About These Notes

These are notes taken from Math 594 at the University of Michigan, taught during the Winter 2019 Semester by Professor Andrew Snowden. All of these notes were typed by Vignesh Jagathese (me!) during the 2019 semester, though the notes were finally organized only by the end of 2021. There are still some minor errors in these notes, and by reading these and benefiting from them, all I ask in return is that you forward any errors to me.

Some information on the course can be found below, followed by a table of contents. These are organized into lecture by lecture notes, with key examples highlighted in the table of contents. In terms of necessary background, this is not meant to be a first time introduction to abstract algebra, so some familiarity with the basic terms will be assumed. You should probably know what a tensor product is, as well as be very comfortable with theoretical linear algebra. Math 593 (the previous course at Michigan) is more than enough background.

This should serve as adequate preparation for half of an algebra prelim exam at most Universities (Math 594 is a 2nd semester prelim preparation course at Michigan). While there are no exercises given, I do hope that you can find some of your own in the various textbooks covering this material (my favorite is *Algebra, Chapter 0* by Paulo Aluffi, though Lang's and Dummit & Foote's books are great references).

Syllabus Summary:

Office Hours: Monday and Thursday: 9:30 - 11:00AM

Course Structure: Math 594 will be split into 4 roughly equal parts, discussing Group Theory, Representation Theory, Field Theory, and Galois Theory. The course is "seriously graded", and is intended to introduce students to the fundamental aspects of Algebra, as well as prepare them for the PhD qualifying exam. The class assumes a basic knowledge of algebra, i.e. what a group, ring, and field are, and some basic properties about them. Since the first part of the class is primarily focused on groups, the initial lectures should serve as a good review of elementary group theory. Similarly, around the half way mark, introductory lectures on field theory will serve as a good review of fields.

Homework is assigned weekly, and (usually) due on Tuesdays. 12 homeworks will be assigned, with the lowest two being dropped. **Grades** will be evaluated as follows:

1. Homeworks 15%
2. Midterm 35%
3. Final 50%

Contents

Math 594: Algebra II **Winter 2019**

Lecture 1: January 10th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

1.1 Group Theory Basics

1.1.1 Basic Definitions

We define a ***group*** to be a set G with a binary operation $\cdot : G \times G \to G$ such that:

1. $\cdot$ is associative: $(xy)z = x(yz)$.
2. $\exists$ an identity 1 such that $\forall g \in G$, $1g = g1 = g$.
3. Every element has an inverse, i.e. $\forall x \in G$, $\exists y$ such that $xy = yx = 1$.

One can prove that the identity is unique, and that the inverse element for a given $x \in G$ is unique. This is why we denote 1 as THE identity, and denote x^{-1} as THE inverse of x.

Note that commutativity (that $ab = ba \; \forall a, b \in G$) is not required. Groups with this property are called ***abelian groups***. When not all of the elements in a group commute with everything, it is important to consider the elements of a group that do commute with everything. This is called the ***center*** of G, denoted $Z(G)$.

$$Z(G) := \{x \in G \mid xy = yx \; \forall y \in G\}$$

If a group has a finite number of elements, we say that the number of elements in G is the ***Order*** of G, and is denoted $\#G$. Subsets of groups can also be groups, and the nice ones are called ***subgroups***.

For a given group G, a subset of G denoted H is a subgroup of G provided that

1. H retains the identity: $1 \in H$
2. H has closure: $\forall a, b \in H$, $ab \in H$
3. H has inverses: $\forall h \in H, h^{-1} \in H$

When H is a subgroup of G, we often write $H \leq G$.

1.1.2 Group Homomorphisms

For groups $(G, \cdot), (H, \times)$, a ***Group Homomorphism*** $f : G \to H$ is a function such that $\forall x, y \in G$, $f(x \cdot y) = f(x) \times f(y)$, and $f(1_G) = 1_H$. For $1_G, 1_H$ being the identities of G and H respectively. If this map is bijective, we say that f is a ***Group Isomorphism***, and if f is an isomorphism from G onto itself (i.e. $f : G \to G$) then f is a ***Group Automorphism***.

If two for any two groups G, H, if $\exists$ an isomorphism $f : G \to H$, then we say that G and H are isomorphic, and that $G \cong H$. In algebra, two groups being isomorphic essentially means they are the same. When we count the number of groups with a certain property, or talk about collections of groups, they are often counted "up to isomorphism", since for any group there are obviously infinitely many groups isomorphic to it.

1.2 Examples of Groups

1.2.1 The Zero Group

For a trivial example, consider $G = \{1\}$. It is easy to check this is a group; note that the empty set $\emptyset$ is not a group, because there must exist an identity.

1.2.2 $(\mathbb{Z}, +)$

The integers under addition do form a group, where 0 is the obvious additive identity. A common mistake is to assume that $(\mathbb{Z}, \times)$ is also a group. This is NOT a group, since even though 1 is the identity, nearly every element in this group does not have an inverse. In fact, only $\{\pm 1\}$ have inverses in $(\mathbb{Z}, \times)$.

1.2.3 The Symmetric Group on n Letters, S_n

We define the ***symmetric group*** on n Letters, denoted S_n, as follows:

$$S_n := \{f : \mathbb{N}_n \to \mathbb{N}_n \mid f \text{ is bijective}\}$$

Where $\mathbb{N}_n$ denotes the set of natural numbers $\{1, \ldots, n\}$. A keen observer may notice that these are precisely the permutations on n letters! We have a convenient notation for these sorts of maps. The map that corresponds to $(i_1, \ldots, i_k)$ is the map which sends $i_1 \to i_2, i_2 \to i_3, \ldots, i_{k-1} \to i_k$, and $i_k \to i_1$. Any elements in $\mathbb{N}_n$ that have not showed up in $(i_1, \ldots, i_k)$ are fixed. Since this only affects k elements, we denote this as a ***k-cycle***. It is easy to check that this is a group; the identity is just the identity map $\text{Id} : \mathbb{N}_n \to \mathbb{N}_n$, composition of functions is associative, and since each f is a bijection, its inverse, f^{-1} is also

a bijection from $\mathbb{N}_n$ to $\mathbb{N}_n$. As an example, we write out all of S_3 below:

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}$$

Where (1) is the identity map. It is pretty easy to check that $\#S_n = n!$. The case where $n = 3$ is above. In general, note that for a list $\{1, \ldots, n\}$, we need to define a map back to $\{1, \ldots, n\}$. 1 can map to any of $\{1, \ldots, n\}$, meaning there are n possibilities for mapping 1. 2 can be mapped anywhere except where 1 was mapped to (if 2 is mapped to where 1 is mapped to, f would no longer be injective, and thus no longer binjective), so 2 has $n - 1$ possible images. 3 would have $n - 2$ by similary logic. Continuing this way ensures that $\#S_n = n(n-1)(n-2)\cdots = n!$.

1.2.4 The Free Group on 2 letters, F_2

For letters a, b we define the ***Free Group*** on 2 letters as follows. Elements are formal words in letters a, a^{-1}, b, b^{-1}, with a notion of equivalence that makes sense (i.e. $abb^{-1}a \equiv aa$). Multiplication is just concatanation, i.e.

$$(aba^{-1})(aabb) = aba^{-1}aabb \equiv ababb$$

To show this is a group, concatanation is associative, we can let aa^{-1} denote the identity, and inverses follow from distributing the inverse symbol across terms, as in a regular group. In addition, Free Groups have a ***Mapping Property***. For any group G, and for any $x, y \in G$, $\exists!$ group homomorphism $f : F_2 \to G$ such that $f(a) = x, f(b) = y$. Proving this is not particularly difficult, existence is trivial and uniqueness follows from the properties of a group homomorphism.

1.2.5 The General Linear Group, $\mathrm{GL}_n(R)$

The ***General Linear Group*** is the set of $n \times n$ invertible matrices with coefficients in R, where R can be anything up to a (not necessarily commutative) ring, though usually it is a field. In other words,

$$\mathrm{GL}_n(R) = \{X \in \mathrm{Mat}_{n\times n}(R) \mid \det(X) \neq 0\}$$

The General Linear Group is in fact a group, with the operation being matrix multiplications. $\mathrm{Id}_n \in \mathrm{GL}_n(R)$, matrix multiplication is associative, and invertibility of elements in $\mathrm{GL}_n(R)$ guarantees inverses.

1.2.6 The Dihederal Group, D_n

Before defining the Dihederal Group, we first build up some basics. Let X be a planar figure of some kind. For our purposes, let $X \subset \mathbb{R}^2$ be this planar figure. A ***rigid motion*** of $\mathbb{R}^2$ is

a bijective, continuous, distance preserving map. The set of all rigid motions is denoted Γ. This clearly forms a group under composition. Consider

$$G := \{\gamma \in \Gamma \mid \gamma(X) = X\}$$

We claim that $G \leq \Gamma$. To show this, note that:

1. Composition of functions is associative
2. The identity map, 1, clearly maps $X \to X$
3. If $\gamma(X) = X$, $\gamma^{-1} \circ \gamma(X) = \gamma^{-1}(X)$, implying that $X = \gamma^{-1}(X)$, guaranteeing inverses.
4. $\gamma(X) = X$ and $\gamma'(X) = X$ implies that $\gamma \circ \gamma'(X) = \gamma(X) = X$, as desired, so we are closed under composition.

We now suppose that X is a regular hexagon. G would then contain rotations by (multiples of) $60°$, and reflections through the center of the hexagon. It is true that the composition of a rotation and a rotation is again a rotation, and the composition of a rotation and a reflection is a reflection. Similarly, the composition of two reflections is a rotation. This follows from the preservation of orientation. Since Γ contains distance preserving maps, the maps are orthogonal, and thus have determinant ± 1. If the determinant is 1, then the map is orientation preserving, and is precisely a rotation. If the determinant is -1, the map is orientation reversing, and is precisely a reflection. The relations above can be checked by multiplying -1 and 1 together with each other and themselves in various ways. While we won't prove this, the following lemma holds:

Lemma 1.1. *Let a be any reflection, and b be any rotation. a has order 2, and b has order 6. Every element of G has the form b^k or ab^k for a unique k such that $0 \leq k \leq 5$.*

By a counting argument, this implies that $\#G = 12$. We define G to be the ***Dihedral Group*** on 6 sides, denoted D_6. Observe that $aba = b^{-1}$. In other words, reflecting, rotating then reflecting again yields the inverse rotation. Using this, we can concretely give D_6 the following presentation:

$$D_6 = \{a, b \mid a^2 = 1, b^6 = 1, ab = b^{-1}a\}$$

Note that this can be extended to D_n just by replacing each 6 with an n. Thus, D_n can be considered to be the automorphisms of a regular n-gon.

1.2.7 Quarternion Group, Q

Consider the set

$$Q := \{\pm 1, \pm i, \pm j, \pm k\}$$

With the following relations:

$$i^2 = j^2 = k^2 = (-i)^2 = (-j)^2 = (-k)^2 = -1$$

$$ij = -ji = k, ik = -ki, jk = -kj$$

This is the ***Quarternion Group***.

1.2.8 The Cyclic Group, C_n

Consider the group

$$C_n := \{1, g, g^2, \ldots, g^{n-1}\}$$

With the obvious group operations, and with the rule that $a^i = a^j$ precisely when $i \equiv j \bmod n$. This group clearly has order n, and is ***generated*** by one element, g.

1.3 Quotient Groups

1.3.1 Cosets

A ***left coset*** of H in G is a set of the form

$$gH := \{gh \mid h \in H\}$$

For some $g \in G$. A ***right coset*** is defined similarly:

$$Hg := \{hg \mid h \in H\}$$

Example: Consider $G = \mathbb{Z}, H = 2\mathbb{Z}$. H corresponds to the even integers. A coset of H is of the form $n + H$ for some $n \in \mathbb{Z}$. In practice, the cosets are precisely $0 + H$ and $1 + H$, where the former is the even integers, and the latter is the odd integers.

Lemma 1.2. *Any two left cosets are either equal or disjoint.*

Proof. Let $gH, g'H$ denote two cosets that are not disjoint. If we show that they are equal, then we're done. Choose $x = gh = g'h'$. This implies that $g = g'h'h^{-1}$, so $g \in g'H$, as $h'h^{-1} \in H$. A similar proof shows that $g' \in gH$. Thus, for any $g'h \in g'H$, $g' \in gH \Rightarrow g'h \in gH$. Similarly, for any $gh \in gH$, $g \in g'H \Rightarrow gh \in g'H$, allowing us to conclude that $gH = g'H$. □

This means that left cosets can partition the group. This means that it is important to consider the number of cosets made by a given subgroup. We define the ***index*** of H in G, denoted $[G : H]$, to be the number of left cosets. It is easy to check that the number of left cosets equals the number of right cosets (consider the explicit bijection $gH \to Hg^{-1}$ such that $gh \mapsto hg^{-1}$). Furthermore, the cardinality of left and right cosets have equal cardinality (just the cardinality of H, consider the bijections $H \to gH, H \to Hg$). From this, we can conclude the following lemma.

Lemma 1.3. *Let G be a (finite) group, and H be a subgroup of G.*

$$[G : H] = \frac{\#G}{\#H}$$

Since $[G : H]$ is a count and thus some positive whole number, this result allows us to conclude Lagrange's Theorem:

Theorem 1.4. ***(Lagrange)*** *Let G be a (finite) group, and H be a subgroup of G. Then, the order of H divides the order of G.*

From this we get the following corrolary:

Lemma 1.5. *If $g \in G$, then the order of g divides the order of G.*

This follows from considering the (cyclic) subgroup generated by g, denoted (g).

1.3.2 Normal Subgroups

Let G be a group, and $H \leq G$ be a subgroup. H is ***normal*** if $\forall g \in G, h \in H$, $ghg^{-1} \in H$. Note that for any $g_1, g_2 \in G$, $g_1 g_2 g_1^{-1}$ is the ***conjugate*** of g_2 by g_1. Thus, a normal subgroup is a subgroup which is closed under conjugation by any element in G, not just the elements in H. From this, we see the following lemma

Lemma 1.6. *if H is normal, then $\forall g \in G$, $gH = Hg$.*

Proof. Let $h \in H, g \in G$. Because H is normal, $h' \in H$.

$$ghg^{-1} = h' \Rightarrow gh = h'g \Rightarrow gH = Hg$$

□

Thus, for a normal subgroup, there is no distinction between left and right cosets. Thus, we refer to them as just ***cosets***.

1.3.3 Defining the Quotient Group

Let G be a group, and $H \leq G$ be a normal subgroup of G. The ***quotient group***, denoted G/H, is defined as follows:

$$G/H := \{gH \mid g \in G\}$$

Where multiplication is defined the obvious way:

$$(gH)(g'H) := gg'H$$

Checking this is a group is not particularly hard. Note that the normality of H is required for G/H to be a group.

There exists a natural (surjective) group homomorphism $\pi : G \to G/H$ such that $\pi(g) = gH$. π is the ***projection map*** from G to G/H.

Example: Consider $G = \mathbb{Z}, H = 2\mathbb{Z}$ again. $G/H = \{0 + H, 1 + H\}$. Note that $(1 + H) + (1 + H) = (1 + 1) + H = 2 + H$. Since H is precisely the even integers, $2 + H = H = 0 + H$.

Math 594: Algebra II **Winter 2019**

Lecture 2: January 15th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

2.1 Group Actions

2.1.1 Basics

let G be a group. We define a ***action*** of G on a set X to be the function

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto gx \end{aligned}$$

Such that

1) Identity is preserved: $\forall x \in X$, $(1, x) \mapsto 1x = x$
2) The action is associative: $g(hx) = (gh)x$

Remark: This is actually the definition of a ***left group action***, since the group element g is acting on the left. A ***right group action*** is defined similarly. In this class, we will primarily be concerned with left group actions, as right group actions are functionally the same.

A set X which G acts on is referred to as a G***-set***.

2.1.2 Orbits and Stabilizers

Let X be a G-set, $x \in X$. We say that the ***Orbit*** of x is the set of things in X that x can map to from the given action by G. More formally, we write

$$\mathcal{O}_x := \{gx \mid g \in G\} \subset X$$

We say the ***Stabilizer*** of x is the set of group elements in G that fix x. More formally,

$$G_x := \{g \in G \mid gx = x\} \subset G$$

Lemma 2.7. *$G_x \leq G$. (that is, G_x is a subgroup of G for any $x \in X$)*

Proof. Fix $x \in X$, G_x the stabilizer of x. Suppose $g, h \in G_x$. We wish to show that $gh \in G_x$.

$$gh(x) = g(h(x)) = gx = x$$

We now show that for $g \in G_x$, $g^{-1}x \in G_x$.

$$g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = x$$

Thus, we can conclude that $G_x \leq G$. □

We say that an action of G on X is ***Transitive*** provided that any element in X can be moved to another by the group action. In other words, $\forall x, y \in X$, $\exists g$ such that $gx = y$. Equivalently, $\mathcal{O}_x = X$ $\forall x \in X$. However, this condition can be relaxed slightly and we still gain transitivity.

Lemma 2.8. *If $\exists x \in X$ such that $\mathcal{O}_x = X$, then the action on X by G is transitive.*

Proof. Fix $y, z \in X$. We want to show that $\exists g \in G$ such that $gy = z$. Well, Since $\mathcal{O}_x = X$, $\exists g_1, g_2 \in G$ such that $g_1 x = y, g_2 x = z$. Let $g = g_2 g_1^{-1}$.

$$gy = g(g_1 x) = g_2 g_1^{-1}(g_1)x = g_2(g_1^{-1}g_1)x = g_2 x = z$$

□

We say that the action of G on X is ***Faithful*** if the map $x \mapsto gx$ is injective. In other words, an action is faithful if $gx = hx$ $\forall x \in X$ implies that $g = h$.

Often, X has some additional structure on it. Rather than just a set, it could be a ring, a field, or any other algebraic structure. If the action on g preserves this structure, we say that g ***acts by _____ automorphism***. The blank can be filled by whatever structure X has.

2.2 Examples of Group Actions

2.2.1 The Symmetric Group acting on $\{1, 2, \ldots, n\}$

Let $G = S_n$, and $X = \mathbb{N}_n = \{1, 2, \ldots, n\}$. Recall that elements of S_n are precisely bijections on $\mathbb{N}_n$ to itself. Thus we define the action the obvious way.

$$g \cdot x = g(x)$$

We first check that this follows axioms 1) and 2) of a group action.

1) The identity element of S_n is the identity map. Clearly, $\mathrm{Id}(x) = x$.

