphi \circ g = f$, i.e.

$$\begin{array}{ccccc}
 & & P & & \\
 & \swarrow \exists g & \downarrow f & & \\
 M & \xrightarrow{\varphi} & N & \longrightarrow & 0
 \end{array}$$

c) Every SES

$$0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\varphi} P \longrightarrow 0$$

splits, i.e. there is a homomorphism $g : P \rightarrow B$ with $\varphi \circ g = \text{id}_P$.

d) There is an R -module P' with $P \oplus P'$ free.

Example. Free R -modules are projective by (d).

△

Example. $\mathbb{Z}/n\mathbb{Z}$ is not a projective \mathbb{Z} -module, since

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

doesn't split.

△

Example. Let $R = \mathbb{C}G$ with G a finite group. Consider a short exact sequence

$$0 \longrightarrow A \hookrightarrow B \xrightarrow{\varphi} C \longrightarrow 0$$

with A, B, C $\mathbb{C}G$ -modules. By Maschke's Theorem, $B = A \oplus A'$, and we have an inverse isomorphism back from C to A' , that shows the sequence splits. So all $\mathbb{C}G$ modules are projective.

But if $G \neq 1$, then $\mathbb{C}G = \bigoplus_i V_i^{\dim V_i}$, with V_i irreducible representations of G . But $V_i \subsetneq \mathbb{C}G$; V_i is a projective $\mathbb{C}G$ module, but is not free.

△

Example. Let R be a PID and M finitely generated; then M is projective if and only if M is free.

△

Example. Due to Quillen-Suslin. If $R = K[x_1, \dots, x_n]$, then a module is projective if and only if it is free.

△

Okay, so let's prove the proposition.

Proof. a) \Rightarrow b): For the short exact sequence

$$0 \longrightarrow A \longrightarrow M \xrightarrow{\varphi} N \longrightarrow 0 ,$$

apply $\text{Hom}_R(P, -)$ to get

$$0 \longrightarrow \text{Hom}_R(P, A) \hookrightarrow \text{Hom}_R(P, M) \xrightarrow{\varphi_*} \text{Hom}_R(P, N) \longrightarrow 0$$

Then there is some $g \in \text{Hom}_R(P, M)$ that maps to f ; then $f = \varphi_* g = \varphi \circ g$, as desired.

b) \Rightarrow c): In this case the map from P to P is given by the identity, and the function that shows that it splits is the map g given by condition b.

c) \Rightarrow d): There is a surjective homomorphism $F \rightarrow P$, with F free, giving

$$0 \longrightarrow P' \longrightarrow F \longrightarrow P \longrightarrow 0 .$$

But this SES splits, via $g : P \rightarrow F$, giving $F = P' \oplus g(P) \cong P' \oplus P$.

d) \Rightarrow a): Let $F = P \oplus P'$, with F free, and take any short exact sequence

$$0 \longrightarrow A \longrightarrow B \xrightarrow{\varphi} C \longrightarrow 0 .$$

We need $\text{Hom}_R(P, B) \rightarrow \text{Hom}_R(P, C)$ to be surjective; take any $f : P \rightarrow C$. Then in the following diagram, there is an (orange) map G making everything commute.

$$\begin{array}{ccc}
 & F = P \oplus P' & \\
 & \downarrow & \\
 \exists G & \text{---} & P \\
 & \downarrow & \\
 & C & \\
 \uparrow \varphi & \leftarrow & \\
 B & \xrightarrow{\varphi} & C \longrightarrow 0
 \end{array}$$

Using the inclusion of P into F , one can get a mapping $g : F \rightarrow C$ which agrees with f . Then we construct the map G by noting that $F = P \oplus P' = F(\mathcal{A})$; then for $a \in \mathcal{A}$, select $b_a \in B$ with $\varphi(b_a) = g(a)$, and extend to a morphism; there is a unique R -module homomorphism $G : F \rightarrow B$ with $a \mapsto b_a$. Then $g = \varphi \circ G$, so we're done. \square

Example. Let X be a compact and smooth manifold, and let $R = C^\infty(X)$ be the set of smooth functions on X . Let $\overset{V}{\downarrow} X$ be a smooth vector bundle, and let M be the set of smooth sections of V . Then M is an R -module. Swan proved that M is a finitely generated projective $C^\infty(X)$ -module. Also, all finitely generated projective $C^\infty(X)$ -modules arise in this way.

△

Now let's define Ext! In particular, we'll define $\text{Ext}_R^n(M, N)$, the n th cohomology group derived from $\text{Hom}_R(-, N)$.

Fix an R -module M , and choose a *projective resolution* of M , i.e. an exact sequence of projective modules

$$\cdots \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0.$$

One must exist, as one can see by using free modules. We then forget M to get the sequence (no longer exact at P_0)

$$\cdots \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_1 \rightarrow P_0 \rightarrow 0,$$

and apply $\text{Hom}_R(-, N)$ to get

$$0 \rightarrow \text{Hom}_R(P_0, N) \xrightarrow{d^1} \text{Hom}_R(P_1, N) \xrightarrow{d^2} \text{Hom}_R(P_2, N) \rightarrow \cdots .$$

Then we define $\text{Ext}_R^n(M, N)$ to be $\ker d^{n+1} / \text{im } d^n$, which is a group. There are some issues with this definition. We have to show it doesn't depend on choice of projective resolution, which is a pretty big choice. But we'll see later that this doesn't matter. The other issue is, why is this useful?

19.3 Injective Modules

This is sort of the same thing, but backwards. There's an analogue of that big proposition we proved.

Proposition 19.3.1. *Let Q be an R -module. TFAE:*

- a) Q is injective, i.e. $\text{Hom}_R(-, Q)$ is exact.
- b) If $\psi : A \rightarrow B$ is an injective homomorphism of R -modules, then every homomorphism from $A \rightarrow Q$ lifts to a homomorphism from $B \rightarrow Q$, i.e.

$$\begin{array}{ccccc}
 0 & \longrightarrow & A & \xrightarrow{\psi} & B \\
 & & \downarrow f & \swarrow \exists g & \\
 & & Q & &
 \end{array}$$

c) If Q is an R -submodule of M , then $M = Q \oplus Q'$ for some R -submodule Q' . Equivalently, every SES

$$0 \longrightarrow Q \longrightarrow M \longrightarrow Q' \longrightarrow 0$$

splits.

The proof is also the same as before, but in reverse, so we leave it out here.

Example. $R = \mathbb{C}G$, for G a finite group. All $\mathbb{C}G$ -modules are injective!

△

Unlike in the projective case, there's not a friendly set of examples like free modules. But there is some setup.

Proposition 19.3.2 (Baer's criterion). *Let Q be an R -module. Then Q is injective if and only if for every left ideal I of R , any R -module homomorphism $g : I \rightarrow Q$ extends to a homomorphism $G : R \rightarrow Q$.*

In the interest of time we won't prove it here, but we might next time.

Example. Let R be a PID, and let $I = Rr$ with $r \neq 0$. Then given a map $f : I \rightarrow Q$, f is determined by $f(r) = q$. For $F : R \rightarrow Q$ to exist, we need $F(r) = f(r) = q$, and we need to be able to "divide" by r to get $F(r) = rF(1)$. The punch line is that Q is injective if and only if $rQ = Q$ for all $r \in R$, $r \neq 0$.

△

Example. We can apply the above example to \mathbb{Z} -modules. For \mathbb{Z} -modules, injective examples are \mathbb{Q} , \mathbb{Q}/\mathbb{Z} , \mathbb{C}^\times . Not-injective examples are things like $\mathbb{Z}/5\mathbb{Z}$ and \mathbb{R}^\times .

△

20 April 19th

20.1 Some more injective modules

Let R be a ring. Fix an R -module N . As we discussed before, $\text{Hom}_R(-, N) : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$ with $M \mapsto \text{Hom}_R(M, N)$ is a contravariant functor, where $f : A \rightarrow B$ maps to $f^* : \text{Hom}_R(B, N) \rightarrow \text{Hom}_R(A, N)$ with $f^*\varphi = \varphi f$. This functor is left exact, i.e. if $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is exact, then so is $0 \rightarrow \text{Hom}_R(C, N) \rightarrow \text{Hom}_R(B, N) \rightarrow \text{Hom}_R(A, N)$. N is injective if $\text{Hom}_R(-, N)$ is exact. But as seen last time, we had a zillion equivalent definitions for a module being injective, e.g. that Q is injective if homomorphisms $A \rightarrow Q$ lift to a homomorphism $B \rightarrow Q$ given an injective map $A \rightarrow B$.

Theorem 20.1.1. *Every R -module M is contained in an injective R -module. (The category $\mathbf{R}\text{-Mod}$ “has enough injectives.”)*

Proof. We’ll prove this when $R = \mathbb{Z}$; the general case will follow from this and is a problem on the next HW.

Let A be a set of generators of M as a \mathbb{Z} -module. Let $F = F(A)$ be the free \mathbb{Z} -module of the set A . Then there exists a surjective homomorphism $\varphi : F \rightarrow M$ of \mathbb{Z} -modules, where for $a \in A$, $a \mapsto a$.

