MATH 776: CLASS FIELD THEORY

These are notes I have taken from an ongoing course taught by Professor Andrew Snowden at the University of Michigan. For suggestions and corrections of errors, email edeany@umich.edu.

Note: For k-algebras A and B, I write $[A, B]_k$ for the set of k-algebra maps from A to B. I routinely use the fact that, if K/k is an algebraic field extension, then all elements of $[A, A]_k$ are isomorphisms. This justifies using the notation $[K, K]_k$ for the Galois group of K over k when K/k is algebraic. This is a small departure from the notation from Professor Snowden's lectures.

1. Thursday, January 10th

Definition 1. An abelian extension of a field k is a field extension K/k of k whose Galois group $[K, K]_k$ is Abelian.

Definition 2. For a group G and a field k, a G-extension of k is a Galois field extension K/k such that $G \cong [K, K]_k$.

An important problem is to understand the abelian extensions of a given ground field k. To motivate us, we can start by thinking about specific cases involving small groups. Throughout, fix a field k of characteristic 0. We aim to describe G-extensions, where G is some small group of our choosing.

Example 3. Take $G = \mathbb{Z}/2\mathbb{Z}$. Any $\mathbb{Z}/2\mathbb{Z}$-extension has the form $k(\sqrt{d})$ for some $d \in k$ which is not a square. To see this, note that such an extension K/k must have degree $\dim_k(K) = |\mathbb{Z}/2\mathbb{Z}| = 2$, so that it must be of the form $k(a)$ for a the root of a degree 2 polynomial $ax^2 + bx + c$. From the quadratic formula, the roots of this polynomial will be $\pm\sqrt{B^2/4 - C} - B/2$, where $B = b/a$ and $C = c/a$. We get $k(a) = k(\sqrt{B^2/4 - C})$.

It is no harder to show that d is unique in $k^\times/((k^\times)^2)$.

Example 4. Take $G = \mathbb{Z}/3\mathbb{Z}$. Take an irreducible polynomial in $k[t]$ of degree 3, and let K be a splitting field of f over k.

$G = [K, K]_k$ is isomorphic to a subgroup of S_3: since k has characteristic 0, f is separable and therefore has three distinct roots in K. Let S be the set of roots of f in K. There is a group homomorphism $\phi : G \to \mathrm{Bij}(S)$ from G to the group of bijections of S, isomorphic to S_3. $\sigma \in G$ is determined by its values on the roots of f, so that ϕ is injective.

In fact, G is isomorphic to a transitive subgroup of S_3, since for any two roots a and b of f, one can construct a k-automorphism $\sigma : K \to K$ with $\sigma(a) = b$. A transitive

subgroup of S_3 must have order at least 3, so that, by enumeration of the subgroups of S_3, it must be A_3 or S_3. We have a theorem characterizing precisely when G is A_3 and when it is S_3.

Theorem. *G is A_3 if and only if the discriminant $\mathrm{disc}(f)$ is a square in k.*

Proof. Factor $f(t) = (t-\alpha)(t-\beta)(t-\gamma)$ in $K[t]$, and write $\delta = (\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$. Recall that the discriminant of f is $\mathrm{disc}(f) = \delta^2$.

For $\sigma \in S_3$, we have $\sigma(\delta) = \mathrm{sgn}(\sigma)\delta$. So

$$G \subset A_3 \iff \forall g \in G : g \in A_3 \iff \forall g \in G : g(\delta) = \delta \iff \delta \in k \iff \mathrm{disc}(f) \in k^2$$

□

Example 5. In the example above, we may take $f(t) = t^3 + at + b$, where $a, b \in k$. One can calculate that $\mathrm{disc}(f) = -4a^3 - 27b^2$. So, to get a $\mathbb{Z}/3\mathbb{Z}$-extension of k, we may pick $a, b \in K$ such that $f(t)$ is irreducible and $-4a^3 - 27b^2 \in K^2$. For instance, taking $k = \mathbb{Q}$, $a = -3$, and $b = -1$, so that $f(t) = t^3 - 3t - 1$, we get $\mathrm{disc}(f) = 81 \in \mathbb{Q}^2$. The splitting field of $f(t)$ is then a $\mathbb{Z}/3\mathbb{Z}$-extension of $\mathbb{Q}$.

Example 6. Take $G = \mathbb{Z}/4\mathbb{Z}$. Suppose K/k is a $\mathbb{Z}/4\mathbb{Z}$-extension. As there is one nontrivial subgroup of $\mathbb{Z}/4\mathbb{Z}$, there is a unique intermediate field F of the extension K/k. Since F/k is a quadratic extension, there is some $d \in k$ with $F = k(\sqrt{d})$. Since K/F is a quadratic extension, there is some element $\alpha+\beta\sqrt{d}$ of F such that $K = F(\sqrt{\alpha+\beta\sqrt{d}})$.