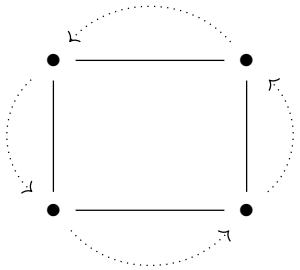
2) The group action being associative follows from function composition being associative. $(gh) \cdot x = g(h(x)) = g \cdot (h \cdot x)$.

This action is also transitive. To see this, Suppose $x \neq y$ for some $x, y \in X$ (the case where they are the same is trivial). We can just take the permutation σ which swaps x, y and fixes all other variables. It is easy to see that $\sigma(x) = y$. As for understanding the stabilizer, we can check that for any $x \in X$, $G_x \cong S_{n-1}$. To see this, take the isomorphism $S_n \to G_x$ which takes a permutation on $n-1$ elements to the permutation that fixes our x and permutes the remaining $n-1$ in accordance with the preimage permutation. It is easy to check that this is a group isomorphism.

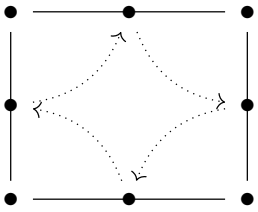
2.2.2 The Dihederal group of order 8 acting on the square

Let $G = D_4$, $X =$ a square $\subset \mathbb{R}^2$. We classify the orbits of points $x \in X$. We have three cases:

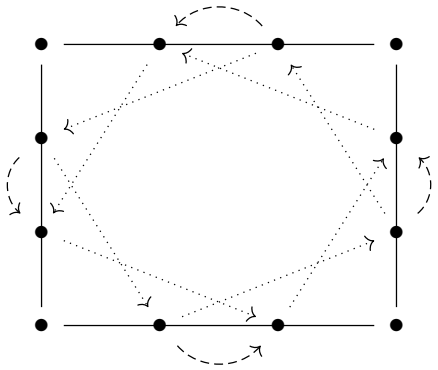
Case 1: Suppose that x is on the vertex of the square. The action can rotate the square by 90 degrees, or reflect the vertex to the vertex on the opposite side of the square. Both of these operations can only yield other vertices, implying that the orbit of x is simply the other vertices on the square, so $\#\mathcal{O}_x = 4$.



Case 2: Suppose that x is the midpoint of a given side of a square. Similarly to above, the rotations and reflections would only yield other midpoints of sides on the square. Thus, the orbit of x contains precisely all 4 midpoints of edges of the square, and $\#\mathcal{O}_x = 4$.



Case 3: If x is anywhere else on the square, then rotations will yield 4 reachable points. After applying a reflection, 4 more points can be reached. The 8 total reachable points are precisely those that are as far away from each vertex of the square as x is to its nearest/farthest vertex. Thus, $\#\mathcal{O}_x = 8$.



2.2.3 The Orthogonal group $\mathrm{O}_2(\mathbb{R})$ acting on $\mathbb{R}^2$

Recall that elements of $O_2(\mathbb{R})$ have a matrix representation. Thus, $O_2(\mathbb{R})$ acts on $\mathbb{R}^2$ the obvious way; by plugging vectors into the matrix.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}$$

First, considering the degenerate case, if $x = (0, 0)$, then $\mathcal{O}_x = \{0\}$ and $G_x = O_2(\mathbb{R})$. We now study the non-degenerate cases. Suppose that $x = (x_1, x_2) \neq 0$. Since Orthogonal maps preserve distance, an orthogonal map can take x to any vector which has the same norm. In other words,

$$\mathcal{O}_x = \{y \in X \mid \|y\| = \|x\|\}$$

This is precisely the circle of radius $\|x\|$ in $\mathbb{R}^2$. Similarly, the only actions which fix x are the trivial action and, if x lies on the x or y axis, the action which reflects about that axis. Thus, $\#G_x = 1$ (or 2 if one of x_1 or x_2 is zero).

2.2.4 The Special Linear Group acting on the upper half plane of $\mathbb{C}$

Let $G = \mathrm{SL}_2(\mathbb{R}) = \{M \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) \mid \det(M) = 1\}$. We define X to be the upper half plane in $\mathbb{C}$, which contains precisely the complex numbers with positive imaginary part. Actions are defined by ***linear fractional transformations*** as such:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \frac{az + b}{cz + d}$$

It is easy to check that this is a group action. This action is in fact transitive. To check this, we show that $\mathcal{O}_i = X$. From Lemma 2.8, we know that this it is sufficient to check only the case where $x = i$. Suppose we want to find a $g \in \mathrm{SL}_2(\mathbb{R})$ such that $gi = z \in \mathbb{C}$ for $z = x + iy$. Set

$$\begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} \cdot i = a^2 i + ab$$

For $a^2 i + ab$ to equal $x + iy$, let $a = \sqrt{y}, b = x/a$.

But what about G_i? We want to find the matrices $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ which fix i. Well,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot i = \frac{ai + b}{ci + d} = \frac{(bd + ac) + (ad - bc)i}{c^2 + d^2}$$

Since $ad - bc = 1$ (since we are in $\mathrm{SL}_2(\mathbb{R})$), it follows that for our matrix to be in the stabilizer of i, $c^2 + d^2 = 1$ and $ac + bd = 0$. From this, we can conclude that $G_i = \mathrm{SO}_2(\mathbb{R})$!

2.2.5 G acting on the quotient group G/H

Recall that G/H is the set of all cosets. This is a group if and only if H is a normal subgroup. However, if H is not-normal subgroup, G/H is still a set that G can act on. Defining the action the obvious way:

$$g \cdot (g'H) = gg'H$$

gives us a well defined group action. This action is in fact transitive. To see this, to take $g_1 H \to g_2 H$ simply set $g = g_2 g_1^{-1}$.

$$(g_2 g_1^{-1}) g_1 H = (g_2 g_1^{-1} g_1) H = g_2 H$$

We now compute the stabilizer. If $x = H$, then

$$G_H = \{g \in G \mid gH = H\} = \{g \in G \mid g \in H\} = H$$

If $x = gH$,

$$G_{gH} = \{g' \in G \mid g'H = gH\} = gHg^{-1}$$

These are both easy to check. This is an interesting result, and is true (in some sense) for any G-set X.

Lemma 2.9. *If X is a G-set, with $x \in X$, $g \in G$, then $G_{gx} = gG_x g^{-1}$.*

Proof. We first check that $gG_x g^{-1} \subset G_{gx}$. Fix $h \in G_x$.

$$ghg^{-1}(gx) = (ghg^{-1}g)(x) = ghx = gx$$

So ghg^{-1} stabilizes gx. The $\supset$ case is similar. □

2.3 Maps of G-sets

If X and Y are G-sets, a ***G-map***, or G equivariant map, is a function $f : X \to Y$ such that $f(g \cdot x) = g \cdot f(x)$, $\forall g \in G, x \in X$. An ***isomorphism of G-sets*** is a bijective G-map. We say that two G sets are isomorphic if there exists an isomorphism of G-sets between them.

Theorem 2.10. *Suppose X is a transitive G-set, and $x \in X$, then map*

$$\begin{aligned} f : G/G_x &\to X \\ gGx &\mapsto gx \end{aligned}$$

Is a well defined isomorphism of G-sets.

Proof. We first check that this map is well defined. Suppose that $gG_x = hG_x$ for some $g, h \in G$. We wish to show that $gx = hx$. Well, if $gG_x = hG_x$, then $h^{-1}g \in G_x$. This implies that

$$gx = h(h^{-1}gx) = (hh^{-1})gx = gx$$

As desired. We now show that f is in fact a G-map.

$$f(g \cdot hG_x) = f(ghG_x) = ghx = g(hx) = g \cdot f(hG_x)$$

To conclude, we show that this is an isomorphism. Set $f(gG_x) = f(hG_x)$. This implies that $gx = hx$. From above, we've proven that $gx = hx \iff gG_xhG_x$ (the same proof works in reverse), so we can conclude that f is injective. As for surjectivity, this is where we use the transitivity of the action. $\forall y \in X$, $\exists g$ such that $gx = y$. Thus

$$f(gG_x) = gx = y$$

Thus, f is a well defined isomorphism of G-sets. □

2.3.1 A Counting Formula For Orbits and Stabilizers

We state an important corollary to the above theorem.

Lemma 2.11. *if G is a finite group that acts on X, and $x \in X$, the order of the orbit of x times the order of the stabilizer of x is the order of G. More concretely,*

$$\#\mathcal{O}_x \cdot \#G_x = \#G$$

Proof. We first prove that $\mathcal{O}_x$ is a transitive G-set. Given $g \in G$, $y \in \mathcal{O}_x$ then $y = hx$ for some h. Well, $gy = ghx$, so $gy \in \mathcal{O}_x$. By the definition of an orbit, $\mathcal{O}_x$ is also clearly transitive. Thus we can cite Theorem 2.10, implying that $G/G_x \cong \mathcal{O}_x$ as G-sets. Because G is finite, this implies that $\#G/\#G_x = \#\mathcal{O}_x$, and the result follows. □

This corollary can be used to prove some interesting combinatorial results.

Example: Define X to be the set of all words of length 9, where the words are comprised of precisely 4 a's, 3 b's, and 2 c's. What is the size of X?

S_9 acts on X by permuting the position of the characters. It is clear that this action is transitive, the justification is similar to the example in 2.2.1. Furthermore, for $x \in X$, note that

$$G_x \cong S_4 \times S_3 \times S_2$$

Since the 4 a's can be permuted with themselves without changing the word, as can the 3 b's and the 2 c's with themselves. Applying lemma 2.11, we get that

$$\#X = \#S_9/\#G_x = \#S_9/(\#S_4 \times \#S_3 \times \#S_2) = \frac{9!}{4!\,3!\,2!}$$

Remark: This is actually called the ***multinomial formula***. We write

$$\binom{a+b+c}{a \quad b \quad c} = \frac{(a+b+c)!}{a!\,b!\,c!}$$

which counts the number of ways to choose 3 disjoint subsets A, B, C from a set of size $a+b+c$, where $\#A = a$, $\#B = b$, and $\#C = c$.

2.3.2 Cayley's Theorem

Suppose X is a set, let $\mathrm{Aut}(X)$ be the set of all bijections from X to itself. This is a group under composition, and if $\#X$ is finite, then $\mathrm{Aut}(X) \cong S_{\#X}$. Observe that giving a G action is the same as giving a group homomorphism $G \to \mathrm{Aut}(X)$. This takes an element g to the map which takes $c \mapsto gx$, which is clearly a bijection, and thus a member of $\mathrm{Aut}(X)$. Furthermore, G acts on itself faithfully by left multiplication ($g \cdot h = gh$). This gives us that $G \to \mathrm{Aut}(G)$ is an injective map. We use this to establish the following Theorem.

Theorem 2.12. *(Cayley) If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.*

Proof. G injects into $\mathrm{Aut}(G)$, and $\mathrm{Aut}(G) \cong S_n$, so the result follows. □

Math 594: Algebra II **Winter 2019**

Lecture 3: January 17th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

3.1 Conjugacy Classes and The Class Equation

3.1.1 An Issue With Right Multiplication Defining a Group Action

Last lecture, we defined an action on G by itself by left multiplication (i.e. $g \cdot h = gh$ $\forall g, h \in G$). This is very clearly a group action. What would happen if we tried to define an action on G by right multiplication? In other words,

Question: is the action $g \cdot h = hg$ a group action?

Answer: NO. This fails one of the group action axioms, namely associativity. To see this, note that

$$g_1 \cdot (g_2 \cdot h) = g_1 \cdot hg_2 = hg_2g_1$$

But

$$(g_1g_2) \cdot h = hg_1g_2$$

Where $hg_1g_2 \neq hg_2g_1$ in general, violating associativity. Note that this wouldn't be a problem if G was abelian, but in this case the right multiplication "action" would just be equivalent to the left multiplication action.

There is a fix for this, though. Define our right multiplication action to be $g \cdot h := hg^{-1}$. It is easy to see that this does in fact define a group action on G by itself. G acting on itself can have interesting properties depending on the action you take. We'll now consider the orbits and stabilizers of the conjugation action, which takes $g \cdot h \mapsto ghg^{-1}$.

3.1.2 Conjugation Classes

The orbits of the action $g \cdot h \mapsto ghg^{-1}$ are called the ***Conjugacy Classes***. Given $h \in G$, we define the conjugacy class of h, denoted C_h, as below.

$$C_h := \{ghg^{-1} \mid g \in G\}$$

Similarly, the stabilizer of h is called the ***Centralizer*** of h, and is defined below:

$$Z_h = \{g \in G \mid ghg^{-1} = h\}$$

Note that $ghg^{-1} = h$ is analogous to saying $gh = hg$. Thus, the centralizer of h contains precisely the elements of G which commute with h.

3.1.3 The Class Equation

If G is finite, Lemma 2.11 gives us the following equation for any $h \in G$:

$$\#G = \#C_h \times \#Z_h$$

Note that the conjugacy classes of G partition G. Thus, we know that

$$\#G = \text{ the sum of sizes of all the conjugacy classes of } G$$

This is called the ***Class Equation*** of G.

Lemma 3.13. *The number of conjugacy classes of size* 1 *is precisely* $\#Z(G)$.

Proof. Suppose that a conjugacy class C_h has size 1. Then, the centralizer of h has size $\#G$, so $Z_h = G$. Thus, h commutes with everything, so $h \in Z(G)$. Similarly, if $h \in Z(G)$, then $Z_h = G$, so we can conclude that $\#C_h = \#Z_h/\#G = 1$. □

3.2 Examples of Conjugacy Classes

3.2.1 $G = D_n$, for n odd

Recall that

$$D_n := \{a^i, a^i b \mid 0 \leq i \leq n-1, a^n = 1, b^2 = 1, bab^{-1} = a^{-1}\}$$

We now compute the conjugacy classes of D_n, and use it to construct the class equation. First, consider the case where g is of the form a^i for some i (in other words, g is a rotation). First we consider conjugaction by a reflection:

$$(a^j b)(a^i)(a^j b)^{-1} = a^j (b a^i b^{-1}) a^{-j} = a^j a^i a^{-j} = a^{-i}$$

And now by a rotation:

$$a^j a^i (a^j)^{-1} = a^{j+i-j} = a^i$$

Thus, $C_{a^i} = \{a^i, a^{-i}\}$. If $i = 0$, $a^i = 1$, and $C_1 = \{1\}$. Otherwise, by n odd, $C_{a^i} = \{a^i, a^{-i}\}$ and has cardinality 2. These are distinct conjugacy classes for each i for $1 \leq i \leq n-1$, so there exist $(n-1)/2$ conjugacy classes of rotations in D_n (note that C_{a^i} and $C_{a^{-i}}$ are the same).

We now consider the reflections case. Let $g = ba^i$ for some i. we first conjugate by another reflection:

$$(a^j b) a^i b (a^j b)^{-1} = a^j b a^i b a^{-j} = a^j a^i a^j b = a^{i+2j} b$$

And then by a rotation:

$$a^j b a^i a^{-j} = a^j b a^{i-j} = a^j a^{j-i} b = a^{2j-i} b$$

This implies that $C_{ba^i} = \{a^{i+2j}b, a^{2j-i}b \mid j \in \mathbb{Z}\}$. Now, I claim. C_{ba^i} contains all reflections in D_n. Suppose we want $a^k b \in C_{ba^i}$. if $i \equiv k \bmod 2$, take $j = \frac{k-i}{2}$. If not, take $j = \frac{n+k-i}{2}$. Since n is odd, it is easy to check that we can reach both even and odd k powers. Thus, we know that C_{ba^i} contains every reflection. Since there are n reflections, $\#C_{ba^i} = n$. Since conjugacy classes are disjoint, there exists only one conjugacy class of reflections. We use this to compute the class equation of D_n.

$$\#D_n = 1 + (2 + \cdots + 2) + n$$

for 1 being the conjugacy class of the identity, each 2 denoting one of the $\frac{n-1}{2}$ conjugacy classes of rotations, and the n denoting the one conjugacy class of reflections. Here, we can cite Lemma 3.13 to conclude that $Z(D_n)$ is trivial. Furthermore, note that there are exactly $2 + \frac{n-1}{2}$ conjugacy classes of D_n.

3.2.2 Relating Conjugacy Classes of S_n and partitions

First, some important results.

Lemma 3.14. *Every element of S_n can be written as a product of disjoint cycles, which is unique up to the reordering of the cycles.*

Proof. It is clear that each element of S_n can be written as the product of disjoint cycles. As for uniqueness of reordering, note that two disjoint cycles commute, since one of the cycles only works on values which the other fixes, and vice versa. □

Lemma 3.15. *For $\sigma \in S_n$ and a k-cycle $(i_1\ i_2\ \ldots\ i_k)$,*

$$\sigma(i_1\ i_2\ \ldots\ i_k)\sigma^{-1} = (i_{\sigma(1)}\ i_{\sigma(2)}\ \ldots\ i_{\sigma(k)})$$

Now let n be a non negative integer. A ***Partition*** of n is an expression (defined up to reordering of terms)

$$n = a_1 + a_2 + \cdots + a_r$$

where each a_i is a positive integer. We define $p(n)$ to be the number of partitions of n, and p to be the ***Partition Function***. We compute the number of partitions for smaller n below.

n	$p(n)$	partitions
1	1	1
2	2	2, 1 + 1
3	3	3, 2 + 1, 1 + 1 + 1
4	5	4, 3 + 1, 2 + 1 + 1, 1 + 1 + 1 + 1, 2 + 2

Given $\sigma \in S_n$, we write $\sigma = \tau_1\tau_2 \ldots \tau_k$, for τ_i each disjoint cycles. We can assume all numbers appear exactly once, since for fixed points j we just append a one cycle (j) to the chain of

disjoint cycles. Since every point is hit, and our chain of disjoint cycles is defined up to reordering, we have that

$$n = \#\tau_1 + \#\tau_2 + \cdots + \#\tau_k$$

is a partition of n. Recall that from Lemma 3.15, the disjoint cycle decomposition of σ won't change under conjugation; the terms inside each cycle will change, but that will not affect the partition. Thus, we arrive at the following theorem.

Theorem 3.16. *The map from the conjugacy classes of S_n to the set of partitions of S_n which takes $\sigma = \tau_1\tau_2\ldots\tau_k \mapsto \#\tau_1 + \#\tau_2 + \cdots + \#\tau_k$ is a bijection.*

This has the immediate corollary that the number of conjugacy classes of S_n is precisely $p(n)$.

As an example, we compute the class equation of S_4.

Partitions	Conjugacy Class Representative	Size of Conjugacy Class
4	(1 2 3 4)	6
3 + 1	(1 2 3)(4)	8
2 + 2	(1 2)(3 4)	3
2 + 1 + 1	(1 2)(3)(4)	6
1 + 1 + 1 + 1	(1)(2)(3)(4)	1

Note that the sum of the sizes of each of the conjugacy classes is 24, which is precisely 4!, the order of S_4.