Let Q be the vector space over \mathbb{Q} with basis A . Then Q is an injective \mathbb{Z} -module; for $n \in \mathbb{Q}^\times$, $nQ = Q$. Note that $Q/\ker \varphi = Q'$ is also an injective \mathbb{Z} -module, because $nQ' = Q'$ for all $n \in \mathbb{Q}^\times$. Since $F \subseteq Q = F \otimes_{\mathbb{Z}} \mathbb{Q}$, and $M = F/\ker \varphi$, $M \subseteq Q/\ker \varphi = Q'$, just as desired. \square

For an R -module M and an injective module Q_0 with $M \subseteq Q_0$, we get an exact sequence

$$0 \rightarrow M \hookrightarrow Q_0 \rightarrow Q_0/M.$$

But $Q_0/M \subseteq Q_1$ with Q_1 exact, so continuing the pattern we get an injective resolution

$$0 \rightarrow M \rightarrow Q_0 \rightarrow Q_1 \rightarrow Q_2 \rightarrow \cdots,$$

which is exact and has Q_i injective.

For an injective resolution

$$0 \rightarrow N \rightarrow Q_0 \rightarrow Q_1 \rightarrow \cdots,$$

throw away N (it’s still useful) and apply $\text{Hom}_R(M, -)$ to get

$$0 \xrightarrow{d^0} \text{Hom}_R(M, Q_0) \xrightarrow{d^1} \text{Hom}_R(M, Q_1) \xrightarrow{d^2} \text{Hom}_R(M, Q_2) \rightarrow \cdots.$$

Then we can define $\text{Ext}_R^n(M, N) = \ker(d^{n+1})/\text{im}(d^n)$. Note that we already defined Ext last time! We claim that this matches the other description of $\text{Ext}_R^n(M, N)$.

20.2 Tensor Products Revisited! D&F§10.4

Let R be a ring that need not be commutative. Let M be a right R -module and let N be a left R -module. (Note that if R is commutative and if M is a left R -module, one can make it into a right R -module by defining $m * r = rm$.)

Definition 20.2.1. A map $\varphi : M \times N \rightarrow L$ to a \mathbb{Z} -module L is R -balanced if

- it is biadditive, i.e. $\varphi(m_1+m_2, n) = \varphi(m_1, n) + \varphi(m_2, n)$ and $\varphi(m, n_1+n_2) = \varphi(m, n_1) + \varphi(m, n_2)$ and
- $\varphi(m, rn) = \varphi(mr, n)$ for all $m \in M$, $n \in N$, $r \in R$.

Define $h : M \times N \rightarrow M \otimes_R N$ to be the *universal R -balanced map of $M \times N$* .

This means that for h and the map $M \times N \rightarrow L$ being R -balanced, there is a unique group homomorphism $M \otimes_R N \rightarrow L$ so that the following diagram commutes:

$$\begin{array}{ccc}
 M \times N & \xrightarrow{h} & M \otimes_R N \\
 & \searrow & \downarrow \text{dashed} \\
 & & L
 \end{array}$$

If the tensor product exists, it's unique up to isomorphism. A sketch of the proof of existence is that you can take F the free \mathbb{Z} -module on $M \times N$, and then you mod out by all the relations you need.

So there is a bijection

$$\{R\text{-balanced } M \times N \rightarrow L\} \leftrightarrow \{\mathbb{Z}\text{-mod. hom. } M \otimes_R N \rightarrow L\}.$$

If R is commutative, M and N are (left/right) R -modules. You can make $M \otimes_R N$ an R -module via

$$r \left(\sum_i a_i m_i \otimes n_i \right) = \sum_i a_i (r m_i) \otimes n_i = \sum_i a_i (m_i r) \otimes n_i.$$

Alternatively! We can look at bimodules.

Definition 20.2.2. For R and S rings, a (S, R) -bimodule is an abelian group M with a left S -module and right R -module structure such that $(rm)s = r(ms)$ for all $r \in R, s \in S, m \in M$.

In this setting we can give the tensor more structure! For M an (S, R) -bimodule and N a left R -module, $M \otimes_R N$ has a left S -module structure given by $s(m \otimes n) = (sm) \otimes n$.



As an example, let G be a finite group with $H \leq G$ a subgroup. Let V be a (complex) representation of H , i.e. a $\mathbb{C}H$ -module. We can construct a representation of G ; namely, $\text{Ind}_H^G(V) = \mathbb{C}G \otimes_{\mathbb{C}H} V$, where $\mathbb{C}G$ is a $(\mathbb{C}G, \mathbb{C}H)$ -bimodule and V is a $\mathbb{C}H$ -module. This is called the *induced representation* of V , and it is a $\mathbb{C}G$ -module, with $\dim \text{Ind}_H^G(V) = [G : H] \dim V$.

Example. Let $G = S_3$ and let $H = A_3 = \langle (123) \rangle$. Then H acts on $V = \mathbb{C}$ via an action ψ , where $\psi((123))$ is multiplication by $e^{2\pi i/3}$. Note that V cannot be an S_3 representation that extends this $H = A_3$ representation.

Then $\text{Ind}_H^G(V)$ is the (unique) two dimensional irreducible representation of S_3 .

△

Let \mathcal{R} be a set of representatives in G of the cosets of H . Then $|\mathcal{R}| = [G : H]$, and $\mathbb{C}G$ can be viewed as $\mathbb{C}G = \bigoplus_{r \in \mathcal{R}} r\mathbb{C}H$, so $\mathbb{C}G \otimes_{\mathbb{C}H} V = \bigoplus_{r \in \mathcal{R}} (r\mathbb{C}H) \otimes_{\mathbb{C}H} V = \bigoplus_{r \in \mathcal{R}} r(\mathbb{C}H \otimes_{\mathbb{C}H} V)$. The dimension of each summand over \mathbb{C} is the same as $\dim_{\mathbb{C}} V$. Take $g \in G$; then for $r \in \mathcal{R}$, there is a unique $r_g \in \mathcal{R}$ and $h \in H$ with $gr = r_g \cdot h$.

Let χ be the character of H acting on V ; then the character of $\text{Ind}_H^G(V)$ is

$$\text{Ind}_H^G(\chi)(g) = \sum_{r \in \mathcal{R}, r^{-1}gr \in H} \chi(r^{-1}gr).$$

So this is a new way of constructing characters.

21 April 21st

21.1 I'm Getting Tensor Every Day

<https://www.youtube.com/watch?v=BipvGD-LCjU>

Let R be a ring, let M be a right R -module and let N be a left R -module. Last time, we defined $M \otimes_R N$ a \mathbb{Z} -module with a specific universal mapping property. Also, for M an (S, R) -bimodule, we can give $M \otimes_R N$ a left S -module structure, where for $s \in S$, $s(m \otimes n) = (sm) \otimes n$. For each s , we have the following commuting diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow{h} & M \otimes_R N \\ \downarrow & \searrow \varphi & \vdots \\ M \times N & \xrightarrow{h} & M \otimes_R N \end{array}$$

where φ is R -balanced, with $\varphi(m, n) = h(sm, n)$, and the map $M \times N \rightarrow M \times N$ is given by $(m, n) \mapsto (sm, n)$, so that the action by s is the uniquely defined map on the right.

Tensoring is a functor; given $f : M \rightarrow M'$ a morphism of right R -modules and $g : N \rightarrow N'$ a morphism of left R -modules, we have $f \otimes g : M \otimes N \rightarrow M' \otimes N'$ generated by $m \otimes n \mapsto f(m) \otimes g(n)$. For a fixed M , $M \otimes_R - : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$ is a covariant functor.

Theorem 21.1.1. $M \otimes_R - : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$ is right exact; for any SES

$$0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\varphi} C \longrightarrow 0,$$

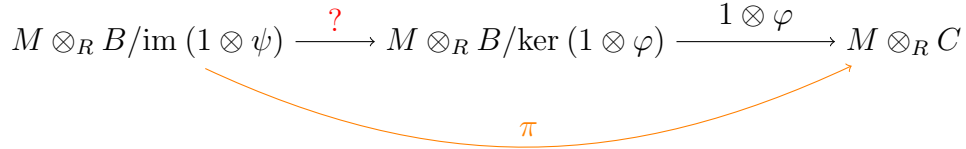
we know that

$$M \otimes_R A \xrightarrow{1 \otimes \psi} M \otimes_R B \xrightarrow{1 \otimes \varphi} M \otimes_R C \rightarrow 0$$

is exact.

Proof. • $1 \otimes \varphi$ is surjective: For $m \in M$ and $c \in C$, we want to verify that $m \otimes c$ is in the image. There exists $b \in B$ with $\varphi(b) = c$, since φ is surjective; then $(1 \otimes \varphi)(m \otimes b) = m \otimes \varphi(b) = m \otimes c$, so we're done.