Now, for which $\alpha, \beta, d \in K$ is K/k a (Galois) $\mathbb{Z}/4\mathbb{Z}$-extension? More precisely, can you find a necessary (but possibly insufficient) criterion for K/k to be a $\mathbb{Z}/4\mathbb{Z}$-extension? There are trivial things to require here (for instance, that $\beta \neq 0$), but here is a nontrivial one:

If K/k is Galois, then the map $[K,K]_k \to [F,F]_k$ sending $\sigma : K \to K$ to the restricted, arestricted map $\sigma|_F^F : F \to F$ is well defined, as F/k is a normal field extension. The unique non-identity element of $[F,F]_k$ then lifts to an element σ of $[K,K]_k$, which must send $\sqrt{d}$ to $-\sqrt{d}$, so that $\sigma(a) = a$ for each $a \in k$, and $\sigma(\sqrt{d}) = -\sqrt{d}$. Then $\sigma(\sqrt{a+b\sqrt{d}}) = \pm\sqrt{a-b\sqrt{d}}$, which in particular is an element of K. Hence, for K/k to be Galois, it is necessary that $\sqrt{a-b\sqrt{d}}$ be contained in K.

This condition is necessary, but still insufficient. A condition that is sufficient as well as necessary is given by requiring that there be $\gamma \in K$ such that $\alpha - d\beta^2 = d\gamma^2$.

To see that this condition is necessary, suppose K/k is a $\mathbb{Z}/4\mathbb{Z}$-extension. Let σ be a generator of the Galois group of K/k. Write $x = \sqrt{\alpha+\beta\sqrt{d}}$ and $y = x\sigma(x)$.

If $y \in K$, then $y = \sigma(y)$, so $x\sigma(x) = \sigma(x)\sigma^2(x)$, so that $x = \sigma^2(x)$. So $x \in k(\sqrt{d})$, a contradiction. So $y \notin K$.

$y^2 \in K$: $x^2 = \alpha + \beta\sqrt{d}$, and $y^2 = x^2\sigma(x^2) = \alpha^2 - \beta^2 d$. So $\gamma^2 y^2 = \alpha^2 - d\beta^2$ for some $\gamma \in k$ using our example on $\mathbb{Z}/2\mathbb{Z}$-extensions. This shows that it is necessary that there be $\gamma \in k$ such that $\alpha - d\beta^2 = d\gamma^2$.

Corollary 7. *$k(\sqrt{d})$ fits into a $\mathbb{Z}/4\mathbb{Z}$-extension if and only if d is the sum of two squares in k.*

Proof. Recall that $\{x \in k^\times | x$ is the sum of two squares in $k\}$ is a subgroup of $k^\times$. □

Example 8. Take $k = \mathbb{Q}$, $d = 5$, $\alpha = 5, \beta = 1$, and $\gamma = 2$. Then $\mathbb{Q}(\sqrt{5+\sqrt{5}})$ is a $\mathbb{Z}/4\mathbb{Z}$-extension of $\mathbb{Q}$.

Proposition 9 (Kummer)**.** *Take $G = \mathbb{Z}/n\mathbb{Z}$. If k contains all nth roots of 1, then any G-extension has the form $k(\sqrt[n]{a})$ for some $a \in k$.*

Recall that a Cyclotomic extension is an extension built from adjoining roots of 1. Taking $k = \mathbb{Q}$, we can form the cyclotomic extension $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. The minimal polynomial of ζ_n over $\mathbb{Q}$ is the Cyclotomic polynomial $\Phi_n(x)$, which is the unique irreducible polynomial with integer coefficients that is a divisor of $x^n - 1$ and not a divisor of $x^k - 1$ for $k < n$. Its roots are the primitive nth roots of unity, i.e. elements of the form $e^{2\pi ik/n}$ with $\gcd(k, n) = 1$. It is a theorem, shown in most introductory field theory and Galois theory courses, that $\Phi_n(x)$ is irreducible.

Set $n \in \mathbb{N}_{\geq 1}$, and set $\zeta_n = e^{2\pi i/n}$ for concreteness. There is a canonical map $\chi : [\mathbb{Q}(\zeta_n), \mathbb{Q}(\zeta)_n]_{\mathbb{Q}} \to (\mathbb{Z}/n\mathbb{Z})^\times$ sending $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta)_n$ to the unique a (coprime to n) such that $\sigma(\zeta_n) = \zeta_n^a$.

This function is in fact a homomorphism: take a, b relatively prime to n such that $\sigma(\zeta_n) = \zeta_n^a$ and $\tau(\zeta_n) = \zeta_n^b$. Then

$$\sigma \circ \tau(\zeta_n) = \sigma(\zeta_n^b) = \sigma(\zeta_n)^b = (\zeta_n^a)^b = \zeta_n^{ab} = \zeta_n^{\chi(\sigma)\chi(\tau)}$$

Now $\chi(\sigma \circ \tau) = \chi(\sigma)\chi(\tau)$ in $\mathbb{Z}/n\mathbb{Z}^\times$.

That χ is injective is clear enough from the fact that an automorphism on the simple extension $\mathbb{Q}(\zeta_n)$ is determined by its value on ζ_n. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, we have $\#[\mathbb{Q}(\zeta_n), \mathbb{Q}(\zeta_n)]_{\mathbb{Q}} = \dim_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) = \deg(\Phi_n) = \phi(n)$, where $\phi(n)$ is Euler's ϕ-function. Hence χ is an injection between sets of the same finite cardinality, and therefore a bijection.