3.3 p Groups

A p ***Group*** is a finite group who's order is some power of p. There are a lot of interesting results about p groups which we will discuss in this class; a few are listed here.

Theorem 3.17. *If G is a nontrivial p group, then $Z(G)$ is nontrivial.*

Proof. let $\#G = p^r$ for some $r \geq 1$, and let $C_1, \ldots, C_k$ denote the conjugacy classes of G. We know that one of them must have order 1, as the conjugacy class of the identity is just itself. Without loss of generality, let C_1 be this conjugacy class. This implies that $\#C_1 = 1$. Since conjugacy classes partition the group, we know that

$$p^r = \#C_1 + \cdots + \#C_k$$

Since $\#C_1 = 1$, $\#C_2 + \ldots \#C_k = p^r - 1$. Furthermore, note that by Lagrange's Theorem, the order of each C_i divides the order of G, since C_i forms a subgroup of G for any i. Thus, each C_i must have an order that is a power of p. From this, we can conclude that there exists at least $p-1$ size 1 conjugacy classes, since if not, $\#C_2 + \cdots + \#C_k$ would not divide $p^r - 1$. Since $p \geq 2$, it follows that there exists at least two conjugacy classes of size 1. From Lemma 3.13, we know then that $\#Z(G) \geq 2$, and $\#Z(G)$ is nontrivial. □

As a corollary to this theorem, we have the following result about groups of order p^2.

Lemma 3.18. *Any group of order p^2 is abelian.*

Proof. Let G be order p^2. By the above theorem, $Z(G)$ has nontrivial order. Thus, choose $x \neq 1 \in Z(G)$. If the order of x is p^2, then G is cyclic, and thus abelian. Note that the order of any element must divide the order of the group. We've already considered the case where x is p^2, and where x is just 1. Thus, the only factor left to divide by is p, implying that if the order of x isn't p^2, it must necessarily be p. In this case, (x), or the set generated by x, is not the whole group G. Thus, we choose $y \notin (x)$. Then, note that

$$(x) \subsetneq (x, y) \subset G$$

Since (x) has order p, and (x, y) is strictly larger, it follows that (x, y) has order p^2 and $(x, y) = G$. Thus, every element can be written in terms of x's and y's. x is central, so it commutes with everything, and y commutes with itself, and x, so we can conclude that G is in fact abelian. □

Note: By the Structure Theorem of Finitely Generated Abelian Groups, this tells us that any group of order p^2 is isomorphic to either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. These correspond to the cases where x has order p^2 and where x has order p respectively.

Theorem 3.19. *Let G be a p-group, and X a G-set such that p does not divide $\#X$. Then we can conclude that G has a fixed point on X, i.e. $\exists x \in X$ such that $gx = x \ \forall g \in G$.*

Proof. Let $\mathcal{O}_1, \ldots, \mathcal{O}_k$ be the orbits of G on X. Note that we have that

$$\#X = \#\mathcal{O}_1 + \cdots + \#\mathcal{O}_k$$

And that $\#\mathcal{O}_i | \#X \ \forall i \leq k$. Furthermore, since G is a p group, and the orbits of G are subgroups, by Lagrange's Theorem, we know that $\#\mathcal{O}_i$ is some power of p, for any i. Since p does not divide the order of X, there must be some orbit $\mathcal{O}_i$ such that $\#\mathcal{O}_i = 1$. □

We now use properties of p-groups and group actions to prove an interesting results about upper triangular matrices over a finite field.

Theorem 3.20. *let $\mathbb{F}_p$ denote the finite field of order P, and $U_n \subset \mathrm{GL}_n(\mathbb{F}_p)$ be the subgroup of upper triangular matrices with 1s on the diagonal. Now suppose that $G \subset \mathrm{GL}_n(\mathbb{F}_p)$ is a p-group. Then $\exists g \in \mathrm{GL}_n(\mathbb{F}_p)$ such that $gGg^{-1} \subset U_n$.*

Proof. The full proof is tedious, so we provide a sketch. Consider $X = \mathbb{F}_p^n \backslash \{0\}$. $\#X = p^n - 1$, and G, a p-group, acts on X. Since p does not divide $p^n - 1$, there exists some fixed vector in X by Theorem 3.19. Without loss of generality, through a change of basis we can let that fixed vector be $\vec{e}_1$. By construction, that is the first column of any matrix in U_n. We now look at the $n-1 \times n-1$ size minor taken by taking any matrix in U_n and cutting the top row and leftmost column. This matrix is still invertible by construction. Because $\vec{e}_1$ is a fixed vector, we can write this $n-1 \times n-1$ matrix as Ag for any $g \in G$. Thus we have that $\{Ag \mid g \in G\} \subset \mathrm{GL}_{n-1}(\mathbb{F}_p)$ is still a p-group, and we work downwards on n. □

3.3.1 The Sylow Theorems (A Statement)

Characterizing p-subgroups leads us to 3 major theorems in Group Theory called the ***Sylow Theorems***. We first provide a definition, then state the three sylow theorems below. They will be proved in a later lecture.

For p a prime, let G be a finite group with order $p^r m$ for some r and some m such that p does not divide m. A ***p-Sylow Subgroup*** is a subgroup of G with order p^r. This is essentially a "maximal p group in G. Since p does not divide m, there cannot be any p subgroups of order greater than p^r in G.

Theorem 3.21. *(Sylow 1) $\exists$ a p-Sylow subgroup in any group G for any prime p.*

Theorem 3.22. *(Sylow 2) Any two p-Sylow subgroups are conjugate.*

Theorem 3.23. *(Sylow 3) If n_p is the number of p-Sylow subgroups, then $n_p \equiv 1$ mod p, and $n_p | m$.*

Remark: if $n_p = 1$, then there exists a unique p-Sylow subgroup, and the p-Sylow is in fact normal. In addition, U_n as defined above is a p-Sylow subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ and Theorem 3.19 can be proven using the Sylow Theorems.

Remark: While for most of these notes we will refer to theorems by their number (e.g. Theorem 3.23), we will often refer to the above theorems as "Sylow 1", "Sylow 2", and "Sylow 3" for convenience. This will be the convention for most theorems that have a well known name (i.e. Lagrange's Theorem).

Math 594: Algebra II **Winter 2019**

Lecture 4: January 22nd

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

4.1 Proofs of the Sylow Theorems

We recall the definition of a p-Sylow subgroup and the statement of the Sylow Theorems from previous lecture. Today, we prove the 3 Sylow Theorems using some interesting tricks with group actions, but first we provide a corollary:

Theorem 4.24. *(Cauchy's Theorem) If G is a group and p is a prime, and p divides the order of G, then G has an element of order p.*

Proof. Let $K \subset G$ be a p-Sylow Subgroup, which we know exists by Sylow 1. In this case, K is a non-trivial p group. Take $g \in K$ to be a non-identity element. then the order of g divides the order of K, and since K has order p^r for some r, it follows that g has order p^s for some $s \leq r$. Well, this implies that the element $g^{p^{s-1}}$ has order p, as desired. □

4.1.1 Preceding Lemmas

Recall the ***binomial coefficient*** $\binom{n}{m} := \frac{n!}{m!(n-m)!}$, for $0 \leq m \leq n$. The binomial coefficient counts how many ways there are to choose m things from n things, and $\binom{n}{m}$ is often verbally referred to as "n choose m". Observe that we have the following properties:

$$\binom{n}{n} = \binom{n}{0} = \binom{n}{1} = \binom{n}{n-1} = 1$$

$$\binom{n}{m} = \binom{n}{n-m}$$

Furthermore, we have the binomial theorem:

Theorem 4.25. *(Binomial Theorem)*

$$(x+y)^n = \sum_{m=0}^{n} \binom{n}{m} x^m y^{n-m}$$

The proof is a very straightforward induction on n. We now use this to prove the "freshman's lemma" modulo p.

Lemma 4.26.

$$(x+y)^p \equiv x^p + y^p \mod p$$

Proof. By the binomial theorem, we have that

$$(x+y)^p = \sum_{m=0}^{p} \binom{p}{m} x^m y^{p-m}$$

Thus, it is sufficient to show that p divides $\binom{p}{k}$ for $0 < k < p$. Well,

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} = \frac{p(p-1)(p-2)\dots(p-k+1)}{k!}$$

There exists a p in the numerator, and every factor of $k!$ is less than p, and thus p cannot divide $k!$, which implies that p divides $\binom{p}{k}$ as desired. Note that for $k = 0, p$, $\binom{p}{k}$ reduces to 1, leaving only $x^p + y^p$ as desired. □

Lemma 4.27. *for any $m \leq n \in \mathbb{N}$, and p a prime, we have*

$$\binom{pn}{pm} \equiv \binom{n}{m} \mod p$$

Proof. From Lemma 4.26, we have that

$$(x+y)^{pn} = ((x+y)^p)^n \equiv (x^p + y^p)^n$$

Applying the binomial theorem on both sides, we find that

$$(x+y)^{pn} \sum_{k=0}^{pn} \binom{pn}{k} x^k y^{pn-k}$$

$$\sum_{\ell=0}^{n} \binom{n}{\ell} x^{p\ell} y^{p(n-\ell)}$$

We now match these polynomials term-wise. Observe that the coefficients for $x^{pm}y^{p(n-m)}$ are precisely $\binom{pn}{pm}$ and $\binom{n}{m}$, so we have equality modulo p. □

Lemma 4.28. *For any $m, r \in \mathbb{N}$, and p a prime,*

$$\binom{p^r m}{p^r} \equiv m \mod p$$

Proof. Just apply lemma 4.27 r times.

$$\binom{p^r m}{p^r} \equiv \binom{p^{r-1} m}{p^{r-1}} \equiv \dots \equiv \binom{m}{1} = m$$

□

4.1.2 Proof of Sylow 1 (Theorem 3.21)

Proof. Let the order of G by $p^r m$ where p does not divide m. Define the set $\mathbb{S}$ as follows:

$$\mathbb{S} := \{S \subset G \mid \ S \text{ is a subset of size } p^r\}$$

Note that G acts on $\mathbb{S}$ by left multiplication:

$$g \cdot S = gS := \{gs \mid s \in S\}$$

Consider some $S \in \mathbb{S}$ with stabilizer G_S. That is, $\forall g \in G_S$, $gS = S$, implying that $G_S h \subset S$ $\forall h \in S$. This implies that S is simply a union of cosets of G_s, further implying that $\#G_S | \#S$. Since S has order p^r, it follows that G_S has order p^i for some i. We now cite the counting formula to obtain that

$$\#\mathcal{O}_S = \frac{\#G}{\#G_S} = \frac{p^r m}{p^i} = p^{r-i} m$$

We have two cases.

1) $i = r$: this is true if and only if G_S has order p^r, so G_S would be a p-Sylow subgroup of G, and we've found the subgroup we were after. Note then that $\mathcal{O}_s$ has order m, which is coprime to p.

2) $i \leq r$: In this case, the p divides the order of $\mathcal{O}_s$.

This implies that p does not divide the order of $\mathcal{O}_s$ if and only if G_s is a p-Sylow. Thus, to show there exists a p-Sylow subgroup of G, it is sufficient to find an S such that p does not divide the order of $\mathcal{O}_S$.

Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_n$ denote the orbits of G on $\mathbb{S}$. This means that

$$\#\mathbb{S} = \#\mathcal{O}_1 + \#\mathcal{O}_2 + \cdots + \#\mathcal{O}_n$$

Since $\mathbb{S}$ contains all the sets of order p^r, and G has order $p^r m$, we know that $\mathbb{S}$ has order $\binom{p^r m}{p^r}$, which by Lemma 4.28 is equivalent to m modulo p. Since p does not divide m, m is not equivalent to 0 mod p, so there exists some orbit which has nonzero order modulo p. The corresponding stabilizer to that orbit is the p-Sylow subgroup we desire. □

4.1.3 Proof of Sylow 2 (Theorem 3.22)

To prove the 2nd Sylow Theorem, we first prove a (slightly stronger) Lemma.

Lemma 4.29. *Let $K \subset G$ be a p-Sylow subgroup, and $H \subset G$ be a p subgroup. then $\exists g \in G$ such that $H \subset gKg^{-1}$.*

Proof. Recall that H acts on G/K by left multiplication. H is a p group, and G/K has size m ($p^r m/p^r = m$), so p does not divide the order of G/K by construction. Thus, by Theorem 3.19 we can conclude that there exists a fixed point. That is, H fixes some gK for some $g \in G$. This directly implies that $H \subset gKg^{-1}$ as desired. □

This lemma has several consequences.

1) If we take K and H as in Lemma 4.29, but also make H a p-Sylow subgroup, we'd have a $g \in G$ such that $H \subset gKg^{-1}$, but since $\#H = \#K = p^r$, we can conclude that $H = gKg^{-1}$. This is precisely the statement of Sylow 2.

2) Any p-subgroup of G is contained in a p-Sylow subgroup. To see this, note that gKg^{-1} is a p-Sylow subgroup, and H in lemma 4.29 was chosen to be any arbitrary p-group.

3) If $K \subset G$ is a p-Sylow subgroup, and H is any arbitrary subgroup, then $\exists g \in G$ such that $gKg^{-1} \cap H$ is a p-Sylow subgroup of H.

   Proof. Let M be a p-Sylow subgroup of H. This implies that M is a p-subgroup of G, so $M \subset gKg^{-1}$, for K a p-Sylow subgroup of G, and $g \in G$, by Lemma 4.29. Well, this implies that $M \subset gKg^{-1} \cap H$, and since M is a p-Sylow subgroup, it is a maximal p-group of H, implying that $M = gKg^{-1} \cap H$. □

4.1.4 Proof of Sylow 3 (Theorem 3.23)

Let H be a subgroup of G. We define the ***normalizer*** of H as

$$N(H) := \{g \in G \mid gHg^{-1} = H\}$$

$N(H)$ is a subgroup of G, and clearly H is a normal subgroup of $N(H)$.

let G be a p group acting on a finite set X. Denote

$$X^G := \{x \in X \mid gx = x \ \forall g \in G\}$$

Observe that $\#X \equiv \#X^G$ modulo p. We now use these new constructions to prove Sylow 3.

Let G be a group, and let X denote the set of all p-Sylow subgroups of G. Then n_p (as defined in the statement of Sylow 3) is simply $\#X$. Note that G acts on X by conjugation. For $K \in X$, we have a stabilizer $G_K = \{g \in G \mid gK = K\}$ Now fix $K \in X$. By above, we know that $n_p = \#X \equiv \#X^K$ modulo p. We claim that $X^K = \{K\}$. To see this, suppose that $H \in X^K$. Then Then $K \subset N(H)$, implying that $K, H \subset N(H)$. Since both are p-Sylows, we can conlude that by Sylow 2, they are conjugate. It follows than that $K = H$, and $X^k = \{K\}$. This means that

$$n_p = \#X \equiv \#X^k = 1$$

modulo p as desired. It follows by the counting formula that $n_p | m$.

4.2 Simple Groups

A group G is called ***simple*** if its only normal subgroups are the trivial subgroup and the group itself. As an example, $\mathbb{Z}/p\mathbb{Z}$ is a simple group.

We define the ***Alternating*** group $A_n \subset S_n$ as follows. consider the group homomorphism $\text{sgn} : S_n \to \{\pm 1\}$ which sends a permutation to its sign. the kernel of this, that is, those permutations which have sign 1, are the alternating group. It is easy to check that this forms a subgroup. Note that A_n is simple for $n \geq 5$. We now use the Sylow theorems to show some interesting facts about finite groups and their simplicity.

Theorem 4.30. *No group of order* 84 *is simple.*

Proof. Note that 84 decomposes into factors $2 \times 2 \times 3 \times 7$. taking $p = 7, m = 12$, we consider the number of 7-Sylow subgroups, n_7. $n_7 \equiv 1 \bmod 7$ (by Sylow 3) so it is one of $1, 8, 15, \ldots$. Furthermore, $n_7 | m = 12$ (again by Sylow 3), but 12 is not 1 modulo 7, so $n_7 = 1$. This implies that there is only 1 p-Sylow subgroup, and the only p-Sylow subgroup of an order 84 group is normal. since it has order 7, it follows then that our order 84 group cannot be simple, as it has a nontrivial normal subgroup. □

Math 594: Algebra II **Winter 2019**

Lecture 5: January 24th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

5.1 Direct Products

5.1.1 External Direct Products

Suppose that G, H are groups. we define the ***(external) Direct Product*** to be $G \times H$, where the elements are a cartesian product of the elements, i.e.

$$G \times H := \{(g, h) \mid g \in G, h \in H\}$$

Where the operation is applied term-wise.

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

This is a notion of direct product where a direct product is generated from two groups. We can define a different notion of direct product where one takes one group, and derive a direct product from the subgroups. We denote this as an internal direct product.

5.1.2 Internal Direct Products

Suppose K is a group, where $G, H \subset K$ are subgroups. We say that K is an ***(internal) Direct Product*** of G and H if

1) $\forall g \in G, h \in H$, $gh = hg$.
2) $G \cap H = \{1\}$
3) $K = GH$

5.1.3 Showing Equivalence

As one could guess, these notions are equivalent. This gives us the following Lemmas:

Lemma 5.31. *Given groups G and H, let K be their semi direct product. then*

$$\overline{G} := \{(g, 1) \mid g \in G\}$$

$$\overline{H} := \{(1, h) \mid h \in H\}$$

Then K is the internal direct product of $\overline{G}$ and $\overline{H}$.

Proof. It is clear that $\overline{G}, \overline{H} \subset K$. Note that

$$(g,1)(g',1) = (gg',1) \in \overline{G}$$

$$(1,h)(1,h') = (1,hh') \in \overline{H}$$

So we have closure, and inverses are not hard to see. Furthermore, elements of $\overline{G}$ and $\overline{H}$ commute.

$$(g,1)(1,h) = (g,h) = (1,h)(g,1)$$

Furthermore, $\overline{G} \cap \overline{H} = \{(1,1)\}$, as for $(1,h) \in G$, $h = 1$ necessarily. □

Lemma 5.32. *Suppose K is a group, and $G, H \subset K$ such that K is an internal direct product of G, H. Then,*

$$f : G \times H \to K$$

which takes $(g,h) \to gh$ is an isomorphism.