• Exactness at $M \otimes_R B$: $(1 \otimes \varphi) \circ (1 \otimes \psi) = 1 \otimes (\varphi \circ \psi) = 0$, so the image is contained in the kernel. Now we have

$$M \otimes_R B / \text{im}(1 \otimes \psi) \xrightarrow{?} M \otimes_R B / \ker(1 \otimes \varphi) \xrightarrow{1 \otimes \varphi} M \otimes_R C$$


It suffices to find a homomorphism $\tilde{\pi} : M \otimes_R C \rightarrow M \otimes_R B / \text{im}(1 \otimes \psi)$ such that $\tilde{\pi} \circ \pi = \text{id}$. We have $M \times C \rightarrow M \otimes_R B / \text{im}(1 \otimes \psi)$, with $(m, c) \mapsto m \otimes b_c + \text{im}(1 \otimes \psi)$, where we choose $b_c \in B$ with $\varphi(b_c) = c$.

Then $\tilde{\pi} \circ \pi(m \otimes b) = \tilde{\pi}(m \otimes \varphi(b)) = m \otimes b + \text{im}(1 \otimes \psi)$, as desired. So then the kernel is contained in the image, as desired. □

Definition 21.1.2. M is *flat* if $M \otimes_R -$ is exact. Similarly, $- \otimes_R N : \mathbf{Mod-R} \rightarrow \mathbf{Ab}$ is right-exact, and N is *flat* if it is exact.

Theorem 21.1.3. *Projective (and free) modules are flat.*

Idea of proof. Reduce to the free case, by taking for P projective the free module $F = P \oplus P'$ that is proven to exist. Then reduce to the finitely generated case, with $F = R^n$, and take $R^n \otimes_R N = (R \otimes_R N)^n = N^n$. Then $R^n \otimes_R -$ applied to a short exact sequence $0 \rightarrow A \xrightarrow{\psi} B \xrightarrow{\varphi} C \rightarrow 0$ becomes $0 \rightarrow A^n \rightarrow B^n \rightarrow C^n \rightarrow 0$, with maps performed pointwise, which is still exact. □

Example. For $R \subseteq S$ commutative rings, fix an ideal $I \subseteq R$, with $0 \rightarrow I \xrightarrow{\psi} R \rightarrow R/I \rightarrow 0$. Apply $S \otimes_R -$ to this sequence to get

$$S \otimes_R I \xrightarrow{1 \otimes \psi} S \otimes_R R \rightarrow S \otimes_R (R/I) \rightarrow 0.$$

Then $\text{im}(1 \otimes \psi) = SI = IS$, the ideal of S generated by I . So $S \otimes_R (R/I) \cong S/IS$. If S is a flat R -module, then $S \otimes_R I \cong SI = IS$.

△

In fact, Hom and \otimes are related! Let S and R be rings, and let M be an (S, R) -bimodule. Then we claim the functors

- $M \otimes_R - : \mathbf{R}\text{-Mod} \rightarrow \mathbf{S}\text{-Mod}$
- $\text{Hom}_S(M, -) : \mathbf{S}\text{-Mod} \rightarrow \mathbf{R}\text{-Mod}$, where for $f \in \text{Hom}_S(M, N)$ and for $r \in R$, define $rf \in \text{Hom}_S(M, N)$ by $rf(m) = f(mr)$. Then $(rf)(sm) = f((sm)r) = f(s(mr)) = sf(mr) = s(rf)(m)$, so this is natural and works 'n' stuff.

are related. These two functors are *adjoints* of each other. In particular, if A is an R -module and B is an S -module, then

$$\text{Hom}_S(M \otimes_R A, B) \cong \text{Hom}_R(A, \text{Hom}_S(M, B)),$$

and this isomorphism is a functorial/natural isomorphism, where we have

$$(f : M \otimes_R A \rightarrow B) \mapsto (a \mapsto (m \mapsto f(m \otimes a))),$$

and in the other direction we have the map

$$(\text{map induced by } (m, a) \mapsto (g(a))(m)) \leftarrow (g : A \rightarrow \text{Hom}_S(M, B))$$

Example. For $H \subseteq G$ finite groups, and V a representation over \mathbb{C} of H , $\text{Ind}_H^G(V) = \mathbb{C}G \otimes_{\mathbb{C}H} V$ is a representation of G . Let $M = \mathbb{C}G$, let $A = V$, let $R = \mathbb{C}H$, and let $S = \mathbb{C}G$. Then we can talk about

$$\begin{aligned} \text{Hom}_{\mathbb{C}G}(\text{Ind}_H^G(V), W) &= \text{Hom}_{\mathbb{C}G}(\mathbb{C}G \otimes_{\mathbb{C}H} V, W) \\ &= \text{Hom}_{\mathbb{C}H}(V, \text{Hom}_{\mathbb{C}G}(\mathbb{C}G, W)) \\ &= \text{Hom}_{\mathbb{C}H}(V, W), \end{aligned}$$

because $\text{Hom}_{\mathbb{C}G}(\mathbb{C}G, W) \cong W$ via $\varphi \mapsto \varphi(1)$. So we can take the dimension of this over \mathbb{C} , which was $\langle \text{Ind}_H^G(\chi_V), \chi_W \rangle = \langle \chi_V, \chi_W|_H \rangle = \langle \chi_V, \text{Res}_H^G(\chi_W) \rangle$, where the first inner product is a sum over G and the second is a sum over H .

△

Armed with this, we will wade merrily into examples of induced representations!

22 April 26th

22.1 Homology/Cohomology

Definition 22.1.1. A *chain complex* is a sequence $\{C_n\}_{n \in \mathbb{Z}}$ of abelian groups with homomorphisms

$$C : \cdots \rightarrow C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \rightarrow \cdots$$

such that $d_n \circ d_{n+1} = 0$ for all n , i.e. “ $d^2 = 0$.”

The book will tell you that $C_n = 0$ for $n < 0$.

We then define $Z_n(C) = \ker(d_n) \subseteq C_n$, the group of *cycles*, and $B_n(C) = \text{im}(d_{n+1}) \subseteq C_n$ the group of boundaries. Note that $B_n(C) \subseteq Z_n(C)$, so we define the *n-th homology group* of a chain complex C is

$$H_n(C) = Z_n(C)/B_n(C).$$

Note that the sequence is *exact* at C_n if and only if $H_n(C) = 0$, and the sequence is exact everywhere if and only if $H_n(C) = 0$ for all n .

Let C and D be chain complexes. A homomorphism $f : C \rightarrow D$, also called a *chain map*, is a collection of homomorphisms $f_n : C_n \rightarrow D_n$ such that the following commutes:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & C_{n+1} & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} \longrightarrow \cdots \\ & & \downarrow f_{n+1} & & \downarrow f_n & & \downarrow f_{n-1} \\ \cdots & \longrightarrow & D_{n+1} & \xrightarrow{d_{n+1}} & D_n & \xrightarrow{d_n} & D_{n-1} \longrightarrow \cdots \end{array}$$

Observe that $f : C \rightarrow D$ induces a group homomorphism $H_n(C) \rightarrow H_n(D)$, with $c + B_n(C) \mapsto f_n(c) + B_n(D)$. To check that this is well-defined, it suffices to check that $f_n(Z_n(C)) \subseteq Z_n(D)$ and $f_n(B_n(C)) \subseteq B_n(D)$, which is a homework problem.

So we have a functor $H_n : \mathbf{Ch} \rightarrow \mathbf{Ab}$, where the first category is the category of chain complexes.

Let $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ be an exact sequence of chain complexes, i.e.

$$\begin{array}{ccccccc}
& \vdots & & \vdots & & \vdots & \\
& \downarrow d & & \downarrow d & & \downarrow d & \\
0 & \longrightarrow & A_n & \xrightarrow{f_n} & B_n & \xrightarrow{g_n} & C_n \longrightarrow 0 \\
& & \downarrow d & & \downarrow d & & \downarrow d \\
0 & \longrightarrow & A_{n-1} & \xrightarrow{f_{n-1}} & B_{n-1} & \xrightarrow{g_{n-1}} & C_{n-1} \longrightarrow 0 \\
& & \downarrow d & & \downarrow d & & \downarrow d \\
& & \vdots & & \vdots & & \vdots
\end{array}$$

Then we claim that the sequence $H_n(A) \xrightarrow{f_*} H_n(B) \xrightarrow{g_*} H_n(C)$ of abelian groups is exact (but f_* need not be injective and g_* need not be surjective).

As a proof, $g \circ f = 0$ so $g_* \circ f_* = 0$, so $\text{im}(f_*) \subseteq \ker(g_*)$. Take any $[b] \in \ker(g_*)$. Then $g_n(b) \in B_n(C)$; so let $c \in C_{n+1}$ be such that $g_n(b) = d(c)$. Then there's a $b' \in B_{n+1}$ with $g_{n+1}(b') = c$. Consider $b - d(b') \in B_n$. Applying g_n , we get $g_n(b - d(b')) = g_n(b) - g_n(d(b')) = d(c) - d(g_{n+1}(b')) = d(c) - d(c) = 0$. So $b - d(b') \in \ker g_n = \text{im } f_n$, so let $b - d(b') = f_n(a')$ with $a' \in A_n$. Then $b - f_n(a') \in B_n(B)$, so $[b] = [f_n(a')]$, so $\ker(g_*) = \text{im}(f_*)$ as desired.