This argument shows that $\chi : [\mathbb{Q}(\zeta_n), \mathbb{Q}(\zeta_n)]_{\mathbb{Q}} \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

This result allows us to find G-extensions for small G with ease. Take some composite number $n = p_1^{k_1} \cdots p_n^{k_n}$, where $p_1, ..., p_n$ are distinct primes. Then

$$[\mathbb{Q}(\zeta_7), \mathbb{Q}(\zeta_7)]_{\mathbb{Q}} \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \left(\prod_{i=1}^n \mathbb{Z}/p_i^{k_i}\mathbb{Z}\right)^\times \cong \prod_{i=1}^n \mathbb{Z}/p_i^{k_i}\mathbb{Z}^\times \cong \prod_{i=1}^n \mathbb{Z}/(p_i - 1)p_i^{k_i - 1}\mathbb{Z}$$

So, for instance, $[\mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_5)]_{\mathbb{Q}} \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ and $[\mathbb{Q}(\zeta_7), \mathbb{Q}(\zeta_7)]_{\mathbb{Q}} \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$.

Exercise 1. *Use $\mathbb{Q}(\zeta_n)$ to show that every finite abelian group appears as the Galois group of a Galois extension of $\mathbb{Q}$.*

Soon we will show a remarkable theorem, stating that the cyclotomic extensions of $\mathbb{Q}(\zeta_n)$, and their subextensions, with corresponding quotient Galois groups, are the only abelian extensions of $\mathbb{Q}$. This is known as the Kronecker-Weber theorem:

Theorem. *(Kronecker-Weber) Exery finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)$ for some n.*

This theorem has an interesting corollary as well:

Theorem. *Let $G_{\mathbb{Q}}$ be the absolute Galois group of $\mathbb{Q}$. The canonical maps of rings $\mathbb{Q}(\zeta_n) \to \mathbb{Q}^{sep}$ induce maps $G_{\mathbb{Q}} \to \mathbb{Z}/n\mathbb{Z}^\times$, and hence a map $G_{\mathbb{Q}} \to lim\mathbb{Z}/n\mathbb{Z}^\times \cong \hat{\mathbb{Z}}^\times$ into their limit. The target here is an abelian group, and so factors through a map $\chi : G_{\mathbb{Q}}^{ab} \to \hat{Z}^\times$. $\chi : G_{\mathbb{Q}}^{ab} \to \hat{\mathbb{Z}}^\times$ is an isomorphism.*

One of the main accomplishments of Class Field Theory is a description of G_K^{ab} for any number field K.

Theorem. *The maximal everywhere-unramified abelian extension of k is finite, and its degree h_k (class number). Its Galois group is canonically isomorphic to $Cl(K)$.*

Here is our plan for the course:

1. Prove the Kronecker-Weber Theorem
2. Statements of Class Field Theory
3. Applications of Class Field Theory
4. Group Cohomology
5. Local Class Field Theory
6. Global Class Field Theory
7. Additional Topics, if time permits

2. Tuesday, February 12th

Let A be an abelian category. For those of us unfamiliar with this notion, an abelian category is a category which behaves like the category of modules over a ring. One can talk about kernels and cokernels, direct sums, and in general treat the objects as though they have elements like modules over a ring do. Abelian categories are the right level of generality for homological algebra. They treat simultaneously the case of R-modules, chain complexes, and sheaves of R-modules.

Definition 10 (Chain Complexes)**.** Let A be an abelian category. A chain complex in A is a pair $(M_n, d_n)_{n \in \mathbb{Z}}$, where $M_n \in \mathrm{Obj}(A)$ and $d_n : M_n \to M_{n-1}$ is a map such that

$d_{n-1} \circ d_n = 0$.

$$\cdots \to M_n \xrightarrow{d_n} M_{n-1} \xrightarrow{d_{n-1}} M_{n-2} \xrightarrow{\cdots}$$

Typically, we just write M_* for a chain complex, and just $d = d_n$.

Note: when A is the category of K-modules for a ring K, we can think of chain complexes in A as certain $K[\epsilon]/\epsilon^2 K[\epsilon]$ modules.

A morphism of chain complexes of $M_* \to N_*$ consists of giving a morphism $f_n : M_n \to N_n$ such that all the corresponding diagrams commute for each $n \in \mathbb{Z}$:

$$\begin{array}{ccc} M_n & \xrightarrow{d} & M_{n-1} \\ \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} \\ N_n & \xrightarrow{d} & N_{n-1} \end{array}$$

We get a category $\mathrm{Ch}(A)$ of chain complexes in A, and in fact this is an abelian category. If M_* is a chain complex, then $d_{n-1} \circ d_n = 0$, so $\mathrm{Im}(d_{n+1}) \subset \ker(d_n) \subset M_n$. The group $H_n(M_*) = \ker(d_n)/\mathrm{Im}(d_{n+1})$ is the nth homology of M_*. M_* is said to be 'acyclic' or 'exact' if all the homologies vanish.