Proof. We first check that f is a group homomorphism.

$$f((g_1,h_1)\cdot(g_2,h_2)) = f(g_1g_2, h_1h_2) = g_1g_2h_1h_2 = g_1h_1g_2h_2 = f(g_1,h_1)f(g_2,h_2)$$

The second to last step follows from G and H commuting. We next check injectivity; take $(g,h) \in \ker(f)$. Then $gh = 1$, implying that $g = h^{-1}$. If this is true, then $g \in H$ (since it is the inverse of something in H), so $g \in G \cap H$, so $g = 1$, since G and H have trivial intersection. Similarly, we can find that $h = 1$, so $g = h = 1$, so $(g,h) = (1,1)$, and the kernel is trivial.

We conclude by showing surjectivity. Given $k \in K$, we can write it in form gh, since $K = GH$. Thus we have that $f(g,h) = k$. □

These two lemmas together show us that external and internal semi direct products are functionally equivalent. Next, we'll generalize this to internal and external semi-direct products, and show their equivalency as well.

5.2 Semi-Direct Products

External semi-direct products are a bit more abstract, so we first build from the internal case.

5.2.1 Internal Semi-Direct Products

Let G be a group, and $N, H \subset G$ are subgroups. We say that G is the ***Internal Semi-Direct Product*** of N, H if

1) $N \cap H = \{1\}$

2) $G = NH (= HN)$

3) N is normal

This is a slightly weaker condition than internal direct products, rather than mandating that every element of N commutes with every element of H, we stipulate only that N is normal. There are no specific restrictions on H. This implies that we cannot necessarily recover G from knowing just H and N. To see why, consider the following example:

Example: Let $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and let $H = \mathbb{Z}/2\mathbb{Z}$, $N = \mathbb{Z}/n\mathbb{Z}$. In this case, G is an internal semi-direct product of H, N. Now, consider the dihederal group D_n.

$$D_n = \{a, b \mid a^2 = 1, b^n = 1, aba^{-1} = b^{-1}\}$$

Take $N = (b), H = (a)$. Clearly $N \cong \mathbb{Z}/n\mathbb{Z}$, $H \cong \mathbb{Z}/2\mathbb{Z}$. However, note that even though G and D_n are internal semi-direct products of $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$, $G \ncong D_n$. To see this, we rewrite G as follows:

$$G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{a, b \mid a^2 = 1, b^n = 1, aba^{-1} = b\}$$

Where the last relation is simply a restatement of $ab = ba$. This is a different final statement than that of D_n, so it is easy to see that these are not isomorphic.

To recover G from an N and H, we need to fix how elements of H conjugate elements of N (in the case of D_n, it's different than expected, but G works how we want it to).

Given $h \in H$, define $\gamma_h \in \text{Aut}(N)$ such that $\gamma_h(g) = hgh^{-1}$, for $g \in N$. This induces a group homomorphism $\varphi : H \to \text{Aut}(N)$ such that $\varphi(h) = \gamma_h$. This specific one is the trivial action by φ, but there can be other group homomorphisms $H \to \text{Aut}(N)$ that define our "recovery" of G.

5.2.2 External Semi-Direct Products

We now define an external semi-direct product in the same vain as an external direct product, using our group homomorphism.

Let H, N be groups, and $\varphi : H \to \text{Aut}(N)$ be a group homomorphism. We define the ***External Semi-Direct Product*** as $N \rtimes_\varphi H$. The elements of $N \rtimes_\varphi H$ are the ordered pairs (n, h) for $n \in N, h \in H$, with the following operation:

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \varphi(h_1)(n_2), h_1h_2)$$

While this is a bit of a convoluted definition, we can think of it like conjugation.

$$(n_1, h_1) \cdot (n_2, h_2) \to n_1h_1n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2 = (n_1(h_1n_2h_1^{-1}))(h_1h_2)$$

Essentially, we are putting all the terms together, separating them by N terms and H terms, and putting them back into a cartesian product. The only difference is that instead of the conjugation action, it is the φ action. It is easy to verify that

$$(1, h)^{-1} = (1, h^{-1})$$

Which leads to the following result:

$$(1,h)(n,1)(1,h)^{-1} = (\varphi(h)(n),1)$$

Implying that conjugation just gives φ back.

5.2.3 Showing Equivalence

We now show that internal and external semi-direct products are functionally equivalent. The proof is very similar to the direct product case, so for brevity we only detail one direction here; the other direction is analogous.

Lemma 5.33. *Let $G = N \rtimes_\varphi H$. Set*

$$\overline{N} := \{(n,1) \mid n \in N\}$$

$$\overline{H} := \{(1,h) \mid h \in H\}$$

Then G is the internal semi-direct product of $\overline{N}, \overline{H}$.

Proof. We first check that $\overline{N}$ is a subgroup of G.

$$(n_1,1)\cdot(n_2,1) = (n_1\varphi(1)(n_2),1) = (n_1n_2,1)$$

So we have closure. Similarly, $(n,1)(n^{-1},1) = (1,1)$, so we have closure under inverses. The proof for $\overline{H}$ being a subgroup is identical.

$\overline{H} \cap \overline{N} = \{(1,1)\}$ for identical reasons to the direct product case. Furthermore, for any $(n,h) \in G$, $(n,1)(1,h) = (n,h)$, so $G = NH$. Finally, from checking that $(1,h)(n,1)(1,h)^{-1} = (\varphi(h)(n),1)$, we know that N is normal. □

Math 594: Algebra II **Winter 2019**

Lecture 6: January 24th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

6.1 Central Extensions

Let A, B, C, f, g be defined as below:

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

This is a ***Short Exact Sequence*** provided that $\mathrm{im}(f) = \ker(g)$, and f is injective, and g is surjective. A, B and C can be any algebraic structure, but in this class they will be groups.

Let G be a group. We define a ***Central Extension*** of G by A to be the short exact sequence

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 0$$

Where $i(A) \subset Z(E)$. Observe that for this to be true, A must necessarily be abelian.

6.1.1 Examples

1. If we let $E = A \times G$, we can define i to be the inclusion map and π to be the projection map.

$$1 \longrightarrow A \xrightarrow{i} A \times G \xrightarrow{\pi} G \longrightarrow 1$$

   This is called the ***trivial extension*** of G by A.

2. Consider the sequence

$$1 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{i} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/p\mathbb{Z} \longrightarrow 1$$

   Where i is the inclusion map, and π is the obvious projection map.

3. Let E be the quarternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$, and let A be the center of Q, $\{\pm 1\}$.

$$1 \longrightarrow A \xrightarrow{i} Q \xrightarrow{\pi} G \longrightarrow 1$$

4. Let $E = \mathrm{GL}_n(k)$ for some field k, and let $A = Z(E) = k^\times$. Let $G = E/A$. This gives us the short exact sequence

$$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} E/A \longrightarrow 1$$

Where i denotes inclusion and π denotes projection to the quotient. This is a short exact sequence in general, but in this case, for our choice of E and A, G is known as $\mathrm{PGL}_n(k)$

6.1.2 Isomorphism of Central Extensions

A question we can ask about Central Extensions is, given G and A, what are all the possible central extensions of A? Are they defined up some isomorphism?

Let $(E, i, \pi), (E, i', \pi')$ denote two different central extensions of G by A. An ***isomorphism of central extensions*** is a group homomorphism $E \to E'$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \updownarrow & & \downarrow & & \updownarrow & & \\ 1 & \longrightarrow & A & \xrightarrow{i'} & E' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \end{array}$$

Let $\mathcal{C}(G, A)$ denote the set of isomorphism classes of central extensions of G by A.

Remark: $\#\mathcal{C}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \geq 2$, since we can take the trivial extension, and example 2 in 6.1.1.

6.2 2nd Group Cohomology

6.2.1 2-Cocycles

For an extension (E, π, i) of G by A, we want to try to decompose E into "G parts" and "A parts". the G parts are given by π (simply project down each element of E to get their G parts) but there isn't a canonical way to choose the A parts.

Since π is surjective, it has a right inverse $s : G \to E$ such that $\pi \circ s = \mathrm{Id}$. One thing to note is that s is not necessarily a group homomorphism. However, we can analyze this failure as follows:

Consider $s(g)s(h)$ and $s(gh)$, What do they have in common? Well,

$$\pi(s(g)s(h)) = \pi(s(g))\pi(s(h)) = gh = \pi \circ s(gh)$$

They are both contained in the same fiber of π. By exactness, $\pi \circ i = 0$. We know then that $s(g)s(h)$ and $s(gh)$ vary by something from $i(A)$ (since these element are precisely those annihilated by π), so they vary by something in A. Since that variation is dependent on g, h, we write

$$s(g)s(h) = i(\psi(g,h))s(gh)$$

Now, what do we know about ψ? We use the associativity of the group to compute $s(g_1)s(g_2)s(g_3)$ two different ways:

$$(s(g_1)s(g_2))s(g_3) = i(\psi(g_1,g_2))s(g_1g_2)s(g_3) = i(\psi(g_1,g_2))i(\psi(g_1g_2,g_3))s(g_1g_2g_3)$$

$$s(g_1)(s(g_2)s(g_3)) = s(g_1)i(\psi(g_2,g_3))s(g_2g_3) = i(\psi(g_2,g_3))s(g_1)s(g_2g_3) = i(\psi(g_2,g_3))i(\psi(g_1,g_2g_3))s(g_1g_2g_3)$$

canceling the $s(g_1g_2g_3)$ terms on both sides, and utilizing the injectivity of i, we arrive at the following identity:

$$\psi(g_1,g_2) + \psi(g_1g_2,g_3) = \psi(g_2,g_3), \psi(g_1,g_2g_3)$$

This is called the ***2-cocycle identity***, and any map $\psi : G \times G \to A$ which satisfies this identity is defined to be a 2-cocycle. We define $Z^2(G,A)$ as the set of these 2-cocycle identities. Observe that $Z^2(G,A)$ is a group under addition, and is abelian.

6.2.2 2 -Coboundaries

$Z^2(G,A)$ doesn't have a canonical definition from a central extension. We defined our $Z^2(G,A)$ from our choice of ψ, which we defined from our choice of s.

What if we chose another s? Let s' denote another section. Observe that $\forall g \in G$, $\pi \circ s(g) = \pi \circ s'(g) = g$, implying that s and s' lie in the same fiber. From similar logic to above, this implies that $\exists!\, \rho$ such that $s'(g) = i(\rho(g))s(g)$. Let's identify ψ with s as above, and similarly identify ψ' with s'. Now observe that

$$\begin{aligned} i(\rho(g))i(\rho(h))i(\psi(g,h))s(gh) & \\ &= i(\rho(g))s(g)i(\rho(h)s(h) \\ &= s'(g)s'(h) \\ &= i(\psi'(g,h))s'(gh) \\ &= i(\psi'(g,h))\rho(gh)s(gh) \\ &= i(\psi'(g,h))i(\rho(gh))s(gh) \end{aligned}$$

This implies that

$$\rho(g) + \rho(h) + \psi(g,h) = \psi'(g,h) + \rho(gh) \Rightarrow (\psi - \psi')(g,h) = \rho(gh) - \rho(g) - \rho(h)$$

Thus, the difference between ψ and ψ' (and thus the difference between s, s') can be measured by how badly ρ fails to be a group homomorphism. Let

$$B^2(G,A) := \{\varphi : G \times G \to A \mid \exists \rho : G \to A \text{ such that } \psi(g,h) = \rho(gh) - \rho(g) - \rho(h)\}$$

$B^2(G,A)$ is the set of ***2-coboundaries*** of the central extensions of G by A.

6.2.3 The 2nd Group Cohomology

We check on homework that $B^2(G,A)$ is a subgroup of $Z^2(G,A)$. Because of this, it makes sense to take a quotient. We define $H^2(G,A) := Z^2(G,A)/B^2(G,A)$ as the ***2nd Group Cohomology*** of G with coefficients in A. Because we mod out by variance in choice of s, this gives us a canonical representation for each extension.

6.3 Relationship between Central Extensions and Group Cohomology

We now prove the claim above; in more sophisticated terms, we prove that $\mathcal{C}(G,A) \cong H^2(G,A)$ as sets. Be aware that $\mathcal{C}(G,A)$ is NOT a group, but $H^2(G,A)$ is, implying that they aren't isomorphic as groups. That being said, this isomorphism can give a group like structure to $\mathcal{C}(G,A)$, by relating two elements of $\mathcal{C}(G,A)$ by their image in $H^2(G,A)$.

Our work above has already showed us that for any section $s \in \mathcal{C}(G,A)$, there exists a ψ in $H^2(G,A)$. That is, we have a mapping

$$\mathcal{C}(G,A) \longrightarrow H^2(G,A)$$

We just need to check if this works in the reverse direction. That is, for any $\psi \in H^2(G,A)$, there exists some section s in $\mathcal{C}(G,A)$ which is identified with that ψ.

We first choose $\psi \in H^2(G,A)$, and normalize ψ such that $\psi(1,h) = \psi(h,1) = 0 \ \forall h \in G$.

Take $E = G \times A$ as a set, and define an operation $(g,a)(h,b) = (gh, \psi(g,h) + a + b)$. Note here that the identity element, from our construction of ψ, is $e = (1,0)$.

$$(1,0)(h,b) = (h, \psi(1,h) + b) = (h,b)$$

$$(h,b)(1,0) = (h, \psi(h,1) + b) = (h,b)$$

Finally, we check associativity.

$$((g_1,a_1)(g_2,a_2))(g_3,a_3) = (g_1g_2, \psi(g_1,g_2)+a_1+a_2)(g_3,a_3) = (g_1g_2g_3, \psi(g_1,g_2)+a_1+a_2+\psi(g_1g_2,g_3)+a_3)$$

$$(g_1,a_1)((g_2,a_2)(g_3,a_3)) = (g_1,a_1)(g_2g_3, \psi(g_2,g_3)+a_2+a_3) = (g_1g_2g_3, \psi(g_1,g_2g_3)+a_1+\psi(g_2,g_3)+a_2+a_3)$$

The first coordinates are both equal, and the second coordinates will be equal if and only if ψ is a 2-cycle. To see this, just cancel out the $a_1 + a_2 + a_3$ term; we arrive at the 2-cocycle identity.

Since $\psi \in H^2(G,A)$, it follows that $E = G \times A$ is a group under this operation. This gives us the short exact sequence

$$1 \longrightarrow A \xrightarrow{i} G \times A \xrightarrow{\pi} G \longrightarrow 1$$

Note that this E is induced by ψ. Suppose we have a ψ' such that it induces an E' similarly. Recall that $\psi - \psi' = 0$, since $\psi, \psi' \in H^2(G, A)$ and $\psi - \psi' \in B^2(G, A)$. Thus, there exists a single induced E.

From here, we can conclude that there exist maps

$$\mathcal{C}(G, A) \rightleftarrows H^2(G, A)$$

We now just need to show they are inverses of each other. Choose $\psi \in H^2(G, A)$ normalized as before, and take $E = G \times A$ as before with the same operations. To go from E back to H^2, pick a section $s : G \to E$. Choose $s(g) = (g, 0)$. Under the operation on E,

$$s(g)s(h) = (g, 0)(h, 0) = (gh, \psi(g, h))$$
$$s(gh) = (gh, 0)$$

But in general,

$$s(g)s(h) = i(\psi(g, h))s(gh) = (1, \psi(g, h))(gh, 0) = (gh, \psi(gh, 1) + \psi(g, h))$$

From here we can conclude the following theorem:

Theorem 6.34. *there exists a (canonical) bijection $\mathcal{C}(G, A) \cong H^2(G, A)$.*

6.3.1 Application of Group Cohomology

We use the above results to prove the following Theorem:

Theorem 6.35. *Suppose G and A are finite. if $(\#G, \#A) = 1$, then $H^2(G, A) = 0$.*

As a corollary, note that if $(\#G, \#A) = 1$, then any central extension of G by A is trivial, and is of the form $G \times A$ or isomorphic to it. Now, onto proving the theorem.

Proof. Choose a 2-cycle $\psi \in Z^2(G, A)$. Define $\rho(g) = \frac{1}{\#G} \sum_{h \in G} \psi(g, h)$ We can divide by the order of G because the orders of G and A are finite and coprime. Observe that

$$\frac{1}{\#G} \sum_{g_3 \in G} (\psi(g_1, g_2) + \psi(g_1 g_2, g_3)) = \frac{1}{\#G} \sum_{g_3 \in G} \psi(g_1, g_2) + \frac{1}{\#G} \sum_{g_3 \in G} \psi(g_1 g_2, g_3) = \psi(g_1, g_2) + \rho(g_1 g_2)$$

And by the 2-cocycle identity,

$$\frac{1}{\#G} \sum_{g_3 \in G} (\psi(g_1, g_2) + \psi(g_1 g_2, g_3)) = \frac{1}{\#G} \sum_{g_3 \in G} \psi(g_2, g_3) + \sum_{g_3 \in G} \psi(g_1, g_2 g_3) = \rho(g_2) + \rho(g_1)$$

This implies that

$$\psi(g_1, g_2) + \rho(g_1 g_2) = \rho(g_2) + \rho(g_1) \Rightarrow \psi(g_1, g_2) = -(\rho(g_1 g_2) - \rho(g_2) - \rho(g_1))$$

So $\psi(g_1, g_2) \in B^2(G, A)$, implying that $\psi = 0$ in $H^2(G, A)$. Thus, we have trivial cohomology. □

Math 594: Algebra II **Winter 2019**

Lecture 7: February 5th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

7.1 The Schur-Zassenhaus Theorem

Recall the following definitions from last class:

- $C^2(G, A)$ is the set of all functions $\psi : G \times G \to A$. It is an abelian group under addition, and the elements are called ***2-cochains***.
- $Z^2(G, A)$ is the set of those 2-cochains ψ that satisfy the 2-cocycle identity:

$$\psi(g_1, g_2) + \psi(g_1 g_2, g_3) = \psi(g_2, g_3), \psi(g_1, g_2 g_3)$$

  $\forall g_1, g_2, g_3 \in G$. It is a subgroup of $C^2(G, A)$, and its elements are called ***2-cocycles***.
- $B^2(G, A)$ is the set of those 2-cochains ψ for which there exists $\rho : G \to A$ (i.e. a 1-cochain) such that $\psi(g, h) = \rho(gh) - \rho(g) - \rho(h)$ $\forall g, h \in G$. It is a subgroup of $Z^2(G, A)$, and its elements are called ***2-coboundaries***.
- $\mathrm{H}^2(G, A)$ is the quotient group $Z^2(G, A)/B^2(G, A)$. It is called the ***second group cohomology*** of G with coefficients in A.
- $\mathcal{C}(G, A)$ is the set of isomorphism classes of central extensions of G by A.

Also recall Theorem 6.35 above. 6.35 immediately implies that if G and A have coprime order, then any extension splits (i.e. $E \cong G \times A$) Using results from Homework 3, problem 7, we know a similar results hold for where A is abelian but not necessarily central. This gives us the following theorem:

Theorem 7.36. *For any exact sequence*

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 0$$

where A and G are finite and have coprime order, and A is abelian, $E \cong G \ltimes A$.