What a chase!

So the functor $H_n : \mathbf{Ch} \rightarrow \mathbf{Ab}$ is a covariant functor, but it's not left exact or right exact. But the failure of the exactness is actually measured by the other homology groups!

Theorem 22.1.2. *We have a (long) exact sequence of abelian groups*

$$\cdots \xrightarrow{\delta_{n+1}} H_n(A) \rightarrow H_n(B) \rightarrow H_n(C) \xrightarrow{\delta_n} H_{n-1}(A) \rightarrow H_{n-1}(B) \rightarrow \cdots,$$

where the $\delta_n : H_n(C) \rightarrow H_{n-1}(A)$ are the connecting homomorphisms.

A special case is if we have a short exact sequence of chain maps $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ with $A_n = B_n = C_n = 0$ for $n < 0$. Then the sequence stops at the end, i.e. we get

$$\cdots \rightarrow H_1(B) \rightarrow H_1(C) \xrightarrow{\delta_1} H_0(A) \rightarrow H_0(B) \rightarrow H_0(C) \rightarrow 0,$$

which is exact. This says that $H_0 : \mathbf{Ch}_{\geq 0} \rightarrow \mathbf{Ab}$ is a covariant right-exact functor.

Recall that $M \otimes_R - : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$ is also a covariant right-exact functor. So if we want this to be somehow analogous to H_0 , what are the analogues of H_i for $i > 0$? Well, this ends up being $\text{Tor}_n^R(M, -)$, where $\text{Tor}_0^R(M, -) = M \otimes_R -$. The construction is going to be *through* the category of chain maps.

Lemma 22.1.3 (Snake Lemma). *Consider the following commutative diagram of abelian groups, with exact rows.*

$$\begin{array}{ccccccc}
& & A & \xrightarrow{f} & B & \xrightarrow{g} & C \longrightarrow 0 \\
& & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\
0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C'
\end{array}$$

Then we have an exact sequence of groups

$$\ker(\alpha) \xrightarrow{\bar{f}} \ker(\beta) \xrightarrow{\bar{g}} \ker(\gamma) \xrightarrow{\delta} \operatorname{coker}(\alpha) \xrightarrow{\bar{f}'} \operatorname{coker}(\beta) \xrightarrow{\bar{g}'} \operatorname{coker}(\gamma),$$

where for $\alpha : A \rightarrow A'$, $\operatorname{coker}(\alpha) = A'/\operatorname{im}(\alpha)$.

Proof. The meat of it is defining δ . For $c \in \ker(\gamma) \subseteq C$, we want an element of A' . g is surjective, so there is a $b \in B$ with $g(b) = c$. Then $\beta(b) \in B'$, and $g'(\beta(b)) = \gamma(g(b)) = \gamma(c) = 0$, so $\beta(b) \in \ker(g') = \operatorname{im}(f')$, so there's a unique $a \in A'$ such that $f'(a) = \beta(b)$. Then $\delta(c) = a + \operatorname{im}(\alpha)$.

We need to check that this is well-defined; the problem is we made a choice of b , which in principle could matter (“W-wait a minute, that’s not unique! It’s not well-defined!”). So, assume we choose any other $\tilde{b} \in B$ such that $c = g(\tilde{b})$. As before, there’s a unique $\tilde{a} \in A'$ with $f'(\tilde{a}) = \beta(\tilde{b})$. But $g(b - \tilde{b}) = g(b) - g(\tilde{b}) = 0$, so $b - \tilde{b} \in \ker g = \operatorname{im} f$, i.e. $b - \tilde{b} = x$ for $x \in A$. But then $f'(a - \tilde{a}) = \beta(b - \tilde{b}) = \beta(f(x)) = f'(\alpha(x))$. By injectivity of f' , this means that $a - \tilde{a} = \alpha(x)$, so $a + \operatorname{im} \alpha = \tilde{a} + \operatorname{im} \alpha$. (“Yes, it is defined - up to an element in the kernel of alpha. Okay?”)

It’s then a good homework exercise to check that the sequence is exact. See also: \square

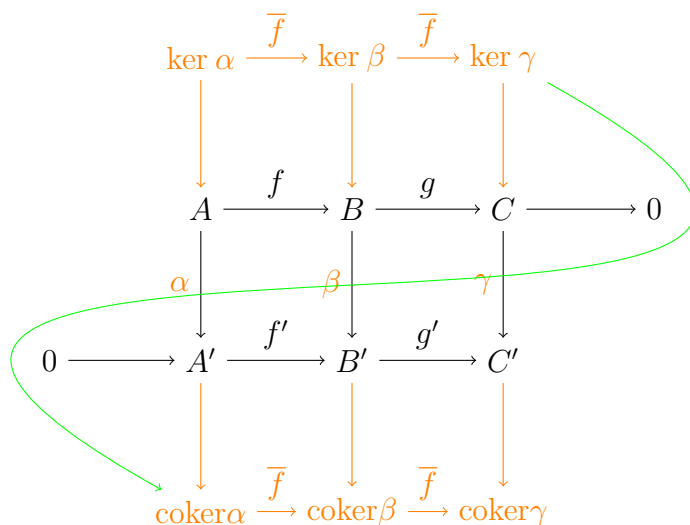
As a supplement: if f is injective, then \bar{f} is injective; if g' is surjective, then \bar{g}' is surjective.

23 April 28th

23.1 Snake Lemma Continued, and More Homological Algebra

<https://www.youtube.com/watch?v=etbcKWEKngv>

Diagrammatically, we can draw out the snake lemma, which says that the orange and yellow sequence is exact:



Recall that a *chain complex* C is a sequence

$$C : \cdots \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \rightarrow \cdots$$

with $d_{n+1} \circ d_n = 0$ for all n , and that $H_n(C) = Z_n(C)/B_n(C) = \ker(d_n)/\text{im}(d_{n+1})$. We also defined chain maps, and stated the theorem that a short exact sequence of chain complexes $0 \rightarrow C \rightarrow D \rightarrow E \rightarrow 0$ gives a long exact sequence of homology groups. In other words, we have the following commuting diagram with exact rows:

$$\begin{array}{ccccccc}
 & \vdots & & \vdots & & \vdots & \\
 & \downarrow d & & \downarrow d & & \downarrow d & \\
 0 & \longrightarrow & C_{n+1} & \xrightarrow{f_{n+1}} & D_{n+1} & \xrightarrow{g_{n+1}} & E_{n+1} \longrightarrow 0 \\
 & & \downarrow d & & \downarrow d & & \downarrow d \\
 0 & \longrightarrow & C_n & \xrightarrow{f_n} & D_n & \xrightarrow{g_n} & E_n \longrightarrow 0 \\
 & & \downarrow d & & \downarrow d & & \downarrow d \\
 0 & \longrightarrow & C_{n-1} & \xrightarrow{f_{n-1}} & D_{n-1} & \xrightarrow{g_{n-1}} & E_{n-1} \longrightarrow 0 \\
 & & \downarrow d & & \downarrow d & & \downarrow d \\
 0 & \longrightarrow & C_{n-2} & \xrightarrow{f_{n-2}} & D_{n-2} & \xrightarrow{g_{n-2}} & E_{n-2} \longrightarrow 0 \\
 & & \downarrow d & & \downarrow d & & \downarrow d \\
 & & \vdots & & \vdots & & \vdots
 \end{array}$$

Theorem 23.1.1. *There is a long exact sequence*

$$\cdots \rightarrow H_n(C) \xrightarrow{f_*} H_n(D) \xrightarrow{g_*} H_n(E) \xrightarrow{\delta_n} H_{n-1}(C) \rightarrow \cdots$$

Proof. We have a snake-like commutative diagram of groups:

$$\begin{array}{ccccccc} C_n/B_n(C) & \xrightarrow{f_n} & D_n/B_n(D) & \xrightarrow{g_n} & E_n/B_n(E) & \longrightarrow & 0 \\ & & \downarrow d & & \downarrow d & & \\ 0 & \longrightarrow & Z_{n-1}(C) & \xrightarrow{f_{n-1}} & Z_{n-1}(D) & \xrightarrow{g_{n-1}} & Z_{n-1}(E) \end{array}$$

We claim that the rows are exact. Using the snake lemma with cokernels from the $n + 1$ st and n th rows of our mongo diagram above gives exactness of the top row; using the snake lemma with kernels for the $n - 1$ st and $n - 2$ nd rows gives exactness for the bottom rows.

Now we want to apply the snake lemma here! $C_n/B_n(C) \rightarrow Z_{n-1}(C)$ has kernel $Z_n(C)/B_n(C) = H_n(C)$ and cokernel $Z_{n-1}(C)/B_{n-1}(C) = H_{n-1}(C)$, and similarly for the other two vertical maps. So this gives the $H_n(C)$ -through- $H_{n-1}(D)$ portion of the sequence, and we can keep going by shifting n . \square

There is also a world of cohomology; it is really the same world. A *cochain complex* C is a sequence of maps

$$\cdots \rightarrow C^{m-1} \xrightarrow{d^m} C^m \xrightarrow{d^{m+1}} C^{m+1} \rightarrow \cdots,$$

where $d^n \circ d^{n-1} = 0$ for all n . The n th co-homology group is $H^n(C) = Z^n(C)/B^n(C)$; there's nothing mysterious here. Defining \tilde{C}_n to be C^{-n} , this would just turn everything into homology. Just as before, a short exact sequence of cochain complexes gives a long exact sequence of cohomology groups.