$H_n : \mathrm{Ch}(A) \to A$ is a functor; if $f : M_* \to N_*$ is a map of chain complexes, then f_n induces a map $H_n(f) : H_n(M) \to H_n(N)$. $f : M_* \to N_*$ is called a quasi-isomorphism if all of these maps are isomorphisms.

Remark. We also have a notion of cochain complexes, where the indices are superscripts, and the differentials increase degree instead of decreasing degree. This is merely a matter of reindexing.

2.1. **Homotopies.**

Definition 11. Let $f : M_* \to N_*$ be a moprhism of complexes. We say f is null homotopic if there are maps $s_n : M_n \to N_{n+1}$ such that $f = s_n d + d s_n$ for each $n \in \mathbb{Z}$.

$$\begin{array}{ccccc} M_{n+1} & \xrightarrow{d} & M_n & \xrightarrow{d} & M_{n-1} \\ \downarrow{\scriptstyle f_{n+1}} & \swarrow{\scriptstyle s_n} & \downarrow{\scriptstyle f_n} & \swarrow{\scriptstyle s_{n-1}} & \downarrow{\scriptstyle f_{n-1}} \\ N_{n+1} & \xrightarrow{d} & N_n & \xrightarrow{d} & N_{n-1} \end{array}$$

$f, g : M_* \to N_*$ are chain homotopic if $f - g$ is null homotopic.

In particular, a null homotopic map induces 0 on homology.

One reason to consider chain homotopy is that chain homootpic maps induce the same map on homology:

Proposition 12. *If $f, g : M_* \to N_*$ are chain homotopic, then they induce equal maps $H_n(M) \to H_n(N)$ for all n. In particular, if f is null homotopic, then it induces 0 in homology.*

Proof. In fact, it suffices to show that a null homotopic map induces 0 on homology. Suppose f is null homotopic, so that there are maps $s_n : M_n \to N_{n+1}$ such that $f_n = s_{n-1} d + d s_n$ for each $n \in \mathbb{Z}$. Consider $H_n(M) \xrightarrow{f} H_n(N)$. Given $x \in H_n(M) = \ker(d_n)/\mathrm{im}(d_{n+1})$, pick $y \in \ker(d_n)$ lifting x. By definition, $f(x)$ is the

class of $f_n(y)$ in $H_n(N)$. $f_n(y) = s_{n-1}(dy) + d(s_n y) \in \mathrm{im}(d)$. Since $y \in \ker(d)$, $dy = 0$, so $s_{n-1}(dy) + d(s_n y) = d(s_n y)$. Now $d(s_n y) \in \mathrm{Im}(d)$, so the class of y is 0 in $H_n(N)$. Hence $f_n(y) = 0$ in $H_n(N)$. □

Definition 13. The homotopy category of $\mathrm{Ch}(A)$, denoted $K(A)$, is the following category: the objects are chain complexes, and the morphisms are homotopy classes of morphisms.

The proposition implies that the homology functor factors through $K(A)$.

$$\begin{array}{ccc} \mathrm{Ch}(A) & \longrightarrow & K(A) \\ \downarrow{\scriptstyle \mathrm{H}_n} & \swarrow{\scriptstyle \mathrm{H}_n} & \\ A & & \end{array}$$

Two complexes M_* and N_* are called homotopy equivalent if there are maps $f : M_* \to N_*$ and $g : N_* \to M_*$ such that fg is homotopic to Id_N, gf is homotopic to Id_M.

Suppose we have a short exact sequence of complexes

$$0 \to A_* \to B_* \to C_* \to 0$$

Let $c \in C_n$ be such that $dc = 0$. Choose $b \in B_n$ lifting c. The image of db_n in C_{n+1} is $dc = 0$, so that we may choose $a = db \in A_{n-1}$. Suppose b' is a second lift of C. Then we can write $b' = b + \epsilon$, $\epsilon \in A_n$. Then $a' = a \in \mathrm{im}(A_{n-1} \to A_n)$, $a' = a$ in $H_{n-1}(A)$.

Now suppose $c = dc'$ for some $c' \in C_{n+1}$. Let $b' \in B_{n+1}$ be a lift of c' Then $b = db'$ is a lift of c. $c = db = d^2 b' = 0$. So $c \mapsto 0$

$$\begin{array}{ccccc} A_n & \longrightarrow & B_n & \longrightarrow & C_n \\ \downarrow & & \downarrow & & \downarrow \\ A_{n-1} & \longrightarrow & B_{n-1} & \longrightarrow & C_{n-1} \end{array}$$

The map ∂ is called the connecting homomorphism. We have a long exact sequence

$$\cdots \overset{H}{\to}_{n+1} (C_*) \overset{H}{\to}_n (A_*) \to H_n(B_*) \to H_n(C_*) \overset{\partial}{\to} H_{n-1}(A) \to \cdots$$

This sequence is exact. This is left as an exercise. This association is functorial.