We use this to help prove the Schur-Zassenhaus Theorem:

Theorem 7.37. *(The Schur-Zassenhaus Theorem) Let G be a finite group of order ab, where $(a, b) = 1$. Suppose that we know that $H \subset G$ is normal and has order a. Then $\exists$ a complementary subgroup $K \subset G$ (complementary implying that $H \cap K = \{1\}$, and $G = HK$) and $G = H \rtimes K$.*

For the rest of the section, fix a, b, G, H. We want to use these to construct a K. We first prove a preceeding lemma then move on to the main proof.

Lemma 7.38. *Any subgroup of G order b is a complement of H.*

Proof. Let $K \subset G$ have order b. We first check that $H \cap K$ is trivial. Well, note that $H \cap K$ is a subgroup of both H and K. Thus, its order divides both the order of H and the order of K. Since H and K have coprime order, $H \cap K$ must have order 1, and thus must be trivial.

We now check that $G = HK$. HK is a subgroup of G, and contains H and K as subgroups. Thus, a, b both divide the order of HK. Well, the order of HK divides the order of G, which is ab, and since a, b are coprime, it follows that HK has order ab, so $HK = G$. □

This lemma implies that we only need to show that there exists a subgroup of K order b such that $G = H \rtimes K$.

7.1.1 Step 1: H is a Minimal Normal Subgroup

We'll proceed by contradiction. Suppose there exists a subgroup $H \subset G$ satisfying the hypothesis of the theorem, but not the result. We show that this H is a minimal normal subgroup (i.e. there is no proper subgroup of H that is normal in G).

Proof. We again proceed by contradiction. Suppose H' is a proper nontrivial subgroup of H that is normal in G. Consider the quotient group G/H'. H/H' is a normal subgroup in G/H', and $\#H/H' = a/a'$, for $a' = \#H$, and $\#G/H' = (a/a')b$. Note that (a/a') and b are relatively prime. By the minimality assumption, the theorem holds for G/H', so $\exists$ a subgroup $\overline{K}$ of G/H' of order b. Let $K \subset G$ be the inverse image of $\overline{K}$. K has order $a'b$, and has a normal subgroup H' of order a', so there exists a complement of H' in K. This is a subgroup of K or order b, so we get a subgroup of G of order b, a contradiction. □

7.1.2 Step 2: H is a p-Group

Fix p a prime such that $p|\#H$. We wish to show that our H is in fact a p-group.

Proof. From Sylow 1, we know that there exists a p-Sylow subgroup of H, denoted P. We claim that $G = HN_G(P)$, for $N_G(P)$ the normalizer of P in G. To see this, fix some $g \in G$. Consider gPg^{-1}. Since H is normal, it follows that gPg^{-1} is also a p-Sylow subgroup of H. By Sylow 2, we know that gPg^{-1} and P are conjugate in H. in other words, $\exists h \in H$ such that $gPg^{-1} = hPh^{-1}$. Putting the h and g terms on one side, we arrive to the conclusion that $h^{-1}g \in N_G(P)$, implying that $g \in HN_G(P)$, and $G \subset HN_G(P)$. The reverse inclusion is clear, so $G = HN_G(P)$.

This claim implies that

$$G/H = HN_G(P)/H \cong N_G(P)/(N_G(P) \cap H)$$

Since G/H has order b, it follows that $N_G(P) \cap H$ has order b. Note that $N_G(P) \cap H$ is a normal subgroup of $N_G(P)$, with order dividing a, since the quotient has order b. By minimality, we have two cases.

First, if $N_G(P)$ is a proper subgroup of G, then the theorem holds for $N_G(P)$, and $H \cap N_G(P)$ has a complement. The order of this is b, so G has a subgroup of order b, a contradiction.

Second, if $G = N_G(P)$, then P is normal in G, and by step 1, we know that $H = P$, so H is thus a p-group in G. □

7.1.3 Step 3: $H \cong \mathbb{Z}/p^n\mathbb{Z}$ For Some n

We first start with a definition. For G a group, H is a ***Characteristic Subgroup*** provided that $\forall \varphi \in \mathrm{Aut}(G)$, $\varphi(H) = H$. In other words, characteristic subgroups are fixed under any automorphism. It is easy to verify that $Z(H)$ is a characteristic subgroup of H. Furthermore, if H is normal in G, and K is a characteristic subgroup of H, then K is normal in G as well.

Proof. We now proceed with the claim; since we know that H is a p-group, it is enough to show that H is abelian. Well, by the above and the minimality assumption, we can conclude that $Z(H) = H$, so H is abelian.

(note to the reader: I am unsure why this works, if you know please send me an email.) □

7.1.4 Step 4: A Final Contradiction

From Theorem 7.36, we know that since H is abelian and has order a (which is coprime to b), it has a complement K of order b such that $G \cong H \rtimes K$. This is a contradiction, as it was assumed that H was a counterexample.

7.2 An Application of Schur-Zassenhaus

Suppose G is a finite group, and p is a prime which divides the order of G. Does p divide the order of $\mathrm{Aut}(G)$ in general? The answer is no. To see why, note that $p | \mathbb{Z}/p\mathbb{Z}$, but $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, it follows that its multiplicative group has order $p-1$, which is not divisible by p. This by itself isn't remarkable, but what is remarkable is that $\mathbb{Z}/p\mathbb{Z}$ is (essentially) the only counter example to the claim made above. In other words, using the Schur-Zassenhaus theorem, we can arrive at the following theorem:

Theorem 7.39. *Let G be a finite group, and p a prime. Then the following are equivalent:*

(a) p divides the order of G, but does not divide the order of $\mathrm{Aut}(G)$.

(b) $G \cong \mathbb{Z}/p\mathbb{Z} \times H$ for some group H, where p does not divide the order of H nor the order of $\mathrm{Aut}(H)$.

This Theorem has the interesting corollary that if p^2 divides the order of G, then p divides the order of $\mathrm{Aut}(G)$.

We first prove the following lemmas:

Lemma 7.40. *Let H_1, H_2 denote finite groups with orders a and b respectively, such that $(a, b) = 1$. Then,*

$$\mathrm{Aut}(H_1 \times H_2) \cong \mathrm{Aut}(H_1) \times \mathrm{Aut}(H_2)$$

Proof. Define $\varphi : \mathrm{Aut}(H_1) \times \mathrm{Aut}(H_2) \to \mathrm{Aut}(H_1 \times H_2)$ such that $\varphi(\sigma, \tau) = ((x, y) \mapsto (\sigma(x), \tau(y)))$. It is easy to see that this map is injective in general. to show that this map is surjective, we need to utilize the hypothesis. Choose $\rho \in \mathrm{Aut}(H_1 \times H_2)$.

First, I claim that $\rho(H_1) = H_1$. To see this, observe that since H_1, H_2 have coprime order, the order of $(x, y) \in H_1 \times H_2$ is precisely the order of x times the order of y. However, $(x, y) \in H_1$ (inclusion defined in the semi direct product sense) has order that divides a, and since automorphisms preserve order, it follows that $\rho(H_1) = H_1$. Similarly, $\rho(H_2) = H_2$. defining σ as ρ restricted to H_1 and τ as ρ restricted to H_2, we have autmorphisms from $H_1 \to H_1$ and $H_2 \to H_2$ respectively. It follows then that $\varphi(\sigma, \tau) = \rho$, and we can conclude. □

Lemma 7.41. *if P is an abelian p-group such that p does not divide the order of* $\mathrm{Aut}(P)$*, then $P \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. By the structure theorem for abelian groups, since P is a finite group of order p^r for some r, it follows that

$$P \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{n_r}\mathbb{Z}$$

Observe that

$$\mathrm{Aut}(\mathbb{Z}/p^{n_1}\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/p^{n_2}\mathbb{Z}) \times \ldots \times \mathrm{Aut}(\mathbb{Z}/p^{n_r}\mathbb{Z}) \subset \mathrm{Aut}(P)$$

This implies that $n_i = 1\ \forall i$, or else p divides $\mathrm{Aut}(P)$. This implies that $P \cong (\mathbb{Z}/p\mathbb{Z})^r$. However, $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^r) = \mathrm{GL}_r(\mathbb{F}_p)$, which p divides for $r \neq 1$. It follows then that $P \cong \mathbb{Z}/p\mathbb{Z}$. □

We now go ahead with proving Theorem 7.39.

Proof. First we show that $(b) \Rightarrow (a)$. Suppose that $G = \mathbb{Z}/p\mathbb{Z} \times H$ for H defined as above. Clearly, p divides the order of G. By our lemma, it follows that $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \times \mathrm{Aut}(H)$, and since p does not divide the order of $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$, it follows that p does not divide the order of $\mathrm{Aut}(G)$.

Next we show that $(a) \Rightarrow (b)$. Fix G such that p divides the order of G, but does not divide the order of $\mathrm{Aut}(G)$. Take P to be a p-Sylow of G. Recall that we have the automorphism $\varphi : G \to Aut(G)$ which takes $g \mapsto \gamma_g$, for γ_g the map which conjugates the input by g. In Homework 1, we've shown that $\ker(\varphi) = Z(G)$. I claim that $P \subset \ker(\varphi)$. To see this,

observe that since P is a p-group, then $\varphi(P)$ is also a p-group, and is a p-subgroup of $\mathrm{im}(\varphi)$, which itself is a normal subgroup of $\mathrm{Aut}(G)$. Since p divides the order of $\varphi(P)$, the order of $\varphi(P)$ divides the order of $\mathrm{im}(\varphi)$, which in turn divides the order of $\mathrm{Aut}(G)$, it follows that the order of $\varphi(P) = 1$, so $P \subset \ker(\varphi) = Z(G)$. This implies that P is abelian.

By Schur-Zassenhaus, P has a complement H, where p does not divide the order of H, and $G \cong P \times H$. By our lemma, $\mathrm{Aut}(G) \cong \mathrm{Aut}(P) \times \mathrm{Aut}(H)$, implying that p does not divide the order of $\mathrm{Aut}(P)$ and $\mathrm{Aut}(H)$. since p does not divide the order of $\mathrm{Aut}(P)$, and P is an abelian p-group, it follows form Lemma 7.41 that $P \cong \mathbb{Z}/p\mathbb{Z}$. Thus we can conclude that $G \cong \mathbb{Z}/p\mathbb{Z} \times H$ for some group H, where p does not divide the order of H nor the order of $\mathrm{Aut}(H)$. $\square$

Math 594: Algebra II **Winter 2019**

Lecture 8: February 7th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

8.1 The Jordan Hölder Theorem

We define a ***composition series*** for G to be a finite series of normal subgroups $\{G_i\}$ such that

$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

Such that G_i/G_{i-1} is simple for all i.

As a remark, note that $G = \mathbb{Z}$ does not have a composition series. To see why, let $H_n = \mathbb{Z}$. For H_n/H_{n-1} to be simple, $H_{n-1} = \mathbb{Z}/p\mathbb{Z}$ for some prime p. Every H_i for $i < n-1$ must also take this form, implying that this will never terminate at 0.

The proposition fails in part because G is an infinite group. There are infinite groups with composition series, but finite groups always have one.

Lemma 8.42. *Every finite group G has a composition series.*

Proof. If G is a simple group, we have $0 = H_0 \subset H_1 = G$ as a valid composition series. If G is not simple, choose $N \subset G$ as a maximum proper normal subgroup. Since G is not simple, $N \neq G$. Thus, N has smaller order than G. By inducting on the order of G, N has a composition series $1 = N_0 \subset \ldots \subset N_r = N$. By the correspondence theorem, G/N is simple. Thus,

$$1 = N_0 \subset \ldots \subset N_{r-1} \subset N \subset G$$

is a composition series. □

Note that composition series are not necessarily unique. As an example of a (finite) with two different composition series, take $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Observe that

$$1 = H_0 \subset \mathbb{Z}/q\mathbb{Z} \subset H_2 = G$$

$$1 = H_0' \subset \mathbb{Z}/p\mathbb{Z} \subset H_2' = G$$

Observe that $H_1/H_0 \cong \mathbb{Z}/q\mathbb{Z}, H_2/H_1 \cong \mathbb{Z}/p\mathbb{Z}$, both simple groups. Similarly $H_1'/H_0' \cong \mathbb{Z}/p\mathbb{Z}, H_2'/H_1' \cong \mathbb{Z}/q\mathbb{Z}$ are also both simple groups. While these are two different composition series, you may notice that the sets of the corresponding quotients of H_i, H_i' are the same, up to reordering and isomorphism. This is true in general for any finite group G, and can be summarized by the following theorem.

Theorem 8.43. *(The Jordan Hölder Theorem) Let G be a finite group. Let*

$$1 = H_0 \subset \ldots \subset H_n = G$$

$$1 = H_0' \subset \ldots \subset H_m' = G$$

Be two composition series. Then $n = m$, and $(H_1/H_0, \ldots, H_n/H_{n-1})$ is just a permutation (up to isomorphism) of $(H_1'/H_0', \ldots, H_n'/H_{n-1}')$

Proof. Done on homework 4, problem 3. If you would like the solution, please email me at vigneshj@umich.edu. □

From Jordan Hölder, we know that any composition series of G will have the same length. Thus we define the ***length*** of G to be the length of its composition series. Similarly, the list of quotients of a composition series are unique up to isomorphism, so we define the components H_i/H_{i-1} to be the ***Jordan Hölder constituents*** of G. If a group has abelian simple groups as Jordan Hölder constituents, it is said to be ***solvable***. For example, every p-group is solvable, as each constituent must be of the form $\mathbb{Z}/p\mathbb{Z}$.

8.2 An Introduction to Representation Theory

We now move into the second part of the course, which discusses Representation Theory. Much of the next three lectures will be introducing the study of finite dimensional representation theory of finite groups. We will build some basic tools of representation theory, then introduce character theory, which greatly simplifies computation in our restricted case. After this, we will survey many examples and explicitly compute representations of common groups (S_4, D_n, etc.) to gain further understanding. Finally, we'll touch on some more advanced topics in Representation Theory, like induced representations, before moving on to our third topic, Field Theory.

The purpose of representation theory is to take problems in abstract algebra, and phrase them as problems in linear algebra, a field which is much better known and much easier to work in. We do this by associating a vector space V over some field k with a group G. We derive this association by identifying an action on V by G.

A ***linear action*** of G on V is a group action $G \times V \to V$ such that $\forall g \in G$, the map $v \mapsto g \cdot v$ is a linear map. (i.e. $g \cdot (\alpha v + \beta w) = \alpha(g \cdot v) + \beta(g \cdot w)$).

Giving a linear action on V is equivalent to giving a group homomorphism $\rho : G \to \mathrm{GL}(V)$ for $\mathrm{GL}(V)$ the group of invertible linear transformations from V to itself. We can rewrite $g \cdot v$ as $\rho(g)(v)$. A ***Representation*** of G is a vector space V equipped with a linear action.

After defining a new object in algebra, the first thing one thinks to do is identify them, so we'll do that here. For representation V, W, we define a ***map of representations*** $f : V \to W$ as a linear map that is ***G-equivariant***, implying that $f(g \cdot v) = g \cdot f(v)\ \forall g \in G, v \in V$.

An ***isomorphism of representations*** is just a map of representations that is bijective. This gives us a good way of determining whether two representations are "the same". If two representations V and W are "the same" they must be isomorphic as vector spaces and that isomorphism needs to be G-equivariant.

Now that we have a notion of equivalence, **our main goal is to classify the representations of G up to isomorphism.**

Let's consider an example of a representation. $\mathbb{C}^3$ admits a representation of S_3, where the action just permutes the elements of a given vector:

$$\sigma \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} a_{\sigma(1)} \\ a_{\sigma(2)} \\ a_{\sigma(3)} \end{bmatrix}$$

The action can be defined in terms of where it sends its basis. For e_1, e_2, e_3 the standard basis of $\mathbb{C}^3$, $\sigma(e_i) = e_{\sigma(i)}$. This generalizes to $S_n, \mathbb{C}^n$ clearly. We can further generalize this form of representation to any group G and set X.

Suppose G acts on a set X. let V be the vector space consisting of all formal sums

$$\sum_{x \in X} a_x[x]$$

For $a_x \in k$ (where k is a field, but in this case we just use $\mathbb{C}$) such that all but finitely many a_x are zero. V has the basis $\{[x]\}_{x \in X}$. G acts linearly on V by

$$g \cdot \sum_{x \in X} a_x[x] = \sum_{x \in X} a_x[g \cdot x]$$

Observe that if $G = S_3, X = \{1, 2, 3\}$, then this is equivalent to the above representation. We denote $V = \mathbb{C}[X]$, where $\dim(V) = \#X$. Representations of this form are called ***permutation representations***.

Observe that G always acts on itself by left multiplication. Thus, in the case were $X = G$, with the G acting on itself by left multiplication, we call $V = \mathbb{C}[G]$ the ***regular representation*** of G. Note that $\dim(V) = \#G$. The regular representation will come back to be very useful later in the class, so take note of this construction.

Note that the regular representation is one we can generate from just G itself, and no other identified vector space or set. Similarly, if we take $V = k$ for some field k, and let G act on it by identity, this is known as the ***trivial representation*** of G.

Note that if we have two representations V, W of G, we can naturally identify $V \oplus W$ as a representation of G called the ***direct sum representation***. To see this, let $\{v_i\}_{i \leq n}$ denote a basis for V and $\{w_j\}_{j \leq m}$ denote a basis for W. Let the representation of G on V correspond to the map $\rho : G \to \mathrm{GL}_n(k)$, and similarly let the representation of G on W correspond to the map $\sigma : G \to \mathrm{GL}_m(k)$. Observe that $\{v_i\}_{i \leq n} \cup \{w_j\}_{j \leq m}$ is a basis for $V \oplus W$. We define a group homomorphism $\tau : G \to \mathrm{GL}_{m+n}(k)$ such that

$$\tau(g) = \begin{bmatrix} \rho(g) & 0 \\ 0 & \sigma(g) \end{bmatrix}$$

It is clear that this is a representation of G on $V \oplus W$.

We consider another example of a representation. Let D_n be the dihederal group, with reflection a and rotation b. Let $\rho : D_n \to \mathrm{GL}_2(\mathbb{C})$ be the unique homomorphism satisfying

$$\rho(a) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \rho(b) = \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix}$$

Note that one can take G to be $\mathrm{GL}(V)$ itself. This is called the ***standard representation*** of $\mathrm{GL}(V)$.