Example (Singular homology). Fix X a topological space. A *standard n -simplex* is defined as

$$\Delta^n = \left\{ (t_0, \dots, t_n) \in \mathbb{R}^{n+1} \mid t_i \geq 0, \sum_i t_i = 1 \right\}.$$

So for $n = 0$, this is a dot; for $n = 1$, this is a line; for $n = 2$, this is a triangle; for $n = 3$, this is a tetrahedron, and so on, and so forth. A *singular n -simplex* in X is a continuous map $\sigma : \Delta^n \rightarrow X$. Then let $C_n(X)$ be the free abelian group on the singular n -simplexes, or the group of n -chains. For $n < 0$, $C_n(X) = 0$.

We then want to define boundary maps $d_n : C_n(X) \rightarrow C_{n-1}(X)$. We write the boundary maps as a signed sum of lower dimensional faces, i.e. for $0 \leq i \leq n$, we have $e_i : \Delta^{n-1} \rightarrow \Delta^n$ where we just embed into the subset with i th coordinate 0. Then the boundary of Δ^n is just $\bigcup_i e_i(\Delta^{n-1})$, so that

$$d_n(\sigma) = \sum_{i=0}^n (-1)^i \sigma \circ e_i \in C_{n-1}(X),$$

because $\sigma \circ e_i$ is a continuous map $\Delta^{n-1} \rightarrow \Delta^n \rightarrow X$. It's an exercise that $d_{n-1}(d_n(\sigma)) = 0$, so we get a chain complex

$$C(X) : \cdots \rightarrow C_n(X) \xrightarrow{d_n} C_{n-1}(X) \xrightarrow{d_{n-1}} C_{n-2}(X) \rightarrow \cdots \rightarrow C_0(X) \rightarrow 0.$$

As before, we define $Z_n(C(X)) = \ker d_n$ and $B_n(C(X)) = \text{im } d_{n+1}$. An element of $C_1(X)$ is an abstract sum of paths; for an element of $Z_1(C_1(X))$, every endpoint of a path has to be a startpoint as well. Singular homology is merely homology of this chain complex.

In this case, H_n is a functor $H_n : \mathbf{Top} \rightarrow \mathbf{Ch}_{\geq 0} \rightarrow \mathbf{Ab}$, where for $f : X \rightarrow Y$ we have $C_n(X) \rightarrow C_n(Y)$ given by $\sigma \mapsto f \circ \sigma$, which gives an induced map $f_* : C(X) \rightarrow C(Y)$. Everything is functorial. And, it's not obvious from this construction, but the homology groups tend to be nice friendly objects. For example, for the smooth compact surface of genus g , $H_1(X) \cong \mathbb{Z}^{2g}$.

△

These examples are a fun and enticing intro to algebraic topology: “If you haven't seen this stuff before, this is sort of too much, and if you have, it's boring.”

Example (Singular cohomology). Given a topological space X with its singular chain complex and an abelian group G , we can apply $\text{Hom}_{\mathbb{Z}}(-, G)$ to define $C^n(X, G) = \text{Hom}_{\mathbb{Z}}(C_n(X), G)$. This gives the cochain complex

$$0 \rightarrow C^0(X, G) \rightarrow \cdots \rightarrow C^n(X, G) \rightarrow C^{n+1}(X, G) \rightarrow \cdots,$$

and $H^n(X, G)$, the n -th cohomology group of X with coefficients in G .

△

Part of why singular homology tends to be super nice for nice spaces is that we can define simplicial homology, where we look at finitely generated groups $D_n(X) \subseteq C_n(X)$ originating from simplicial complex structures on a space. But, it turns out simplicial homology and singular homology agree where simplicial homology can be computed, so this massive simplification yields the same result.

Next time, we'll talk about derived functors.

24 May 3rd

24.1 Cohomology Cont: Next Ext and More Tor

Recall that in cohomology we have a cochain complex

$$C : 0 \rightarrow C^0 \xrightarrow{d^1} C^1 \xrightarrow{d^2} C^2 \rightarrow \cdots,$$

where $d^n \circ d^{n-1} = 0$, and $H^n(C) = \ker(d^{n+1})/\text{im}(d^n)$. For $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ a short exact sequence of cochain complexes, we get a long exact sequence of cohomology groups

$$0 \rightarrow H^0(A) \xrightarrow{f^*} H^0(B) \xrightarrow{g^*} H^0(C) \\ \xrightarrow{\delta} H^1(A) \rightarrow H^1(B) \rightarrow H^1(C) \xrightarrow{\delta} H^2(A) \rightarrow \dots,$$

where δ is the connecting homomorphism that we discussed last time.

Now fix a ring R and a left R -module N . We have a functor $\text{Hom}_R(-, N) : \mathbf{R}\text{-Mod} \rightarrow \mathbf{Ab}$ which is contravariant and left exact, so for a SES of R -modules $0 \rightarrow A \rightarrow B \rightarrow C$, we have $0 \rightarrow \text{Hom}_R(C, N) \rightarrow \text{Hom}_R(B, N) \rightarrow \text{Hom}_R(A, N)$. Then Ext will be about extending this to an exact sequence that continues $\text{Hom}_R(A, N) \xrightarrow{\delta} \text{Ext}_R^1(C, N) \rightarrow \text{Ext}_R^1(B, N) \rightarrow \text{Ext}_R^1(A, N) \xrightarrow{\delta} \text{Ext}_R^2(C, N) \rightarrow \dots$, just like exists for cohomology. We want functors $\text{Ext}_R^n(-, N) : \mathbf{R}\text{-Mod} \rightarrow \mathbf{Ab}$, each of which measures the failure of exactness of the last.

So we begin our construction. Let A be an R -module and choose a projective resolution of A given by

$$\dots \rightarrow P_3 \rightarrow P_2 \rightarrow P_1 \rightarrow P_0 \rightarrow A \rightarrow 0,$$

where each P_n is a projective R -module and the sequence is exact. We have proven before that this exists. Apply $\text{Hom}_R(-, N)$ and remove the first term to get

$$0 \rightarrow \text{Hom}_R(P_0, N) \rightarrow \text{Hom}_R(P_1, N) \rightarrow \dots,$$

a cochain complex. Taking the n -th cohomology group gives us

$$\text{Ext}_R^n(A, N) := H^n(\text{Hom}_R(P, N)).$$

We have to prove that this is well-defined. As an aside, if A is projective, note that using the resolution $0 \rightarrow A \rightarrow A \rightarrow 0$ gives that $\text{Ext}_R^n(A, N) = 0$ for all $n \geq 1$; it turns out this is an if and only if. Also, a special case is that $\text{Ext}_R^0(A, N) = \ker(\text{Hom}_R(P_0, N) \rightarrow \text{Hom}_R(P_1, N)) = \text{Hom}_R(A, N)$. In particular, $\text{Ext}_R^0(-, N)$ is just the functor we started with, $\text{Hom}_R(-, N)$, so our analogy with cohomology is going well!

Example. Fix R -modules A and B . Then an extension is a short exact sequence of R -modules

$$0 \longrightarrow A \longrightarrow E \longrightarrow B \longrightarrow 0.$$

We always have $0 \rightarrow A \rightarrow A \oplus B \rightarrow B \rightarrow 0$. Extensions E and E' are *equivalent* if there exists a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

where the maps $A \rightarrow A$ and $B \rightarrow B$ are the identity and the map $E \rightarrow E'$ is an isomorphism. There's a bijection

$$\{\text{extensions of } B \text{ by } A \text{ up to equivalence}\} \leftrightarrow \text{Ext}_R^1(B, A).$$

The bijection is obtained by applying $\text{Hom}_R(-, A)$ to the extension to get

$$\cdots \rightarrow \text{Hom}_R(E, A) \rightarrow \text{Hom}_R(A, A) \xrightarrow{\delta} \text{Ext}_R^1(B, A).$$

We then map E to the image of the identity map under δ .

△

There's still this pesky issue of whether or not Ext depends on the projective resolution; we'll get to this eventually (spoiler: it doesn't), but for now, we will continue to ignore it until it resolves (ha, ha) itself on its own.