2.2. **Projectives and Injectives.**

Definition 14. An object P of A is projective if, whenever $p : M \to N$ is an epimorphism, and f is a given map, there is g such that $p \circ g = f$.

$$\begin{array}{ccc} & & P \\ & \overset{\exists}{\swarrow} & \downarrow \\ M & \overset{\forall}{\twoheadrightarrow} & N \end{array}$$

Equivalently, $\mathrm{Hom}(P, -)$ is exact. We say A has enough projectives if every object is a quotient of some projective.

Definition 15. Dual notion is called injective. An object I in A is injective if, for each monomorphism $i : N \to M$ in A, and each map $f : N \to I$, there is $g : M \to I$ such that $g \circ i = f$.

$$\begin{array}{ccc} & & I \\ & \overset{f}{\nearrow} & \uparrow{\scriptstyle g} \\ N & \overset{i}{\hookrightarrow} & M \end{array}$$

Equivalently, $\mathrm{Hom}(-, I)$ is exact.

Example 16. Let A be the category of R-modules for a ring R. Then

(1) Any free R-module is projective.
(2) Any ideal in a Dedekind domain is projective.
(3) $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are injective $\mathbb{Z}$-modules.

2.3. **Projective Resolutions.**

Definition 17. Let $M \in A$. A projective resolution of M is an exact sequence

$$\cdots \to P_2 \to P_1 \to P_0 \xrightarrow{\epsilon} M \to 0$$

with each P_i projective. We call ϵ the augmentation map. P_* is the complex

$$\cdots \xrightarrow{P}_2 \xrightarrow{P}_1 \xrightarrow{P}_0 \to 0 \to 0 \cdots$$

We can regard M as a complex in degree 0. Then $\epsilon : P_* \to M$ is a quasi-isomorphism. $P_* \to M$, where M is the chain complex centered in degree zero:

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \epsilon} & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

So, do projective resolutions exist? If A has enough projectives, then every object has a projective resolution.

Proposition 18. *If A has enough projectives, every object has a projective resolution.*

Resolutions are unique up to homotopy.

Proposition 19. *Let $\epsilon : P_0 \to M$ be a projective resolution, let $\delta : Q_* \to N$ be any resolution, and let $f : M \to N$ be a morphism in A. Then there is a map of complexes $g : P_* \to Q_*$ lifting f. Furthermore, if g' is a second lift, then g and g' are chain homotopic.*

Note that we're note assuming that Q_* is a projective resolution at all.

Proof.

$$\begin{array}{ccccccc} \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \\ & \downarrow & \searrow & \downarrow & \searrow & \downarrow & \\ \longrightarrow & Q_2 & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \end{array}$$

To prove the second part, it suffices to assume $f = 0$ and show that the lift of the 0 map is 0. We may lift g_0 onto Q_1 by S_1. Having lifted g_0 to s_0, $g_1 - s_0 d$ then lifts to s_1: to see this, set $h = g_1 - s_0 d$, and note that $dh = dg_1 - ds_0 d = 0$. Inductively, $g_n - s_{n-1} d$ always lifts to s_n, so that $ds_n = g_n - s_0 d$. □

Corollary 20. *Any two projective resolutions of M are homotopy equivalent.*

Proof. Let $P_* \to M$ and $Q_* \to M$ be projective resolutions. We can lift 1_M to maps $f_* : P_* \to Q_*$ and $g_* : Q_* \to P_*$. Then $g_* \circ f_*$ and 1_{P_*}, as lifts of 1_M, are homotopy equivalent maps. Similarly, $f_* \circ g_*$ and 1_{Q_*} are homotopy equivalent. This shows that f_* and g_* are inverse isomorphisms in the homotopy category of chain complexes. □

Corollary 21. *There is a functor $\pi : A \to K(A)$ assigning to each A a non-augmented projective resolution of A.*

Proposition 22. *Proposition (horseshoe lemma) $0 \to L \to M \to N \to 0$ exact sequence in A. Let $\epsilon : P \to L$ and $\phi : R \to N$ be projective resolutions. Let $Q_n = P_n \oplus R_n$. There are maps $g_n : R_n \to P_{n-1}$ such that $Q_n \to Q_{n-1}$ $(x, y) \mapsto (dx + g_n y, dy)$ makes Q_* into a complex and $\Delta : Q_* \to M$ is a projective resolution of M. Proof left as an exercise.*

2.4. **Derived Functors.** Assume A has enough projectives. Let B be a second abelian category. Let $F : A \to B$ be a right exact functor; F is additive (i.e. $F(M \oplus N) = F(M) \oplus F(N)$), and given exact sequence $A \to B \to C \to 0$, then $F(A) \to F(B) \to F(C) \to 0$ is exact.

Example 23. Let A be $\mathrm{Mod}|_R$, R a commutative ring. Fix $N \in A$. Define $F : A \to B$, $M \mapsto M \otimes_R N$. This is a right exact functor. It's exact if and only if N is flat.

Definition 24. Let $i \in \mathbb{Z}$. The ith derived fucntor of F is denoted $L_i F$ is $(L_i F)(M) = H_i(F(P_*))$, where P_* is a projective resolution of M. In other words L_i is the composition $A \xrightarrow{\pi} K(A) \xrightarrow{F} K(B) \xrightarrow{H_i} B$. Note that $L_i F = 0$ for $i < 0$.