If we have a representation, it may be useful to know about any subspaces that are also representations. More concretely, if V is a representation of G, a ***subrepresentation*** of G is a subspace $W \subset V$ such that W is ***G-stable*** (i.e. $\forall w \in W, g \in G,\ g \cdot w \in W$). A representation where the only subrepresentations are 0 and the whole space are called ***irreducible***.

Let $f : V \to W$ be a map of G-representations. One can easily verify that

(1) $\ker(f)$ is a subrepresentation of V.

(2) $\mathrm{im}(f)$ is a subrepresentation of W.

(3) $\mathrm{coker}(f)$ is a subrepresentation of W.

Similarly, if V is a representation and U is a subrepresentation, then V/U is a subrepresentation, with the action $g \cdot (v + U) = g \cdot v + U$. One can even take a short exact sequence of representations

$$0 \longrightarrow V_1 \xrightarrow{\ i\ } V_2 \xrightarrow{\ \pi\ } V_3 \longrightarrow 0$$

That satisfies all the usual requirements of a short exact sequence. The sequence would ***split*** if $\exists$ a right inverse of π that is a G-map. That is, $V_2 \cong V_1 \oplus V_3$. In this case, V_3 would be a ***complementary subrepresentation*** of V_1 in V_2. As an example of complementary subrepresentations, consider the representation of S_2 on $\mathbb{C}^2$ given by

$$U = \{[\begin{smallmatrix} a \\ a \end{smallmatrix}] \mid a \in \mathbb{C}\} \subset \mathbb{C}^2$$

This has the complementary representation

$$W = \{[\begin{smallmatrix} a \\ -a \end{smallmatrix}] \mid a \in \mathbb{C}\} \subset \mathbb{C}^2$$

However, this doesn't work over any field. Observe that if we replaced $\mathbb{C}^2$ with $\mathbb{F}_2^2$, then $-1 = 1$, so $U = W$!

Math 594: Algebra II **Winter 2019**

Lecture 9: February 12th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

9.1 The Jordan Hölder Theorem (again)

Let V be a representation of G. A ***composition series*** of V is a series of subrepresentations $0 = V_0 \subset V_1 \subset \ldots \subset V_n = V$ such that V_i/V_{i-1} is irreducible for all i.

Just like with groups, not every representation has a composition series. Similarly to groups, though, every finite dimensional representation does.

Lemma 9.44. *If V is finite dimensional, it has a composition series.*

Proof. If $V = 0$ or V is irreducible, then we can immediately conclude, so we assume that this is not the case. Then, we choose V_1 to be the a nonzero subrepresentation with minimal dimension. V_1 is irreducible, since if there was a subrepresentation in V_1, it must have lower dimension, and thus must be 0. Now note that $\dim(V/V_1) < \dim(V)$. By inducting on the dimension of V, we can assume that V/V_1 has a composition series

$$0 = W_0 \subset \ldots \subset W_n = V/V_1$$

Taking each V_i to be the inverse image of each W_i will yield a composition series $0 = V_1 \subset \ldots \subset V_n = V$ of V. To see why, note that

$$V_i/V_{i-1} \cong W_{i-1}/W_{i-2}$$

□

Composition series in this context are very similar to the case of groups. It follows that there is an analogous Jordan Hölder Theorem for representations.

Theorem 9.45. *(Jordan Hölder Theorem) For any two composition series of a finite dimensional representation V, the irreducible subquotients are equivalent up to permutation and isomorphism.*

Proof. See Homework 5, Problem 1. If you would like a solution to this, please email me at vigneshj@umich.edu. □

Just as before, since these irreducible subquotients are uniquely defined, we denote them the ***Jordan Hölder constituents*** of V.

9.2 Complete Reducibility of Representations

Let V be a representation of G. We say V is ***completely reducible*** if it is isomorphic to the direct sum of irreducible representations.

Lemma 9.46. *If V is completely reducible, it is isomorphic to the direct sum of its Jordan Hölder constituents.*

Proof. Let $V = \bigoplus_{i=1}^{j} W_i$. Since direct sum is invariant under permutation, it is sufficient to show that the W_i representations can be used to construct a composition series. Well, take

$$V_0 = 0$$

$$V_1 = W_1$$

$$V_2 = W_1 \oplus W_2$$

$$V_3 = W_1 \oplus W_2 \oplus W_3$$

And so on. This gives us a composition series, as $V_k/V_{k-1} \cong W_k$, which is irreducible. It then follows that V is isomorphic to these constituents, and we conclude. □

Lemma 9.47. *Let V be a finite dimensional representation of G. Then, the following statements are equivalent:*

(1) V is completely reducible.

(2) Every subrepresentation U of V has a complementary subrepresentation.

Proof. First we show that (2) ⇒ (1). If V is irreducible, then it is completely reducible. Thus, we suppose that V is not irreducible and choose U a nonzero proper subgroup. By (2), U has a complementary subgroup U', so $V = U \oplus U'$. By inducting on the dimension of V, it follows that U, U' are both completely reducible. Thus, V is completely reducible, and we can conclude the first implication.

We next check that (1) ⇒ (2). Let $V = \bigoplus_{i=1}^{n} W_i$, for each W_i irreducible. Let U be a subresentation of V. Let $I \subset \{1, 2, \ldots, n\}$ be a maximal set such that $\bigoplus_{i \in I} W_i \cap U = 0$. I claim that $\bigoplus_{i \in I} W_i$ is a complementary subrepresentation of U'. We already have a trivial intersection with U, so it suffices to show that $W_j \in U + U'$ $\forall 1 \leq j \leq n$. If $j \in I$, Then $W_i \subset U'$, so we can conclude. if not, by the maximality of I, $U' \oplus W_j \cap U \neq 0$. Suppose $\exists$ some nonzero $x + y \in (U' \oplus W_j) \cap U$ with $x \in U', y \in W_j$, and $x + y \in U$. Note that if $y = 0$, then $x \in U, U'$, and $x = 0$, so $x + y = 0$, a contradiction. Thus, assume y nonzero. This implies that $0 \neq y \in W_j \cap (U + U')$. Well, $W_j \cap (U + U')$ is a nonzero suprepresentation of W_j, so since W_j is irreducible, $W_j \cap (U + U') = W_j$. It follows then that $W_j \subset (U + U')$, as desired. □

9.2.1 Maschke's Theorem

One may wonder what kind of Representations are completely reducible. If a representation is completely reducible, then it can be viewed at the level of irreducible representations. We'll find later that this is very useful. It turns out that when the group is finite and has a representation over a field where $|G| \neq 0$, then the representation is always completely reducible. This result is called Maschke's Theorem, and is stated and proven more explicitly below:

Theorem 9.48. *(Maschke's Theorem) Let G be a nonzero finite group, and k a field where $|G| \neq 0$ (always true in characteristic zero. If k has characteristic p, then p cannot divide $|G|$). Then, every finite dimensional representation of G over k is completely reducible.*

Proof. Let V be a representation of G over k, and let U be a subrepresentation of V. Take a short exact sequence of representations

$$0 \longrightarrow U \xrightarrow{i} V \xrightarrow{\pi} V/U \longrightarrow 0$$

Choose an arbitrary map $s_0 : V/U \to V$ such that $\pi \circ s = \mathrm{Id}$. Note that this map is in all likelyhood not a G-equivariant map. To remedy this, we average over the group and try to derive one. Define $s : V/U \to V$ such that

$$s(x) = \frac{1}{|G|} \sum_{g \in G} g s_0(g^{-1}x)$$

I claim that $\pi \circ s$ is the identity, and s is a G equivariant map. The first claim is immediate, as

$$\pi \circ s(x) = \pi\left(\frac{1}{|G|} \sum_{g \in G} g s_0(g^{-1}x)\right) = \frac{1}{|G|} \sum_{g \in G} g[\pi \circ s_0](g^{-1}x) = \frac{1}{|G|} \sum_{g \in G} g g^{-1} x = \frac{1}{|G|} \sum_{g \in G} x = x$$

Next, we check that s is G equivariant. That is, for any $g \in G$, $s(hx) = hs(x)$. We do this by doing a change of variables in the summation.

$$s(hx) = \frac{1}{|G|} \sum_{g \in G} g s_0(g^{-1}hx) = \frac{1}{|G|} \sum_{hg' = g, g' \in G} hg' s_0((hg')^{-1}hx) = \frac{1}{|G|} h \sum_{g' \in G} g' s_0((g')^{-1}x) = hs(x)$$

Thus, $\exists s : V/U \to V$ such that $\pi \circ s = \mathrm{Id}$, and such that s is G-equivariant. This implies that the sequence splits, and $V \cong V/U \oplus U$. Now consider $U' = \mathrm{im}(s)$. We claim that U' is a complementary subrepresentation of U. Let $x \in V$. Note that $x = s(\pi(x)) + x - s(\pi(x))$, where $s(\pi(x)) \in U'$, and $x - s(\pi(x)) \in \ker(\pi)$, since $\pi(x - s(\pi(x))) = \pi(x) - \pi(x) = 0$. This implies that any $x \in V$ can be represented by the sum of elements in U, U', so it follows that $V = U + U'$.

To conclude, we need to show that $U \cap U' = 0$. choose $x \in U \cap U'$. $\pi(x) = 0$ by exactness, and $x = s(y)$, for some y.

$$0 = \pi(x) = \pi(s(y)) = y \Rightarrow s(0) = x \Rightarrow x = 0$$

Thus, any subrepresentation U has a complementary subrepresentation U', so we can conclude by Lemma 9.47. □

9.3 Schur's Lemma

Now that we've shown that we can decompose any representation of a finite group into a product of irreducibles, it remains to be seen the power of irreducibility. To see this, we introduce a very powerful and useful result in representation theory, Schur's Lemma. First, we introduce some new notation.

Let V and W be two representations of G. $\mathrm{Hom}(V, W)$ is the set of all linear maps $V \to W$. $\mathrm{Hom}_G(V, W)$ is the subspace of $\mathrm{Hom}(V, W)$ containing all G-equivariant maps of $\mathrm{Hom}(V, W)$.

Lemma 9.49. *(Schur's Lemma) Let V and W be irreducible representations of G.*

(1) If V is not isomorphic to W, then $\mathrm{Hom}_G(V, W) = 0$.

(2) If $V = W$, and if k is algebraically closed, then $k \cong \mathrm{Hom}_G(V, V)$, with an isomorphism given by $\alpha \mapsto \alpha \mathrm{Id}_V$. Note that every map in $\mathrm{Hom}_G(V, W)$ can be expressed in the form $\alpha \mathrm{Id}_V$.

Proof. Let's consider claim (1) first. Let $f : V \to W$ be a G-equivariant map. Suppose f is nonzero. Then, $\ker(f) \subset V$ is a proper subrepresentation of V. Since f is nonzero, $\ker(f) \neq V$. Since V is irreducible, $\ker(f) = 0$. Similarly, $\mathrm{im}(f)$ is a subrepresentation of V. Since f is nonzero, $\mathrm{im}(f) \neq 0$. Since V is irreducible, $\mathrm{im}(f) = V$. These two claims together imply that f is a bijection, which is a contradiction, as V is not isomorphic to W. Thus, $f = 0$, and $\mathrm{Hom}_G(V, W) = 0$.

Now we prove claim (2). Let $f : V \to W$ be a G equivariant map. Since V is finite dimensional, and k is algebraically closed, f has an eigenvector and eigenvalue. Let $f(v) = \alpha v$. for some $\alpha \in k$ nonzero, $v \in V$. Note that $v \in \ker(f - \alpha \mathrm{Id}_V)$, so it is nonzero. Since V is irreducible, and $\ker(f - \alpha Id_V) \neq 0$, $\ker(f - \alpha \mathrm{Id}_V) = V$, so $f = \alpha \mathrm{Id}_V$. □

We now use Schur's Lemma to prove some remarkable corollaries.

Lemma 9.50. *Let k be algebraically closed, and V be a finite dimensional irreducible representation of G. Then, $\exists$ a homomorphism $\alpha : Z(G) \to k^\times$ such that $g \cdot v = \alpha(g)v$. $\forall g \in Z(G)$.*

Proof. for $g \in Z(G)$, note that $\varphi_g : v \mapsto g \cdot v$ is a G equivariant map. To see this, note that

$$\varphi_g(hv) = ghv = hgv = h\varphi_g(v)$$

By Schur's Lemma, $\exists$ a scalar $\alpha(g)$ such that $g \cdot v = \alpha(g)v$. The result follows. □

Lemma 9.51. *Let G be abelian, k an algebraically closed field. Then, any irreducible representation of G is 1 dimensional.*

Proof. From the previous lemma, and the fact that $Z(G) = G$, $\exists$ a homomorphism $\alpha : G \to k^\times$ such that $g \cdot v = \alpha(g)v$. This implies that any subspace of V is a subrepresentation of V. Since V is irreducible, it follows that any subrepresentation must be 0 dimensional, so V must be 1 dimensional. □

Lemma 9.52. *Let k be a field of characteristic p. If $x \in k$ such that $x^p = 1$, then $x = 1$.*

Proof.

$$x^p = 1 \Rightarrow x^p - 1^p = 0 \Rightarrow (x-1)^p = 0 \Rightarrow x - 1 = 0 \Rightarrow x = 1$$

Note that the second implication follows from Lemma 4.26. □

Lemma 9.53. *Let K be an algebraically closed field of characteristic p, and let G be a p-group. Then the only irreducible representation of G is the trivial representation.*

Proof. This is clear if $G = 1$, so suppose not, We know that $Z(G)$ is nontrivial, since G is a p-group. Applying Lemma 9.50, we know that $\exists\ \alpha : Z(G) \to k^\times$ such that $g \cdot v = \alpha(g)v$. By Lemma 9.51, since G is a p-group, $\alpha = 1$. This implies that $Z(G)$ acts trivially on V, so we can regard V as a representation on $G/Z(G)$ that is still irreducible. By induction on the order of G, it follows that V is the trivial representation. □

Note that if every irreducible representation is trivial, it follows that any completely reducible representation is trivial.

let V and W be representations of G. Observe that $\mathrm{Hom}(V, W)$ is naturally a representation of G through the action $g \cdot f(v) := g \cdot f(g^{-1} \cdot v)$.

For any representation of G U, we define U^G as the set of fixed points of the action (i.e. $U^G := \{x \in U \mid g \cdot x = x \ \ \forall g \in G\}$).

Lemma 9.54. $\mathrm{Hom}_G(V, W) = (\mathrm{Hom}(V, W))^G$

Proof. Let $f : V \to W$ be a linear map in $(\mathrm{Hom}(V, W))^G$. $g \cdot f = f$ implies that $(g \cdot f)(v) = f(v)$. From the action, we know that $g \cdot (f) = g \cdot f(g^{-1} \cdot v)$. It follows then that

$$f \in (\mathrm{Hom}(V, W))^G \iff (g \cdot f)(v) = f(v) \iff g \cdot f(v) = f(g \cdot v) \iff f \in \mathrm{Hom}_G(V, W)$$

□

Math 594: Algebra II **Winter 2019**

Lecture 10: February 14th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

Suppose G is a finite group. Then recall that every finite dimensional representation of G over $\mathbb{C}$ is completely reducible. Thus, to understand all $\mathbb{C}$ representations, it suffices to understand irreducible ones.

10.1 An Introduction to Character Theory

First, we recall some linear algebra results. We define the ***trace*** of a matrix A to be the sum of all the diagonal entries. Recall that $\mathrm{tr}(A) = \mathrm{tr}(BAB^{-1})$ for any invertible B, implying that trace in invariant under change of basis. Thus, for any linear map $T : V \to V$, $\mathrm{tr}(T) := \mathrm{tr}(A)$ for any matrix representative A.

Let $\rho : G \to \mathrm{GL}(V)$ be a representation of G We define the ***character*** of ρ (or V) to be the function

$$\chi_\rho, \chi_V : G \to \mathbb{C}$$

such that $g \mapsto \mathrm{tr}(g|_V)$, where $g|_V$ denotes the image of G under a representation.

As an example, take the permutation representation of S_3, $\rho : S_3 \to \mathrm{GL}_3(\mathbb{C})$. Observe that

$$\chi_\rho(1) = \mathrm{tr} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 3$$

$$\chi_\rho((1\ 2)) = \mathrm{tr} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 1$$

$$\chi_\rho((1\ 2\ 3)) = \mathrm{tr} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 0$$

Observe that $\chi_\rho(1) = \dim(\mathbb{C}^3)$, and that the character computes the number of fixed points for the group element. These are true in general. In general, $\chi_\rho(1) = \dim(V)$, and for any permutation representation assigned to a G-set X, $\chi_V(g)$ is the number of fixed points of g on X.

10.1.1 Basic Properties of Characters

When proving results of characters, we assume (until stated otherwise) that G is a finite group and that any representations V, W are representations over $\mathbb{C}$. $\mathbb{C}$ can in theory be any algebraically closed characteristic 0 field, but we use $\mathbb{C}$ for now.

Lemma 10.55. $V \cong W \Rightarrow \chi_V = \chi_W$.

Proof. Let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be a representation of V, and let $\sigma : G \to \mathrm{GL}_n(\mathbb{C})$ be a representation of W. $V \cong W$ implies that there exists some matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ such that $\rho(g) = A\sigma(g)A^{-1}$. Since trace is invariant under conjugation, the result follows. □

Lemma 10.56. *Let ρ be a representation of G on V and let $g, h \in G$. Then $\chi_\rho(hgh^{-1}) = \chi_\rho(g)$.*

Proof.

$$\chi_\rho(g) = \mathrm{tr}(\rho(g)) = \mathrm{tr}(\rho(h)\rho(g)\rho(h)^{-1}) = \mathrm{tr}(\rho(hgh^{-1})) = \chi_\rho(hgh^{-1})$$

□

Lemma 10.57. *Let ρ, σ be representations of G on V. Then $\chi_{\rho\oplus\sigma} = \chi_\rho + \chi_\sigma$.*

Proof. Observe that $\rho \oplus \sigma$ takes

$$g \mapsto \begin{bmatrix} \rho(g) & 0 \\ 0 & \sigma(g) \end{bmatrix}$$

And the result follows. □

Lemma 10.58. *Let ρ be a representation of G on V and let $g \in G$. Then $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.*

Proof. Since G is finite, g has finite order. Thus, $\rho(g)$ is conjugate to a matrix with roots of unity ζ_i along the diagonal. $\rho(g^{-1})$ would then be conjugate to a matrix with the inverses of those roots ζ_i^{-1} along the diagonal, which would then just be their complex conjugate $\overline{\zeta_i}$. Thus,

$$\chi_\rho(g^{-1}) = \sum_{i=1}^{n} \zeta_i^{-1} = \sum_{i=1}^{n} \overline{\zeta_i} = \overline{\chi_\rho(g)}$$

□

Recall that for two representations of G on V, W respectively, denoted $\rho : G \to \mathrm{GL}_n(\mathbb{C}), \sigma : G \to \mathrm{GL}_m(\mathbb{C})$, $\mathrm{Hom}(\rho, \sigma)$ is a natural representation. We define $\mathrm{Hom}(\rho, \sigma)$ as all linear maps A from $\mathbb{C}^n \to \mathbb{C}^m$ such that $g \cdot A = \sigma(g)A\rho(g^{-1})$. First, we prove a lemma about trace, then characterize $\chi_{\mathrm{Hom}(\rho,\sigma)}$.