Let B be an R -module with projective resolution

$$\cdots \rightarrow P'_2 \rightarrow P'_1 \rightarrow P'_0 \rightarrow B \rightarrow 0,$$

which we use to define $\text{Ext}_R^n(B, N)$. Let $f : A \rightarrow B$ be a homomorphism of R -modules; the ultimate goal is a homomorphism $f^* : \text{Ext}_R^n(B, N) \rightarrow \text{Ext}_R^n(A, N)$.

$$\begin{array}{ccccccc} \cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0 \\ & & \downarrow f_2 & & \downarrow f_1 & & \downarrow f_0 & & \downarrow f & & \\ \cdots & \longrightarrow & P'_2 & \longrightarrow & P'_1 & \longrightarrow & P'_0 & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

We claim that all the red maps $f_n : P_n \rightarrow P'_n$ exist, and they make the diagram commute. In other words, we have a chain map. We'll start with the P_0 map; we have

$$\begin{array}{ccc} & P_0 & \\ & \downarrow & \\ \exists & \swarrow & A \\ & & \downarrow \\ P'_0 & \longrightarrow & B \longrightarrow 0 \end{array}$$

By projectivity, there's a map $P_0 \rightarrow P'_0$; define this to be f_0 . We then proceed by induction; if we've defined maps up through f_n , does f_{n+1} exist?

$$\begin{array}{ccccc}
P_{n+1} & \xrightarrow{d_{n+1}} & P_n & \xrightarrow{d_n} & P_{n-1} \\
\downarrow \text{?} & & \downarrow f_n & & \downarrow f_{n-1} \\
P'_{n+1} & \xrightarrow{d'_{n+1}} & P'_n & \xrightarrow{d'_n} & P'_{n-1}
\end{array}$$

By commutativity, $d'_n(f_n(d_{n+1}(P_{n+1}))) = f_{n-1}(d_n(d_{n+1}(P_{n+1}))) = 0$, so $f_n(d_{n+1}(P_{n+1})) \subseteq \ker(d'_n) = \text{im}(d'_{n+1})$, so then we can construct the following diagram and get the edge $P_{n+1} \rightarrow P'_{n+1}$, which exists because P_{n+1} is projective; we define this map to be f_{n+1} .

$$\begin{array}{ccc}
& P_{n+1} & \\
& \downarrow d_{n+1} & \\
& P_n & \\
& \downarrow f_n & \\
P'_{n+1} & \xrightarrow{d'_{n+1}} & \text{im}(d'_{n+1}) \longrightarrow 0
\end{array}$$

\exists (indicated by a red dashed arrow from P_{n+1} to P'_{n+1})

So applying Hom to our projective resolutions gives the following:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \text{Hom}_R(P_0, N) & \longrightarrow & \text{Hom}_R(P_1, N) & \longrightarrow & \dots \\
& & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \text{Hom}_R(P'_0, N) & \longrightarrow & \text{Hom}_R(P'_1, N) & \longrightarrow & \dots
\end{array}$$

The cochain maps induces a group homomorphism between cohomology groups $\text{Ext}_R^n(B, N) \rightarrow \text{Ext}_R^n(A, N)$. But this is making it worse, because we chose our f_n 's. However, fret not; the end is near.

Proposition 24.1.1. *The homomorphism $\text{Ext}_R^n(B, N) \rightarrow \text{Ext}_R^n(A, N)$ does not depend on the choices of f_n .*

Before we prove this, here's a nice corollary and its proof:

Corollary 24.1.2. *$\text{Ext}_R^n(A, N)$ is independent of choice as well; more precisely, a different projective resolution of A will produce a canonically isomorphic group.*

Proof. This is exactly the setting where we consider $A = B$. So we have the diagram

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \downarrow & = & \\
\cdots & \longrightarrow & P'_2 & \longrightarrow & P'_1 & \longrightarrow & P'_0 & \longrightarrow & A & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \downarrow & = & \\
\cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0
\end{array}$$

The top two rows induce a map $\text{Ext}_R^n(A, N)' \rightarrow \text{Ext}_R^n(A, N)$ which is well-defined by the proposition. The bottom two rows induce a map $\text{Ext}_R^n(A, N) \rightarrow \text{Ext}_R^n(A, N)'$, and the composition $\text{Ext}_R^n(A, N) \rightarrow \text{Ext}_R^n(A, N)' \rightarrow \text{Ext}_R^n(A, N)$ is the identity, because that could arise from ignoring the middle row and extending the identity map to a chain map on the *same* projective resolution! By the proposition, this gives the same map. Similarly, composing the other way gives the identity, so we have two natural maps that are inverses, and thus a natural isomorphism. \square

Now for a sketch of the proof of the proposition.

Sketch of proof. Make different choices $\tilde{f}_n : P_n \rightarrow P'_n$. This gives the following diagram:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
& & f_2 - \tilde{f}_2 & & f_1 - \tilde{f}_1 & & f_0 - \tilde{f}_0 & & 0 & & \\
\cdots & \longrightarrow & P'_2 & \longrightarrow & P'_1 & \longrightarrow & P'_0 & \longrightarrow & B & \longrightarrow & 0
\end{array}$$

We want to show that the induced homomorphism $\text{Ext}_R^n(B, N) \rightarrow \text{Ext}_R^n(A, N)$ is 0.

We're just concerned with the difference, so without loss of generality let's redefine $f = 0$ and $\tilde{f}_n = 0$. So we have

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0 \\
& \swarrow s_2 & \downarrow f_2 & \swarrow s_1 & \downarrow f_1 & \swarrow s_0 & \downarrow f_0 & & \downarrow 0 & & \\
\cdots & \longrightarrow & P'_2 & \longrightarrow & P'_1 & \longrightarrow & P'_0 & \longrightarrow & B & \longrightarrow & 0
\end{array}$$

and we claim that there exist R -module homomorphisms $s_n : P_n \rightarrow P'_{n+1}$ such that $f_n = d'_{n+1}s_n + s_{n-1}d_n$. We construct them inductively; if $d_{n+1}s_n = f_n - s_{n-1}d_n$, then we have

$$\begin{array}{c}
P_n \\
\downarrow f_n \\
P'_{n+1} \xrightarrow{d'} d'(P'_{n+1}) \longrightarrow 0
\end{array}$$

and at that point we use the definition of projectivity.

Then finally we take $[\varphi] \in \text{Ext}_R^n(B, N)$ and we want to show it is sent to 0. Well, φ is a homomorphism $\varphi : P'_n \rightarrow N$ such that $\varphi \circ d'_{n+1} = 0$. This is mapped to $[\varphi \circ f_n] \in \text{Ext}_R^n(A, N)$ and we need that $\varphi \circ f_n = \psi \circ d_n$ for some $\psi : P_{n-1} \rightarrow N$. But, well,

$$\begin{aligned}
\varphi \circ f_n &= \varphi \circ (d'_{n+1}s_n + s_{n-1}d_n) \\
&= \varphi \circ d'_{n+1} \circ s_n + (\varphi \circ s_{n-1}) \circ d_n,
\end{aligned}$$

so we let $\psi = \varphi \circ s_{n-1}$, and we are done. □

25 May 5th

25.1 Last time

We fixed an R -module N and were looking at the functor $\text{Hom}_R(-, N) : \mathbf{R}\text{-Mod} \rightarrow \mathbf{Ab}$, which is contravariant and left exact. For an R -module A , we choose a projective resolution:

$$\cdots \rightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \rightarrow A \rightarrow 0.$$

Apply $\text{Hom}_R(-, N)$ and remove the A term to get

$$0 \rightarrow \text{Hom}_R(P_0, N) \rightarrow \text{Hom}_R(P_1, N) \rightarrow \cdots,$$

which is a cochain complex. So taking the n -th cohomology group for $n \geq 0$, we can define $\text{Ext}_R^n(A, N) = \ker(d^{n+1})/\text{im}(d^n)$, a set of derived functors. Note that $\text{Ext}_R^0(A, N) = \text{Hom}_R(A, N)$, the functor we started with, and that the choice of resolution doesn't matter. Also, a map $f : A \rightarrow B$ induces a map $f_* : \text{Ext}_R^n(B, N) \rightarrow \text{Ext}_R^n(A, N)$, so we really have a contravariant functor $\text{Ext}_R^n : \mathbf{R}\text{-Mod} \rightarrow \mathbf{Ab}$.

Example. Let $R = \mathbb{Z}$ and let $A = \mathbb{Z}/m\mathbb{Z}$. So we have a projective resolution

$$\cdots \rightarrow 0 \rightarrow 0 \rightarrow \mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \rightarrow A \rightarrow 0.$$

So when we apply $\text{Hom}_{\mathbb{Z}}(-, N)$ and remove the A term, we get

$$0 \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) = N \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) = N \rightarrow 0 \rightarrow \cdots,$$

where $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \cong N$ via evaluation at 1, and the induced map $N \rightarrow N$ is just multiplication by m .

Then

$$\text{Ext}_{\mathbb{Z}}^n(\mathbb{Z}/m\mathbb{Z}, N) \cong \begin{cases} mN = \{x \in N \mid mx = 0\} & \text{if } n = 0 \\ N/mN & \text{if } n = 1 \\ 0 & \text{if } n \geq 2. \end{cases}$$

△

Example. Let $R = \mathbb{Z}/m^2\mathbb{Z}$ and let $A = \mathbb{Z}/m\mathbb{Z}$; so our projective resolution is

$$\cdots \xrightarrow{\times m} R \xrightarrow{\times m} R \xrightarrow{\times m} R \rightarrow A \rightarrow 0,$$

and applying Hom_R and omitting A gives us

$$0 \rightarrow N \xrightarrow{\times m} N \xrightarrow{\times m} \cdots,$$

so

$$\text{Ext}_R^n(\mathbb{Z}/m\mathbb{Z}, N) = \begin{cases} mN & \text{if } n = 0 \\ mN/mN & \text{if } n \geq 1. \end{cases}$$

△

So all that remains is an analogue of that long exact sequence of homology.