Proposition 25. $L_0 F = F$.

Proof. Let $P_* \to M$ be a projective resolution, so that $P_1 \to P_0 \to M \to 0$ is exact. Then $F(P_1) \to F(P_0) \to F(M) = 0$ is exact, since F is right exact. That says that $F(M)$ is the cokernel of $F(P_1) \to F(P_0)$, so that $L_0 F(M) = H_0(F(P)) = F(M)$. □

Proposition 26. *Consider a short exact sequence in $0 \to M_1 \to M_2 \to M_3 \to 0$ in A. There is a long exact sequence*

$$\cdots \to L_1(M_2) \to L_1(M_3) \to L_0(M_1) \to L_0(M_2) \to L_0(M_3) \to 0$$

3. Thursday, February 14th

Last time it was shown how, given a right exact functor $F : A \to B$ between abelian categories, there are functors $L_i F$ of F, which we may form by taking $(L_i F)(M) = H_i(F(P_*))$ for a projective resolution $\epsilon : P \to M$. It then follows that

(i) $L_i F = 0$ for $i < 0$
(ii) $L_0 F = F$
(iii) $L_i F(P) = 0$ for any projective P for $i \neq 0$.

(iv) There is a long exact sequence in L_iF's associated to a short exact sequence in A.

In fact, these properties characterize L_i:

Proposition 27. *Given a functor $F_* : A \to B$ such that*

(1) $F_i = 0$ for $i < 0$,
(2) $F_0 = F$,
(3) Functorial long exact sequence in T's for each SES in A.
(4) $F_i(P) = 0$ if $i > 0$, P projective.

Then there is a natural isomorphism $F_i \cong L_iF$.

Proof. It suffices to show that a $\mathbb{Z}$-indexed sequence of functors F_* satisfying (i), (ii), (iii), and (iv) is terminal among functors satisfying (i), (ii), and (iii). We show the case for F_1; the rest are similar and work via a simple induction argument. To proceed, take a functor F_* satisfying (i), (ii), (iii), and (iv), and a functor G_* satisfying (i), (ii), and (iii).

Take an object $M \in \mathrm{Obj}(A)$ and an exact sequence $0 \to K \to P \to M \to 0$ with P projective. This gives two exact sequences,

$$\cdots \to F_1(K) \to F_1(P) \to F_1(M) \to F(K) \to F(P) \to F(M) \to 0$$

and

$$\cdots \to G_1(K) \to G_1(P) \to G_1(M) \to F(K) \to F(P) \to F(M) \to 0$$

We have a commutative diagram:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & G_1(P) & \longrightarrow & G_1(M) & \longrightarrow & F(K) & \longrightarrow & F(P) \\
 & & & & & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \mathrm{Id}} \\
\cdots & \longrightarrow & F_1(P) & \longrightarrow & F_1(M) & \longrightarrow & F(K) & \longrightarrow & F(P)
\end{array}$$

Now $F_1(P) = 0$, so that $F_1(M) \to F(K)$ is a kernel map. By the universal property of the kernel, there is a unique map $G_1(M) \to F_1(M)$ making the diagram below commute:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & F_1(P) & \longrightarrow & F_1(M) & \longrightarrow & F(K) & \longrightarrow & F(P) \\
 & & & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \mathrm{Id}} \\
\cdots & \longrightarrow & G_1(P) & \longrightarrow & G_1(M) & \longrightarrow & F(K) & \longrightarrow & F(P)
\end{array}$$

This gives maps $G_1(M) \to F_1(M)$ for each M which assemble into a natural tranformation using the functoriality of (iii). □

3.1. **Ext.** Let M and N be objects in A. Define a functor $[M, -] : A \to \mathrm{Ab}$ sending X to $[M, -] = \mathrm{Hom}(M, X)$, and define a functor $[-, N] : A^{op} \to \mathrm{Ab}$ sending Y to $[Y, N] = \mathrm{Hom}(Y, N)$. Both of these are left-exact (note that the determination of whether a functor is left or right exact is made using the target category, not the domain category). If A has enough injectives, then we may form $R^*[M, -]$. If A^{op} has

enough injectives (i.e. A has enough projectives), then we may form $R^*[-, N]$.

Proposition 28. *If A has enough injectives, then $R^*[M, -](N) \cong R^*[-, N](M)$.*

Proof. Fix an object M in A. We will show that N maps to $R^i[-, N](M)$ is the derived functor of $[M, -]$ by checking the conditions in proposition 27.