Lemma 10.59. *Let X be an $n \times n$ matrix, Y an $m \times m$ matrix. define $T : \mathrm{Mat}_{m,n}(\mathbb{C}) \to \mathrm{Mat}_{m,n}(\mathbb{C})$ so that T takes $A \mapsto YAX$. Then.*

$$tr(T) = tr(X)tr(Y)$$

Proof. Observe that the set of $e_{i,j} \in \mathrm{Mat}_{m,n}(\mathbb{C})$, which takes 1 on coordinate (i, j) and 0 elsewhere, is a basis. Note that

$$T(e_{1,1}) = Y \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & & & \\ 0 & 0 & \dots & 0 \end{bmatrix} X = \begin{bmatrix} Y_{11} & 0 & \dots & 0 \\ Y_{21} & 0 & \dots & 0 \\ \vdots & & & \\ Y_{m1} & 0 & \dots & 0 \end{bmatrix} X = \begin{bmatrix} Y_{11}X_{11} & Y_{11}X_{12} & \dots & Y_{11}X_{1n} \\ Y_{21}X_{21} & Y_{21}X_{22} & \dots & Y_{21}X_{2n} \\ \vdots & & & \\ Y_{m1}X_{m1} & Y_{m1}X_{m2} & \dots & Y_{m1}X_{mn} \end{bmatrix}$$

This implies that $T_{e_{i,j}} = Y_{ii}X_{jj}E_{i,j}$ plus some other basis vectors. Thus,

$$\mathrm{tr}(T) = \sum_{i,j}(E_{i,j} \text{ coefficients}) = \sum_{i,j} X_{j,j}Y_{i,i} = \mathrm{tr}(X)\mathrm{tr}(Y)$$

□

Lemma 10.60. $\chi_{\mathrm{Hom}(\rho,\sigma)} = \overline{\chi_\rho}\chi_\sigma$.

Proof. We use Lemma 10.59, and then 10.58.

$$\chi_{\mathrm{Hom}(\rho,\sigma)} = \mathrm{tr}(\sigma(g))\mathrm{tr}(\rho(g)^{-1}) = \chi_\sigma(g)\overline{\chi_\rho(g)}$$

□

10.1.2 Computing Dimension with Characters

Lemma 10.61. *Let V be a representation of G. Then*

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

Proof. Define a linear map $A : V \to V$ such that

$$A(v) = \frac{1}{|G|}\sum_{g\in G} g\cdot v$$

clearly $gAv = Av$, so $\mathrm{im}(A) \subset V^G$. Similarly, for $v \in V^G$, $Av = v$, so we can conclude that $\mathrm{im}(A) = V^G$. Now, recall by rank nullity that $\dim(V) = \dim(\ker(A)) + \dim(\mathrm{im}(A))$. We use this notion to compute $\mathrm{tr}(A)$. let $v_1, \ldots, v_n$ denote a basis for V^G, and $v_{n+1}, \ldots, v_m$ denote a basis for $\ker(A)$. $Av_i = v_i$ $\forall 1 \le i \le n$, and $Av_i = 0$ $\forall n+1 \le j \le m$. Thus,

$$A = \begin{bmatrix} \mathrm{Id} & 0 \\ 0 & 0 \end{bmatrix}$$

so $\mathrm{tr}(A) = n = \dim(V^G)$. But, $A = \frac{1}{|G|}\sum_{g\in G}\rho(g)$, implying that $\mathrm{tr}(A) = \frac{1}{|G|}\sum_{g\in G}\chi_V(g)$, and we conclude. □

Lemma 10.62. *Let V, W be representations of G. Then,*

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

Proof. Follows from applying Lemma 10.60, Lemma 9.54, then Lemma 10.61. □

Observe that the trace function and χ_V are both invariant under conjugation. We can define a set of all of these, called ***class functions***. We define a class function on G to be a function $\varphi : G \to \mathbb{C}$ such that $\varphi(hgh^{-1}) = \varphi(g)\ \forall g, h \in G$. Let $\mathcal{C}(G)$ denote the set of all these functions. Note that $\mathcal{C}(G)$ is a $\mathbb{C}$ vector space, and has dimension equal to the number of conjugacy classes on G.

$\mathcal{C}(G)$ can in fact be imbued with an inner product. For $\psi.\varphi \in \mathcal{C}(G)$, define

$$\langle \varphi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \psi(g) = \frac{1}{|G|} \sum_{C \text{ a conjugacy class}} |C| \overline{\varphi(C)} \psi(C)$$

The second equality follows because we can instead sum over the conjugacy classes of G, since within the same conjugacy class, $\psi(g), \varphi(g)$ wouldn't change. Observe that $\langle -, - \rangle$ is a hermetian inner product, since $\langle \alpha\varphi, \beta\psi \rangle = \overline{\alpha}\beta\langle \varphi, \psi \rangle$ for $\alpha, \beta \in \mathbb{C}$. Furthermore, it is non-degenerate. For a conjugacy class C_1, C_2, define $\delta_{C_i}(g)$ to be 1 with $g \in C_i$ and 0 otherwise. Observe that

$$\langle \delta_{C_1}, \delta_{C_2} \rangle = \begin{cases} |C|/|G| & c_1 = c_2 \\ 0 & \text{otherwise} \end{cases}$$

Furthermore, from Lemma 10.62 we can conclude that

$$\dim(\mathrm{Hom}_G(V, W)) = \langle \chi_V, \chi_W \rangle$$

Note that in the irreducible case, we already know the dimension of $\mathrm{Hom}_G(V, W)$ from Schur's Lemma. This gives us a a form of orthogonality for χ_V, χ_W, called Schur Orthogonality.

Lemma 10.63. *(Schur Orthogonality) Let V, W be irreducible representations of G. Then,*

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & V = W \\ 0 & \textit{otherwise} \end{cases}$$

Proof. Observe that by Schur's Lemma,

$$\mathrm{Hom}_G(V, W) = \begin{cases} \text{(1-dimensional)} & V = W \\ 0 & \text{otherwise} \end{cases}$$

Applying the previous result, we have

$$\langle \chi_V, \chi_W \rangle = \dim(\mathrm{Hom}_G(V, W)) = \begin{cases} 1 & V = W \\ 0 & \text{otherwise} \end{cases}$$

□

As a corollary, we have that the number of irreducible representations up to isomorphism is a lower bound on the dimension of $\mathcal{C}(G)$. We prove later that equality actually holds, and that the characters of the irreducible representations actually form a basis of $\mathcal{C}(G)$.

Let ρ_{reg} denote the regular representation (the permutation representation associated to G acting on itself by left multiplication). Let χ_{reg} denote the character of this representation. Since it is a permutation representation, $\chi_{\text{reg}}(g)$ counts the number of fixed points of g. Thus,

$$\chi_{\text{reg}}(g) = \begin{cases} |G| & g = e \\ 0 & \text{otherwise} \end{cases}$$

Implying that

$$\langle \chi_V, \chi_{\text{reg}} \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)} \chi_{\text{reg}}(g) = \overline{\chi_V(1)} = \dim(V)$$

Lemma 10.64. *Let V be a representation of G, and let $V = \bigoplus_{i=1}^{n} W_i^{m_i}$ be its decomposition into irreducibles, for $W_1, \ldots, W_n$ non isomorphic irreducible representations. Then, $\langle \chi_V, \chi_{W_i} \rangle = m_i$.*

Proof. Note that by construction, $\chi_V = \sum_{i=1}^{n} m_i \chi_{W_i}$. We can then conclude the result by Schur Orthgonality. □

In the regular representation case, observe that each m_i is equal to $\dim(W_i)$. This gives us the following result:

$$\mathbb{C}[G] \cong \bigoplus_{i=1}^{r} V_i^{\dim(V_i)}$$

Taking dimension on both sides, we find that

$$|G| = \sum_{i=1}^{r} \dim(V_i)^2$$

We are now ready to conclude the dimension argument for $\mathcal{C}(G)$.

Theorem 10.65. *Let $W_1, \ldots, W_r$ be irreducible representations of G. then, $\chi_{W_1}, \ldots, \chi_{W_r}$ form a basis for $\mathcal{C}(G)$.*

Proof. Schur orthogonality tells us that all χ_{W_i} are orthogonal with each other, so we have linear independence. It is sufficient to show that $\chi_{W_1}, \ldots, \chi_{W_r}$ span $\mathcal{C}(G)$. Now we choose $\varphi \in \mathcal{C}(G)$. It is enough to show that $\langle \chi_{W_i}, \varphi \rangle = 0$ for all i implies that $\varphi = 0$.

Let (ρ, V) be any representation. Define the operation $\rho(\varphi)$ by

$$\rho(\varphi) \cdot v = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} g \cdot v$$

Well,

$$\operatorname{tr}(\rho(\varphi)) = \operatorname{tr}\left(\frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} g \cdot v \right) = \operatorname{tr}\left(\frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \rho(g) \right) = \langle \varphi, \chi_\rho \rangle$$

Furthermore, observe that $\rho(\varphi)$ is G equivariant. We see this by making a change of variables, and utilizing the fact that φ is a class function.

$$\begin{aligned}
\rho(\varphi)hv &= \frac{1}{|G|}\sum_{g\in G}\overline{\varphi(g)}gh\cdot v \\
&\Rightarrow h^{-1}\rho(\varphi)hv \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{\varphi(g)}h^{-1}gh\cdot v \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{\varphi(hgh^{-1})}g\cdot v \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{\varphi(g)}g\cdot v \\
&= \rho(\varphi)v \\
&\Rightarrow \rho(\varphi)hv = h\rho(\varphi)v
\end{aligned}$$

Finally, observe that if V is an irreducible representation, then

$$\rho(\varphi) = \frac{\langle\varphi,\chi_V\rangle}{\dim(V)}\cdot \mathrm{Id}_V$$

Since V is irreducible, it follows that $\rho(\varphi) = \alpha\cdot\mathrm{Id}_V$ for some α. Observe that

$$\langle\varphi,\chi_V\rangle = \mathrm{tr}(\rho(\varphi)) = \dim(V)\cdot\alpha$$

And the result follows.

Now, note that if $\langle\varphi,\chi_{W_i}\rangle = 0$, then $\rho(\varphi) = 0$ on any irreducible representation by the above conclusion. Since any representation is completely reducible, then $\rho(\varphi) = 0$ on any representation at all. This implies that it is zero on the regular representation, so $\rho_{\mathrm{reg}}(\varphi) = 0$. Thus,

$$\rho_{\mathrm{reg}}(\varphi)[1] = \frac{1}{|G|}\sum_{g\in G}\overline{\varphi(g)}\rho_{\mathrm{reg}}(g)\cdot[1] = \frac{1}{|G|}\sum_{g\in G}\overline{\varphi(g)}\rho_{\mathrm{reg}}(g)\cdot[g]$$

In a regular representation, $[g]$ forms a basis, so it follows that $\varphi(g) = 0\ \forall g\in G$. Thus, $\varphi = 0$, and the result follows. □

Note that this theorem implies that

$$\text{(Number of Irreducible representations)} = \dim(\mathcal{C}(G)) = \text{(Number of conjugacy classes)}$$

Furthermore, we have that Irreducible characters form an orthonormal basis for $\mathcal{C}(G)$.

Math 594: Algebra II **Winter 2019**

Lecture 11: February 19th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

11.1 The Representation Ring

Let $\mathcal{R}_+(G) \subset \mathcal{C}(G)$ denote the set of all characters. We've already shown that $\chi_V + \chi_W = \chi_{V\oplus W}$ is a character, so we have closure under addition. Furthermore, $\chi_V\chi_W = \chi_{V\otimes W}$ is a character, so we also have closure under multiplication. Furthermore, note that χ_1, the character for the trivial representation, is the multiplicative identity. This is really close to being a ring! The problem is, we don't have additive inverses. We remedy this as follows:

A ***Virtual Character*** is an element of $\mathcal{C}(G)$ of the form $\chi_V - \chi_W$ where V, W are representations. Let $\mathcal{R}(G)$ denote the set of all characters and virtual characters. This is closed under $+, -, \times$, and conjugation. Thus, $\mathcal{R}(G)$ is a ring! We call $\mathcal{R}(G)$ the ***Representation Ring*** of G.

We now do an example. Let $G = \mathbb{Z}/4\mathbb{Z} = \langle\sigma\rangle$. We compute the character table below:

	1	σ	σ^2	σ^3
χ_1	1	1	1	1
χ_2	1	i	-1	$-i$
χ_3	1	-1	1	-1
χ_4	1	$-i$	-1	i

Where χ_1 is the character of the trivial representation. We won't explain why this character table looks like this here, but note that every irreducible representation over an abelian group is 1 dimensional, so we have 1s along the first column. After that, we compute the remaining values by utilizing the order of $\mathbb{Z}/4\mathbb{Z}$, and the fact that over $\mathbb{C}$, $i, -i$ are the only order 4 elements.

Note that χ_1 is the "1" element of $\mathcal{R}(G)$. If we denote χ_2 as x, observe that $\chi_3 = x^2, \chi_4 = x^3$. Thus, we have that

$$\mathcal{R}(G) \cong \mathbb{Z} \oplus \mathbb{Z}x \oplus \mathbb{Z}x^2 \oplus \mathbb{Z}x^3 = \mathbb{Z}[x]/(x^4 - 1)$$

In general, if $\chi_1, \ldots, \chi_r$ are irreducible characters of G, for any representation V $\chi_V = m_1\chi_1 + \cdots + m_r\chi_r$ for $m_1, \ldots, m_r$ such that

$$V = \bigoplus_{i=1}^{r} W_i^{\oplus m_i}$$

This implies that $\mathcal{R}_+(G) = \mathbb{Z}_{\geq 0}\chi_1 + \cdots + \mathbb{Z}_{\geq 0}\chi_1$. Implying that

$$\mathcal{R}(G) = \mathbb{Z}\chi_1 + \cdots + \mathbb{Z}\chi_r$$

so $\mathcal{R}(G) \cong \mathbb{Z}^r$.

11.2 Character table of D_5

We compute the character table of $G = D_5 = \langle a, b \mid a^2 = 1, b^5 = 1, aba = b^{-1}\rangle$. G has 4 conjugacy classes, and thus 4 irreducible representations. One of these is the trivial representation, so it will always compute to 1 on each conjugacy class. Furthermore, using the fact that $\sum(\dim V_i)^2 = |G| = 10$ for V_i each irreducible representation, note that the only way to sum 4 squares to 10 is $1 + 1 + 4 + 4$. This gives us the following table:

	C_1	C_2	C_3	C_4
χ_1	1	1	1	1
χ_2	1			
χ_3	2			
χ_4	2			

Now, observe that $D_5 = \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/5\mathbb{Z}$ This implies that D_5 factors through $\mathbb{Z}/2 \cong D_5/(b)$, and any 2 dimensional representation ρ_n is of the form

$$\begin{aligned} \rho_n : & D_5 \to \mathrm{GL}_2(\mathbb{C}) \\ & a \mapsto \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \\ & b \mapsto \begin{bmatrix} e^{2\pi i n/5} & 0 \\ 0 & e^{-2\pi i n/5} \end{bmatrix} \end{aligned}$$

For $n = 1, 2$. This allows us to solve for the rest of the character table.

	C_1	C_2	C_3	C_4
χ_1	1	1	1	1
χ_2	1	1	1	-1
χ_3	2	$2\cos(2\pi/5)$	$2\cos(4\pi/5)$	0
χ_4	2	$2\cos(4\pi/5)$	$2\cos(8\pi/5)$	0

The last two rows follow from this representation, and the row for χ_2 follows from an orthogonality argument.

11.3 Character table of S_5

Before preceeding, we prove a simple lemma.

Lemma 11.66. *if χ_V is an irreducible character, and χ_W is 1 dimensional, then $\chi_V\chi_W$ forms an irreducible representation.*

Proof. Suppose not. Then $\chi_V\chi_W$ can be written as a sum of irreducible characters as follows:

$$\chi_V\chi_W = \chi_1 + \cdots + \chi_n$$

For $n \geq 2$. Well, this implies that

$$\chi_V = \chi_1\overline{\chi_W} + \cdots = \chi_n\overline{\chi_W}$$

This is a contradiction, since χ_V is irreducible. □

We will now compute the character table of S_5. Recall that conjugacy classes of S_n correspond to n-partitions (see 3.2.2 for more information). Thus, S_5 has 7 conjugacy classes, corresponding to the possible ways to partition 5. This implies that there are 7 conjugacy classes for S_5. One of these is the trivial representation. Furthermore, we can combinatorially compute the size of each of the conjugacy classes. This gives us the following character table:

conj. class	(1)	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3)(4 5)	(1 2 3 4)	(1 2 3 4 5)
partition	$\sum_5 1$	$2+\sum_4 1$	$2+2+1$	$3+1+1$	$3+2$	$4+1$	5
size	1	10	15	20	20	30	24
χ_1	1	1	1	1	1	1	1
χ_2							
χ_3							
χ_4							
χ_5							
χ_6							
χ_7							

What other irreducible representations are there? Well, we have a sign representation, which is 1 dimensional, and who's simply takes each permutation to its sign, 1 or -1. We also have the standard representation, which is characterized as follows:

Recall the permutation representation $S_5 \circlearrowright \mathbb{C}^5$, which acts by permuting the coefficients of the basis vectors. Consider the vector space $V \subset \mathbb{C}^5$ where the coefficients sum to zero. This is stable under the group action, and is the standard representation of S_5. Note that this is 4 dimensional, as we can parameterize the coefficients by $(z_1, z_2, z_3, z_4, 1 - \sum z_i)$. We know that $\chi_1 + \chi_{\text{std}} = \chi_{\text{perm}}$, and χ_{perm} is computed by counting the number of fixed points in the permutation, or 1s in the partition. Thus, to compute χ_{std}, we just count the number of 1s and subtract 1 this gives us

conj. class	(1)	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3)(4 5)	(1 2 3 4)	(1 2 3 4 5)
partition	$\sum_5 1$	$2+\sum_4 1$	$2+2+1$	$3+1+1$	$3+2$	$4+1$	5
size	1	10	15	20	20	30	24
χ_1	1	1	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1	-1	1
χ_{std}	4	2	0	1	-1	0	-1
χ_4							
χ_5							
χ_6							
χ_7							

Recall from lemma 11.66, $\chi_{\text{sgn}\otimes\text{std}}$ is also an irreducible representation. This is computed by just taking the product of the χ_{std} and χ_{sgn}.