Theorem 25.1.1. *Let $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ be a short exact sequence of R -modules. Then there is a long exact sequence*

$$\begin{aligned} 0 \rightarrow \text{Hom}_R(C, N) \rightarrow \text{Hom}_R(B, N) \rightarrow \text{Hom}_R(A, N) \\ \xrightarrow{\delta} \text{Ext}_R^1(C, N) \rightarrow \text{Ext}_R^1(B, N) \rightarrow \text{Ext}_R^1(A, N) \\ \xrightarrow{\delta} \text{Ext}_R^2(C, N) \rightarrow \cdots \end{aligned}$$

Sketch of proof. We examine the following diagram.

$$\begin{array}{ccccccc}
& \vdots & & \vdots & & \vdots & \\
& \downarrow & & \downarrow & & \downarrow & \\
0 & \longrightarrow & P_1 & \longrightarrow & P_1 \oplus P'_1 & \longrightarrow & P'_1 \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & P_0 & \longrightarrow & P_0 \oplus P'_0 & \longrightarrow & P'_0 \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & 0 & & 0 & & 0
\end{array}$$

If the left and right columns are projective resolutions, we claim we can fill in the middle arrows (in red), so that the middle column is exact and the diagram commutes.

The inductive step of this proof is that in the following step, we choose λ and μ so that the diagram commutes.

$$\begin{array}{ccccccc}
0 & \longrightarrow & P_n & \longrightarrow & P_n \oplus P'_n & \longrightarrow & P'_n \longrightarrow 0 \\
& & \downarrow & \searrow \lambda & \downarrow \pi & \swarrow \mu & \downarrow \\
0 & \longrightarrow & P_{n-1} & \longrightarrow & P_{n-1} \oplus P'_{n-1} & \longrightarrow & P'_{n-1} \longrightarrow 0
\end{array}$$

For λ this is easy. For μ , we use the fact that P'_n is projective, or use the fact that the short exact sequences are split (but for the base case, we must use the projectivity of P'_0 , since the bottom exact sequence may not be split).

So then we apply the functor to the entire diagram.

$$\begin{array}{ccccccc}
& \vdots & & \vdots & & \vdots & \\
& \uparrow & & \uparrow & & \uparrow & \\
0 \leftarrow \text{Hom}_R(P_1, N) & \longleftarrow & \text{Hom}_R(P_1 \oplus P'_1, N) & \longleftarrow & \text{Hom}_R(P'_1, N) & \longleftarrow & 0 \\
& \uparrow & & \uparrow & & \uparrow & \\
0 \leftarrow \text{Hom}_R(P_0, N) & \longleftarrow & \text{Hom}_R(P_0 \oplus P'_0, N) & \longleftarrow & \text{Hom}_R(P'_0, N) & \longleftarrow & 0 \\
& \uparrow & & \uparrow & & \uparrow & \\
& 0 & & 0 & & 0 &
\end{array}$$

This is a short exact sequence of cochain complexes. But a short exact sequence of cochain complexes gives a long exact sequence in cohomology, which is exactly the sequence we want. \square

The same argument works for any contravariant left exact functor $F : \mathbf{R}\text{-Mod} \rightarrow \mathbf{Ab}$; that's all we used in any of these proofs. So given a contravariant left exact functor F , we define $R^n F : \mathbf{R}\text{-Mod} \rightarrow \mathbf{Ab}$, the n -th right derived functor of F . And a short exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ leads to a long exact sequence $0 \rightarrow F(C) \rightarrow F(B) \rightarrow F(A) \xrightarrow{\delta} (R^1 F)(C) \rightarrow \dots$. The construct is the "exact" same as what we've already done for $\text{Hom}_R(-, N)$, with projective resolutions, applying the functor, and taking the n -th cohomology.

We can extend the idea even further by replacing $\mathbf{R}\text{-Mod}$ with any so-called *abelian category* (with enough projectives), and an example of that will be given...soon.

But for now, let's consider a covariant left exact functor $F : \mathbf{R}\text{-Mod} \rightarrow \mathbf{Ab}$ instead (no more switching arrows!). For example, $\text{Hom}_R(M, -)$. For an R -module A , choose an injective resolution

$$0 \rightarrow A \rightarrow Q_0 \rightarrow Q_1 \rightarrow \dots,$$

an exact sequence of injective modules. Then take the co-chain complex

$$0 \rightarrow F(Q_0) \rightarrow F(Q_1) \rightarrow \dots,$$

and define $(R^n F)(A)$ the n -th cohomology group. We won't do it here, because it's the same argument as the contravariant case, but one has to check that $R^n F : \mathbf{R}\text{-Mod} \rightarrow \mathbf{Ab}$ are well-defined covariant functors and that if you start with a short exact sequence you get the long exact sequence of derived functors that you want. In the special case when $F = \text{Hom}_R(M, -)$, the functors you get are called $\text{Ext}_R^n(M, -)$.

A big claim that we and the book both don't address is that the two definitions of $\text{Ext}_R^n(M, N)$ line up, i.e. that $\text{Ext}_R^n(-, N)(M) = \text{Ext}_R^n(M, -)(N)$.

Example. Let $R = \mathbb{Z}$. Let's try to understand $\text{Ext}_{\mathbb{Z}}^n(A, \mathbb{Z})$. We have an injective resolution

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \xrightarrow{\varphi} \mathbb{Q}/\mathbb{Z} \rightarrow 0,$$

where φ is the quotient map. Applying $\text{Hom}_{\mathbb{Z}}(A, -)$ and removing \mathbb{Z} gives us

$$0 \rightarrow \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}) \rightarrow \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) \rightarrow 0.$$

So then $\text{Ext}_{\mathbb{Z}}^0(A, \mathbb{Z}) = \text{Hom}_{\mathbb{Z}}(A, \mathbb{Z})$, since that's exactly what will be quotiented to 0. Also, $\text{Ext}_{\mathbb{Z}}^1(A, \mathbb{Z}) = \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) / \{\varphi \circ f \mid f \in \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q})\}$. Beyond that, they are all zero.

△

Example (Group cohomology.). Let G be a finite group, and consider the functor $F : \mathbb{Z}G\text{-Mod} \rightarrow \mathbf{Ab}$ given by $A \mapsto A^G = \{a \in A \mid ga = a \forall g \in G\}$.

Given a short exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$, we define group cohomology to be the derive dfunctors, so that we have a long exact sequence

$$0 \rightarrow A^G \rightarrow B^G \rightarrow C^G \xrightarrow{\delta} H^1(G, A) \rightarrow H^1(G, B) \rightarrow \dots$$

In other words, $H^n(G, A) = (R^n F)(A)$. Note that $A^G = \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$, so these are also $\text{Ext}_{\mathbb{Z}G}^n(\mathbb{Z}, A)$.

△

Example (Tor.). Consider a covariant right exact functor $F : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$, for example $M \otimes_R -$. For an R -module A , choose a projective resolution

$$\dots \rightarrow P_1 \rightarrow P_0 \rightarrow A \rightarrow 0.$$

Then apply F and remove A , to get

$$\dots \rightarrow F(P_2) \rightarrow F(P_1) \rightarrow F(P_0) \rightarrow 0.$$

This is a chain complex instead of a cochain complex, so we can define $(L_n F)(A)$ to be the n -th homology group of this complex. If one feels like going through the machinery again, one can show that $L_n F : \mathbf{R-Mod} \rightarrow \mathbf{Ab}$ is well-defined and covariant, and given a short exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$,

$$\dots (L_1 F)(A) \rightarrow (L_1 F)(B) \rightarrow (L_1 F)(C) \xrightarrow{\delta} F(A) \rightarrow F(B) \rightarrow F(C) \rightarrow 0.$$

If $F = M \otimes_R -$, we define $L_n F = \text{Tor}_n^R(M, -)$.

△

26 May 10th

26.1 The Cohomology of Groups

Let G be a finite group, let A be a $\mathbb{Z}G$ -module (or a G -module), i.e. an abelian group A with a G -action that respects the group law.

Consider the fixed point functor $\mathbb{Z}G\text{-Mod} \rightarrow \mathbf{Ab}$ given by $A \mapsto A^G = \{a \in A \mid ga = g\forall g \in G\}$, which is covariant and left exact.

Example. $G = \text{Gal}(\mathbb{C}/\mathbb{R})$; then $1 \rightarrow \{\pm 1\} \rightarrow \mathbb{C}^\times \rightarrow \mathbb{C}^\times \rightarrow 1$, where the $\mathbb{C}^\times \rightarrow \mathbb{C}^\times$ map is given by $x \mapsto x^2$, is a SES of G -modules. Applying the fixed point functor gives the SES $1 \rightarrow \{\pm 1\} \rightarrow \mathbb{R}^\times \rightarrow \mathbb{R}^\times \rightarrow 1$. Observe that $A^G = \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$, where f in $\text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$ corresponds to $f(1)$.