(i) This is immediate.
(ii) We can note that $R^0[-, N](M) = [M, N] = [M, -](N)$.
(iii) Let $0 \to N_1 \to N_2 \to N_3 \to 0$. Take a projective resolution of M, and apply $H^i([P_*, -])$ to $0 \to N_1 \to N_2 \to N_3 \to 0$. We get an exact sequence because P_i is projective. So

$$0 \to \mathrm{Hom}(P_*, N_1) \to \mathrm{Hom}(P_*, N_2) \to \mathrm{Hom}(P_*, N_3) \to 0$$

is an exact seqeucne of complexes, so we get a long exact sequence in homology.
(iv) We must show that $R^i[-, I](M) = 0$ for an injective I in $i > 0$. Take a projective resolution $P_* \to M$. Then $R^i[-, I](M)$ is the ith cohomology of the complex $[P_*, I]$. Now P_* is an exact sequence and $\mathrm{Hom}(-, I)$ is an exact functor.

□

Assume A has enough projectives or enough injectives. Define Ext^i to be the ith right derived functor of Hom. $\mathrm{Ext}^*(M, N)$ can be computed using a projective resolution of M or an injective resolution of N.

Example 29. To compute $\mathrm{Ext}^i(\mathbb{Z}/n\mathbb{Z}, M)$, take the projective resolution $\cdots \to 0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to 0$ of $\mathbb{Z}/n\mathbb{Z}$. Hom with M to get

$$0 \to \mathrm{Hom}(\mathbb{Z}, M) \xrightarrow{n} \mathrm{Hom}(\mathbb{Z}, M) \to \mathrm{Hom}(0, M) \to 0$$

Taking homology, we get $M[n]$ in degree 0 and M/nM in degree 1.

3.2. **Tor.** Say R is a ring, which is not necessarily commutative. Let M be a right R-module and N a left R-module. Define $M \otimes_R - : R\text{-mod} \to \mathrm{Ab}$ $X \mapsto M \otimes_R X$ and $- \otimes_R M : \text{mod-}R \to \mathrm{Ab}$, Y maps to $Y \otimes_R N$.

Proposition 30. $L_i M \otimes_R -(N) \cong L_i - \otimes_R M(N)$

The proof here is just like before.

Definition 31. Tor_i is the left derived functor of $- \otimes_R -$.

3.3. **G-modules.**

Definition 32. For a group G, a G-module is an abelian group M with a left action of G, where G acts linearly. That is, $g(x + y) = gx + gy$ for each $g \in G$ and each $x, y \in M$. This is equivalent to a left module over the group algebra $\mathbb{Z}[G]$. We write Mod_G for the category of G-modules. This category has enough projectives and injectives, since it is a module category.

Note: we can pass in between $\mathbb{Z}[G]$-modules. If M is a right $\mathbb{Z}[G]$-modules, then setting $gx = xg^{-1}$ for $g \in G$, $x \in M$ gives a left $\mathbb{Z}[G]$-module structure.

If M and N are left $\mathbb{Z}[G]$-modules, then we define two tensor products: $M \otimes_{\mathbb{Z}} N$, the ordinary tensor product of abelian groups, is a $\mathbb{Z}[G]$-module where $g(x \otimes y) = gx \otimes gy$. $M \otimes_G N$ is the tensor product over $\mathbb{Z}[G]$, thinking of M as a right module. $M \otimes_G N = M \otimes_R N / \{g^{-1}x \otimes y = x \otimes gy\}$.

If M is G-mod, put $M^G = \{x \in M | gx = x \forall g \in G\}$. The functor $M \mapsto M^G$ is left exact; this can be seen from the fact that it is naturally isomorphic to $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, where $\mathbb{Z}$ is a $\mathbb{Z}[G]$ module with trivial action. Write $H^i(G, -)$ (group cohomology) for the ith right derived functor. Explicitly, $H^i(G, M) = H^i((I^*)^G)$ where $M \to I_*$ is injective resolution of M as a G-module. Viewing $\mathbb{Z}$ as a G-module with trivial action, $M^G \cong \mathrm{Hom}_G(\mathbb{Z}, M)$, so that $H^i(G, M) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

By the balancing property of Ext, we can compute this using a projective resolution of $\mathbb{Z}$. We get to choose any resolution, and so we arrive at the question of whether there is a best resolution to choose. There is indeed a resolution more useful than the others, and it is called the Bar resolution.

Let P_r be the free $\mathbb{Z}$-module with basis G^{r+1}. We'll write $[g_0, ..., g_r]$ for the basis element of P_r corresponding to $(g_0, ..., g_r) \in G^{r+1}$. We give this the structure of a G-module where $g \cdot (g_0, ..., g_r) = (gg_0, ..., gg_r)$. P_r is a G-module via $g[g_0, ..., g_r] = [gg_0, ..., gg_r]$. P_r is a free $\mathbb{Z}[G]$-module since G^{r+1} is a free G-set. We build the Bar resolution using these as the terms. We define a differential $d : P_r \to P_{r-1}$, where $[g_0, ..., g_r]$ maps to $\sum_{i=0}^{r}(-1)^i[g_0, ..., \hat{g}_i, , ..., g_r]$. We define $\epsilon : P_0 \to \mathbb{Z}$ to send $[g]$ to 1. One can check that $d^2 = 0$ and $\epsilon d = 0$.

Proposition 33. *The complex*

$$\cdots \to P_2 \xrightarrow{d} P_1 \xrightarrow{d} P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

is exact.

Proof. We will construct a null-homotopy. Pick $h \in G$ arbitrarily. Define $s_r : P_r \to P_{r+1}$ sending $[g_0, ..., g_r] \mapsto [h, g_0, ..., g_r]$. Set $s_{-1} : \mathbb{Z} \mapsto P_0$ to send 1 to $[h]$.

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & \mathbb{Z} \\
 & & \downarrow & \swarrow^{s_1} & \downarrow & \swarrow^{s_0} & \downarrow & \swarrow^{s_{-1}} & \downarrow \\
\cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & \mathbb{Z}
\end{array}$$

It is not hard to show that $ds_r + s_{r-1}d = \mathrm{Id}$ on P_r. Similarly, $\epsilon s_{-1} = \mathrm{Id}$ on $\mathbb{Z}$. This shows that the identity map of this complex is null homotopic, so that Id and 0 induce the same map on H_i, so that $H_i = 0$. □

Remark. The maps s_* are not G-equivariant. Indeed, the proof shows the existence of a chain complex which is null homotopic is $K(\mathbb{Z})$, but not null homotopic in $K(\mathrm{Mod}_G)$. So we have a complex which is acyclic but not null homotopic.

Corollary 34. $H^i(G,M) = H^i(Hom_G(P_*,M))$.

Let's examine this more closely. An element of $\mathrm{Hom}_G(P_r,M)$ corresponds to a G-equivariant map $G^{r+1} \to M$. We call these maps homogenous r-cochains. Write $\tilde{C}^r(G,M)$ for the group of maps $\phi : G^{r+1} \to M$ such that $\phi([gg_0,...,gg_r]) = g\phi([g_0,...,g_r])$. $d : \tilde{C}^r(G,M) \to \tilde{C}^{r+1}(G,M)$ sends $\phi([g_0,...,g_{r+1}])$ to $\sum_{i=0}^{r+1}(-1)^i\phi([g_0,...,\hat{g}_i,...,g_{r+1}])$. We define $\tilde{Z}^r(G,M) = \ker(d|_{\tilde{C}^r(G,M)})$ and $\tilde{B}^r(G,M) = \mathrm{Im}(d|_{\tilde{C}^{r-1}(G,M)})$.

Proposition 35. $H^i(G,M) = \tilde{Z}^i(G,M)/\tilde{B}^i(G,M)$.

Definition 36. An inhomogeneous R-cochain is an arbitrary function $G^r \to M$. Write $C^r(G,M)$ for the group of these. Given $\phi \in C^r(G,M)$ define $d\phi \in C^{r+1}(G,M)$ by

$$d\phi(g_1,...,g_{r+1}) = g_1\phi(g_2,...,g_{r+1}) + \sum_{i=1}^{r}(-1)^i\phi(g_1,...,g_ig_{i+1},...,g_r) + (-1)^{r+1}\phi(g_1,...,g_r)$$

We have an isomorphism $\tilde{C}^r(G,M) \to C^r(G,M)$ sending ϕ to the function sending $(g_1,...,g_r) \mapsto \phi([1,g_1,g_1g_2,g_1g_2,g_3,...,g_1\cdots g_r])$. This is compatible with d's. We then define inhomogeneous r-cocycles $Z^r(G,M) = \ker(d|_{C^r})$, and inhomogeneous r-coboundaries $B^r(G,M) = \mathrm{im}(d|_{C^{r-1}})$.

Proposition 37. $H^i(G,M) = Z^i(G,M)/B^i(G,M)$, *and* $H^0(G,M) = M^G$.

Example 38. Now look at $H^1(G,M)$. An element of $Z^1(G,M)$ is a function $\phi : G \to M$ such that $d\phi = 0$. $d\phi$ means $\phi(gh) = g\phi(h) + \phi(g)$. This is called a crossed homomorphism from G into M. $B^1(G,M)$ consists of functions $\phi : G \to M$ such that $\phi(g) = dx(g) = gx - x$ for some x. These are called principal crossed homomorphisms.

Proposition 39. *Now we have the following formula for* H^1*:*

$$H^1(G,M) \cong \{\phi : G \to M | \phi(gh) = g\phi(h) + \phi(g) \forall g,h \in G\}/\{\phi : G \to M | \exists x \in G : \phi(g) = gx - x\}$$

Note that, if G acts trivially on M, then a crossed homomrphsims is simply a homomorphism $G \to M$, and a principal crossed homomorphism is 0. So $\mathrm{H}^1(G,M)$ is $\mathrm{Hom}_{Grp}(G,M)$.

3.4. **Galois Cohomology.** Suppose G is profinite. A discrete G-module is a G-module M such that, for any $x \in M$, $\{g \in G | gx = x\}$ is an open subgroup of G; this is the same as saying that the action of G on M is continuous. If M has finite rank as a $\mathbb{Z}$-module, then discrete is the same as saying that the action factors through a finite quotient of G.

Definition 40. Define $H^i(G,M)$ as the derived functor of $(\,)^G$ on the category of discrete G-modules (it can be shown that this has enough injectives). We have $H^i(G,M) = \lim_{U \subset G} H^i(G/U, M^U)$.