△

So we can look now at our derived functors.

Definition 26.1.1. The n -th cohomology group of G is given by

$$H^n(G, A) = \text{Ext}_{\mathbb{Z}G}^n(\mathbb{Z}, A).$$

So the sequence keeps going, giving us

$$0 \rightarrow A^G \rightarrow B^G \rightarrow C^G \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow \dots,$$

the long exact sequence.

Choose a projective resolution of \mathbb{Z} as a $\mathbb{Z}G$ -module. Define F_n to be $\mathbb{Z}G^{n+1}$, a free $\mathbb{Z}G$ -module with basis $(1, g_1, \dots, g_n)$, for $g_i \in G$. Then we have a free resolution

$$\dots \rightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z} \rightarrow 0,$$

where $d_n : F_n \rightarrow F_{n-1}$ is given by $(g_0, \dots, g_n) \mapsto \sum_{i=0}^n (-1)^i (g_0, \dots, \hat{g}_i, \dots, g_n)$.

Applying $\text{Hom}_{\mathbb{Z}G}(-, A)$ and removing the \mathbb{Z} term gives

$$0 \rightarrow \text{Hom}_{\mathbb{Z}G}(F_0, A) \rightarrow \text{Hom}_{\mathbb{Z}G}(F_1, A) \rightarrow \dots,$$

and then the n -th cohomology group $H^n(G, A)$. To get a better handle on this, we have

$$\begin{aligned} \text{Hom}_{\mathbb{Z}G}(F_n, A) &= \{\phi : G^{n+1} \rightarrow A \mid g\phi(g_1, \dots, g_{n+1}) = \phi(gg_1, \dots, gg_{n+1}) \forall g, g_i \in G\} \\ &= \{\varphi : G^n \rightarrow A\}, \end{aligned}$$

by saying that $\varphi(g_1, \dots, g_n) = \phi(1, g_1, \dots, g_n)$. We then have a chain complex

$$0 \rightarrow C^0(G, A) \xrightarrow{d} C^1(G, A) \xrightarrow{d} \dots,$$

where

$$(d\varphi)(g_1, \dots, g_{n+1}) = g_1\varphi(g_2, \dots, g_{n+1}) + \sum_{i=0}^n (-1)^i \varphi(g_1, \dots, g_{i-1}, g_i \cdot g_{i+1}, \dots, g_{n+1}) + (-1)^{n+1} \varphi(g_1, \dots, g_n).$$

So $Z^n(G, A)$, the group of cocycles, is $\{\varphi \in C^n(G, A) \mid d\varphi = 0\}$, and $B^n(G, A)$, the group of coboundaries, is $d(C^{n-1}(G, A))$.

Let's work out a special case.

$$H^1(G, A) = \frac{\{\varphi : G \rightarrow A \mid \varphi(\sigma\tau) = \sigma\varphi(\tau) + \varphi(\sigma) \forall \sigma, \tau \in G\}}{\{\varphi : G \rightarrow A \mid \exists a \in A, \varphi(g) = ga - a\forall g\}},$$

so when G acts trivially on A , this is just $\text{Hom}(G, A)$.

Assume that G is cyclic of order m , with $G = \langle \sigma \rangle$. Consider the “norm,” $N = 1 + \sigma + \dots + \sigma^{m-1} \in \mathbb{Z}G$. Then $N(\delta - 1) = (\delta - 1)N = \delta^m - 1 = 0$. We have a free resolution

$$\dots \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \rightarrow 0,$$

where $\varepsilon : \mathbb{Z}G \rightarrow \mathbb{Z}$ is just the sum of the coefficients. So we then have the cochain complex

$$0 \rightarrow \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \rightarrow \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \rightarrow \dots,$$

and each of these Hom groups is isomorphic to A . Then $H^0(G, A) = A^G$ and

$$H^n(G, A) = \begin{cases} NA/(\sigma - 1)A & \text{if } n \geq 1 \text{ odd} \\ A^G/NA & \text{if } n \geq 2 \text{ even.} \end{cases}$$

In this case $NA = \{a \in A \mid Na = 0\}$.

Recall from a long long time ago, Hilbert 90.

Theorem 26.1.2 (Hilbert 90.). *Let L/K be a finite Galois extension with $G = \text{Gal}(L/K)$ cyclic. If $a \in L^\times$ with $N_{L/K}(a) = 1$, then $a = \sigma(b)b^{-1}$ for some $b \in L^\times$.*

Hilbert 90 is the same result as saying that the group $H^1(G, L^\times) = 0$; for the latter statement, we don't need the cyclic assumption.

Using the short exact sequence $1 \rightarrow \{\pm 1\} \rightarrow \mathbb{C}^\times \rightarrow \mathbb{C}^\times \rightarrow 1$ from earlier as an example, the machinery we've developed gives the long exact sequence

$$\begin{aligned} 1 \rightarrow \{\pm 1\} \rightarrow \mathbb{R}^\times \rightarrow \mathbb{R}^\times \rightarrow H^1(\text{Gal}(\mathbb{C}/\mathbb{R}), \{\pm 1\}) &= \text{Hom}(\text{Gal}(\mathbb{C}/\mathbb{R}), \{\pm 1\}) = \mathbb{Z}/2 \\ &\rightarrow H^1(\text{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) = 0 \rightarrow \dots \end{aligned}$$

Sometimes, when the example is gnarlier, the machinery can tell you helpful things about these groups. We'll spend the rest of today talking about the groups $H^2(G, A)$ and seeing how they show up.

Definition 26.1.3. Fix a finite group G and an abelian group A . An *extension* of G by A is a short exact sequence of groups:

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 0.$$

For an extension E of G by A , let $s : G \rightarrow E$ be a function (not necessarily a homomorphism) such that $\pi \circ s = \text{id}$ and such that $s(1) = 1$. Then G acts on A via the action that for $g \in G$ and $a \in A$,

$$g \cdot a = i^{-1}(s(g) \cdot i(a) \cdot s(g)^{-1}) \in A.$$

This is a well-defined group action that at some point uses the fact that A is abelian. For $g, h \in G$, $s(gh)$ and $s(g)s(h)$ are both sent to gh by π , so $s(g)s(h)s(gh)^{-1} \in \ker \pi = \text{im } i$, so $i^{-1}(s(g)s(h)s(gh)^{-1}) \in A$. This gives a function $[\cdot, \cdot] : G^2 \rightarrow A$ depending on s , known as a “factor set.” This factor set is in $Z^2(G, A)$, and is an example of a cocycle showing up.

But since it’s in $Z^2(G, A)$, it gives an element of $H^2(G, A)$; while the cocycle may depend on your choice of s , the element of $H^2(G, A)$ will be independent of choice of s .

Theorem 26.1.4. Fix an action of G on A . Then for \sim the discussed equivalence of extensions, there is a bijective correspondence

$$\{\text{ext'ns of } G \text{ by } A \text{ inducing the given action}\} / \sim \longleftrightarrow H^2(G, A).$$

26.2 Central simple algebras

Let L/K be a finite Galois extension with $G = \text{Gal}(L/K)$. Take $\varphi \in Z^2(G, L^\times)$, and define B_φ to be the L -vector space of formal sums $\sum_{\sigma \in G} a_\sigma \cdot u_\sigma$, for u_σ a basis and $a_\sigma \in L$.

Give B_φ a multiplication, via $u_\sigma \cdot \alpha = \sigma(\alpha)u_\sigma$ for $\sigma \in G$ and $\alpha \in L$, and satisfying the relation $u_\sigma u_\tau = \varphi(\sigma, \tau) \cdot u_{\sigma\tau}$. Under this somewhat gnarly multiplication, B_φ is a ring, with K in the center of B_φ . It is a fact that B_φ is a central simple K -algebra, which says that:

- B_φ is a K -algebra;
- B_φ has no nontrivial left or right ideals; and
- The center of B_φ is K .

Similarly here, there’s a one-to-one correspondence

$$\{\text{fin. dim'l central simple } K\text{-alg } B \mid B \otimes_K L \cong M_n(L)\} / \sim \longleftrightarrow H^2(G, L^\times),$$

where we’re quotienting out by \sim , or “similarity,” where B_1 and B_2 are similar if $M_m(B_1) \cong M_n(B_2)$ for some m, n . $H^2(G, L^\times)$ is also called $\text{Br}(L/K)$, the *relative Brauer group*, with group law $[B_1] \cdot [B_2] = [B_1 \otimes B_2]$.

Example. $H^2(\text{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) \cong \mathbb{Z}/2$, and is in bijection with finite dimensional central simple \mathbb{R} -algebras. This set consists of \mathbb{R} and \mathbb{H} . One can do the same thing with $H^2(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \overline{\mathbb{Q}}^\times)$, which is some gigantic fun thing.

△