	(1)	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3)(4 5)	(1 2 3 4)	(1 2 3 4 5)
partition	$\sum_5 1$	$2+\sum_4 1$	$2+2+1$	$3+1+1$	$3+2$	$4+1$	5
size	1	10	15	20	20	30	24
χ_1	1	1	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1	-1	1
χ_{std}	4	2	0	1	-1	0	-1
$\chi_{\text{sgn}\otimes\text{std}}$	4	-2	0	1	1	0	-1
χ_5							
χ_6							
χ_7							

Note that $\chi_6 := \chi_5\chi_{\text{sgn}}$ is also an irreducible representation, so we know that they have the same dimension. There is only way to sum two of the same square, another square, $1, 1, 1, 4$ and 4 to get 5!, or the order of G, so we know the dimensions of the rest of the representations. We also know that χ_7 is fixed by the sign representation (since if it wasn't we'd have another unique irreducible representation), implying that $\chi_{7\otimes\text{sgn}} = \chi_7$. Thus, wherever the sign of the permutation is -1, χ_7 is zero, since it must be fixed via multiplication.

	(1)	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3)(4 5)	(1 2 3 4)	(1 2 3 4 5)
partition	$\sum_5 1$	$2+\sum_4 1$	$2+2+1$	$3+1+1$	$3+2$	$4+1$	5
size	1	10	15	20	20	30	24
χ_1	1	1	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1	-1	1
χ_{std}	4	2	0	1	-1	0	-1
$\chi_{\text{sgn}\otimes\text{std}}$	4	-2	0	1	1	0	-1
χ_5	5						
$\chi_{5\otimes\text{sgn}}$	5						
χ_7	6	0			0	0	

We finish this computation in the next lecture.

Math 594: Algebra II **Winter 2019**

Lecture 12: February 21st

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

12.1 Finishing the character table of S_5

We continue with computing the character table of S_5. We proceed with constructing the χ_5 term. Let X denote the set of all subset of $\{1,2,3,4,5\}$ of cardinality 2. $S_5 \circlearrowright X$ by permuting the tuples. This gives us a permutation representation $\mathbb{C}[X]$, which is $|X| = \binom{5}{2} = 10$ dimensional. because this is a permutation representation, $\chi_V(g)$ computes the number of fixed points of $g \in S_5$.

If g is a fixed point, then $g \cdot \{i,j\} = \{i,j\}$. There are two ways this happens. Either g fixes i and j, or $g \cdot i = j, g \cdot j = i$. The number of times the first case occurs is precisely the number of 1s in the partition associated with g choose 2, and the number of times the second case occurs are the number of 2s in the partition associated with g. Observe that $\langle \chi_V, \chi_1 \rangle = \langle \chi_V, \chi_{\text{std}} \rangle = 1$. Setting $\varphi = \chi_v - \chi_1 - \chi_{\text{std}}$, I claim that φ is an irreducible character. We can compute that $\langle \varphi, \varphi \rangle = 1$, implying that φ is irreducible as desired. By counting the dimension $\chi_v - \chi_1 - \chi_{\text{std}}$ we can set $\varphi = \chi_5$. We can compute $\chi, \chi_1, \chi_{\text{std}}$ on any $g \in S_5$, so we can compute χ_5 and χ_6, the latter of which which we defined as the product of χ_5 and χ_{sgn}.

	(1)	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3)(4 5)	(1 2 3 4)	(1 2 3 4 5)
partition	$\sum_5 1$	$2 + \sum_4 1$	$2+2+1$	$3+1+1$	$3+2$	$4+1$	5
size	1	10	15	20	20	30	24
χ_1	1	1	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1	-1	1
χ_{std}	4	2	0	1	-1	0	-1
$\chi_{\text{sgn}\otimes\text{std}}$	4	-2	0	1	1	0	-1
χ_5	5	1	1	-1	1	-1	0
$\chi_{5\otimes\text{sgn}}$	5	-1	1	-1	-1	1	0
χ_7	6	0			0	0	

We can then compute χ_7 using orthogonality arguments, since $\langle \chi_7, \chi_i \rangle = 0 \ \forall i < 7$. This gives us the final character table:

	(1)	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3)(4 5)	(1 2 3 4)	(1 2 3 4 5)
partition	$\sum_5 1$	$2+\sum_4 1$	$2+2+1$	$3+1+1$	$3+2$	$4+1$	5
size	1	10	15	20	20	30	24
χ_1	1	1	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1	-1	1
χ_{std}	4	2	0	1	-1	0	-1
$\chi_{\text{sgn}\otimes\text{std}}$	4	-2	0	1	1	0	-1
χ_5	5	1	1	-1	1	-1	0
$\chi_{5\otimes\text{sgn}}$	5	-1	1	-1	-1	1	0
χ_7	6	0	-2	0	0	0	1

12.2 Induced Characters and the Schur Functor

Let X denote the set of all subset of $\{1,2,3,4,5\}$ of cardinality 2 as before. We know that $S_5 \circlearrowright X$ by permuting the tuples.$\{1,2\}$ has stabilizer $S_2 \times S_3$, since S_2 corresponds to just swapping the elements, and S_3 corresponds to the permutations on $3,4,5$ which fix $1,2$. Note that $S_5 \circlearrowright X$ defines a transitive action. This implies that $X \cong S_5/(S_2 \times S_3)$ by Theorem 2.10. Thus, $\mathbb{C}[X] \cong \mathbb{C}[G/H]$ as representations. Turns out, this generalizes!

12.2.1 A Generalization of the Permutation Representation

If G is a group and H is any subgroup, We get a permutation representation $\mathbb{C}[G/H]$.

Example: Let $G = S_5, H = S_1 \times S_4$. $G/H \cong \{1,2,3,4,5\}$, so $\mathbb{C}[G/H] \cong \mathbb{C}^5$.

But, we can generalize this even further. Note that any element in $\mathbb{C}[G/H]$ has the form $\sum_{g\in G/H} c(g)[g]$, for some complex numbers c dependent on g, hence we denote then $c(g)$. This is actually just a function on left cosets $c : G/H \to \mathbb{C}$ such that $g \mapsto c(g)$. A similar construction can be realized for right cosets: $H\backslash G \to \mathbb{C}$ where $g \mapsto c'(g) := c(g^{-1})$. Observe that since we are in the quotient of h, these maps are fixed under H. In other words, $c(hg) = c(g)\ \forall h \in H, g \in G$. We define a set of all of these such functions:

$$\text{Fun}_H(G,\mathbb{C}) := \{f : G \to \mathbb{C} \mid f(hg) = f(g)\}$$

We see that

$$\text{Fun}_H(G,\mathbb{C}) \cong \mathbb{C}[G/H]$$

Where $f \in \text{Fun}_H(G,\mathbb{C})$ maps to $\sum_{g\in G/H} f(g^{-1})[g]$ under the isomorphism.

12.2.2 The Induced Representation

We define an action $G \circlearrowright \text{Fun}_H(G,\mathbb{C})$ by $(g \cdot f)(g') = f(g'g)$. this allows us to easily extend the definition of $\text{Fun}_H(G,\mathbb{C})$ to any representation. For any G representation V, define

$$\text{Fun}_H(G,V) := \{f : G \to V \mid f(hg) = f(g)\}$$

Where the action is above. This is the ***induced representation*** on V by H, denoted $\mathrm{Ind}_H^G(V)$.

Examples:

$$\mathbb{C}^5 \cong \mathbb{C}[S_5/(S_4 \times S_1)] \cong \mathrm{Ind}_{S_4 \times S_1}^{S_5}(\text{trivial rep.})$$

$$\mathbb{C}[X] \cong \mathbb{C}[S_5/(S_3 \times S_2)] \cong \mathrm{Ind}_{S_3 \times S_2}^{S_5}(\text{trivial rep.})$$

We have the following strong theorem on the characters of these induced representations.

Theorem 12.67. *(Brower's Theorem for Induced Characters) Let G be a finite group. Let 1_H denote the set of all 1 dimensional representations of H, for H any subgroup of G. Then,*

$$\{\mathrm{Ind}_H^G(V) \mid V \in 1_H, H \subset G\}$$

generates $\mathcal{R}(G)$ (the ring of virtual characters) as an abelian group.

12.2.3 The Schur Functor

Let V, W be representations of G. naturally, $V \otimes W$ is a representation of G, where $G \circlearrowright V \otimes W$ by $g \cdot (v \otimes w) = gv \otimes gw$ (While this is only defined on elementary tensors, the general definition follows linearly). Recall that $\chi_V \chi_W = \chi_{V \otimes W}$. In addition, we have that $\mathrm{Hom}(V, W) \cong V^* \otimes W$.

From here, we know that $V \otimes V$ is a G representation. Note that $S_2 \circlearrowright V \otimes V$ by swapping the entries around. This action commutes with the G action (i.e. $\sigma \cdot g \cdot (v \otimes v') = g \cdot \sigma \cdot (v \otimes v')$ for any $g \in G$, $\sigma \in S_2$). Thus, we can realize $V \otimes V$ as a representation of $S_2 \times G$, where

$$(\sigma, g) \cdot (v \otimes v') = \sigma \cdot g \cdot (v \otimes v') = g \cdot \sigma \cdot (v \otimes v')$$

Now consider the subspace $W \subset V \otimes V$ consisting of elements fixed by S_2. We denote this as $\mathrm{Sym}^2(V)$ (you may have seen this notation used to describe a certain quotient vector space of $V \otimes V$; these are the same thing.) Turns out, this is a G stable subrepresentation. This follows from the commutativity of the actions. We wish to show that if $x \in W, g \cdot x \in W$. Well, $\sigma \cdot g \cdot x = g \cdot \sigma \cdot x = g \cdot x$, so $\mathrm{Sym}^2(V)$ is G stable.

In general, if V is a representation of G, then $V^H := \{v \in V \mid h \cdot v = v \ \forall h \in H\}$ is a G subrepresentation. Consider W^-, the subspace of elements where $(1\ 2) \cdot x = -x$. This is $\bigwedge^2(V)$ (you may have also seen this as a quotient vector space of $V \otimes V$; still the same thing). In general, $V \otimes V = \mathrm{Sym}^2(V) \oplus \bigwedge^2(V)$.

If you recall from our character table of S^5, Our 6 dimensional irreducible representation, with character denoted χ_7, is actually $\bigwedge^2(V)$, for V the standard representation of S_5, with character denoted χ_3.

As one would think, this generalizes to $V^{\otimes n}$. $G \times S_n \circlearrowright V^{\otimes n}$ from similar logic to above, and

$$\mathrm{Sym}^n(V) = \{x \in V^{\otimes n} \mid \sigma x = x \ \forall \sigma \in S_n\}$$

$$\bigwedge^n(V) = \{x \in V^{\otimes n} \mid \sigma x = (\text{sgn}\sigma)x \ \forall \sigma \in S_n\}$$

We can extend this further. If W is a representation of S_n, we can consider $\text{Hom}_{S_n}(W, V^{\otimes n})$ (the S_n equivariant linear maps between $W, V^{\otimes n}$) as a representation of G, with action $(g \cdot f)(w) = g \cdot f(w)$. Recall that irreducible representations of S_n are are naturally parameterized by n-partitions. Given some partition λ of n, we have an associated irreducible representation W_λ of S_n. We define the ***Schur Functor*** associated with partition λ to be the functor

$$S_\lambda(V) = \text{Hom}_{S_n}(W_\lambda, V^{\otimes n})$$

Math 594: Algebra II **Winter 2019**

Lecture 13: March 12th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

13.3 An Introduction to Field Theory

We now move onto the third part of the course, Field Theory. We will primarily concern ourselves with field extensions and their properties. We first reviews some basics of fields, then the basics of extensions. After that, we tackle algebraic numbers, algebraic extensions, and algebraic closure. Finally, we lightly touch on transcendental extensions, before moving on to the final main topic of the course, Galois Theory.

13.3.1 Field Basics, Homomorphisms, and Characteristic

A ***Field*** is a set K equipped with two operations, $+$ (addition) and $\cdot$ (multiplication) such that

- $(K, +)$ forms an abelian group, with identity 0.
- $(K\backslash\{0\}, \cdot)$ forms an abelian group, with identity 1 (where $0 \neq 1$). This is often referred to as the ***multiplicative group*** of K and is denoted $K^\times$.
- Distributive law holds (i.e. $\forall x, y, z \in K, x(y+z) = xy + xz$)

For those familiar with ring theory, one can think of a field K as an integral domain where all nonzero elements are unit, and $0 \neq 1$. Thus, any field has an inherent ring structure. We now proceed with some examples of fields.

13.3.1.1 Examples:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields. We will see later that $\mathbb{R}$ is a field extension of $\mathbb{Q}$, and $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.
- $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a field, but only for p prime.
- Let $K = \{0, 1, \omega, \omega + 1\}$ such that $1 + 1 = 0, 1 + (\omega + 1) = \omega, \omega^2 = \omega + 1$. This is a field, and is actually the unique field up to isomorphism on 4 elements, and is often denoted $\mathbb{F}_4$.

- $\mathbb{Q}(i)$, or the $\mathbb{Q}$-span of $\{1, i\}$ in $\mathbb{C}$. This is a simple example of a field extension. We will see more of these.
- If K is any field, let $K(T)$ denote the set of rational functions in the variable T with coefficients in K. This forms a field. To see why, note that $K(T)$ is the field of fractions of $K[T]$, or the ring of polynomial functions on T with coefficients in K.

Now that we know about some fields, it makes sense to discuss maps between them. For K, L fields, $f : K \to L$ is a ***field homomorphism*** if f is compatible with $+, \cdot$ and satisfies $f(0) = 0, f(1) = 1$. A ***field isomorphism*** is a bijective field homomorphism.

Lemma 13.68. *All field homomorphisms are injective.*

Proof. Let $f : K \to L$ denote a field homomorphism, and choose $x \in \ker(f)$, and suppose that $x \neq 0$. We wish to derive a contradiction, which would show that the kernel is trivial. Well,

$$1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1}) = 0f(x^{-1}) = 0$$

A contradiction. Thus, f is injective. □

For K a field, we have a natural ring homomorphism $\varphi : \mathbb{Z} \to K$ where $n \mapsto \sum_n 1$. Either this map is injective, or it is not. If it is, then $1 + 1 + \ldots \neq 0$ in K for any number of 1s. If this is true, we say that K is ***Characteristic*** 0. We now consider the case where φ is not injective. Let n be the minimal $n > 0$ such that $\varphi(n) = 0$. First, observe that n is prime. If it wasn't, then we could say that $n = ab$ for $a, b \neq 1$. Then

$$0 = \varphi(n) = \varphi(ab) = \varphi(a)\varphi(b)$$

Implying that one of $\varphi(a)$ or $\varphi(b)$ is zero, violating the minimality of n. Thus, n is prime. Thus, $\ker(\varphi)$ is of the form $p\mathbb{Z}$, and φ induces an injection $\mathbb{Z}/p\mathbb{Z} \to K$. If this is the case, we say that K has ***characteristic*** p. Note that characteristic is NOT the order of the field, we can have characteristic p fields that are of order p^n, and even infinite ones!

13.3.2 Field Extensions

An ***Extension*** is a tuple (L, K, i) where L, K are fields, and $i : K \to L$ is a field homomorphism. We usually identify K as a subfield of L, and denote the extension L/K.

Observe that for a field extension L/K, we can treat L as a K-vector space (this is clear; in fact, L is an L-vector space). We denote the ***degree*** of L/K as $[L : K] = \dim_K(L)$. We now go through some examples of field extensions and their degrees:

13.3.2.1 Examples:

- $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, since $\mathbb{Q}(i)$ has $\mathbb{Q}$-basis $\{1, i\}$.
- $[\mathbb{C} : \mathbb{R}] = 2$, since $\mathbb{C}$ has $\mathbb{R}$-basis $\{1, i\}$.
- $[\mathbb{F}_4, \mathbb{F}_2] = 2$, since $\mathbb{F}_4$ (as in the third example in 14.2.1.1) has $\mathbb{F}_2$ basis $\{1, \omega\}$.
- $[\mathbb{C}(T) : \mathbb{C}] = \infty$, since $(T, T^2, T^3, \dots)$ are all $\mathbb{C}$-linearly independent.

13.3.3 Algebraic and Transcendental Numbers

Let L/K be an extension, and $x \in L$. We say that x is ***algebraic*** over K if $\exists f \in K[T]$ monic (the first coefficient is 1) such that $f(x) = 0$. Observe that any polynomial can be written this way since K is a field, as we can divide by the coefficient of the leading term. If x is not algebraic, x is ***transcendental***.

13.3.3.1 Examples:

- $\sqrt{2} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ (our corresponding function $f(x) = x^2 - 2$ has coefficients in $\mathbb{Q}$)
- $e, \pi \in \mathbb{C}$ are transcendental over $\mathbb{Q}$ (this is known to many, but is actually a nontrivial result).
- $T \in K(T)$ is transcendental over K.

Lemma 13.69. *Let L/K be an extension. Let $K \subset A \subset L$ be a subset such that A is closed under $+, \cdot$ and contains $1, 0$, and $\dim_K(A) < \infty$. Then,*

(a) Every element of A is algebraic over K.

(b) A is a field.

Proof. We prove part (a) first. Let $x \in A$ be nonzero. Then $\{1, x, x^2, \dots\}$ form a linearly dependent set over A (since A is finite degree, and this is an infinite set). Thus, there is some K-algebraic relation that x satisfies, so x is algebraic over A.

We now prove part (b). Note that for any $x \in A$, we have a term $x^{-1} \in L$. We just wish to show that $x^{-1} \in A$, and then we can conclude that A is a field. Choose a_i such that

$$x^d + a_{d-1}x^{d-1} + \cdots + a_0 = 0$$

This implies that

$$x^{d-1} + a_{d-1}x^{d-2} + \cdots + a_0 x^{-1} = 0$$

Further implying that

$$x^{-1} = -\frac{x^{d-1} + a_{d-1}x^{d-2} + \cdots + a_1}{a_0} \in A$$

□

Lemma 13.70. *Let L/K be an extension, and $x \in L$. Then the following are equivalent:*

(1) x is algebraic over K.

(2) $\exists$ a field $K \subset M \subset L$ such that $[M : K] < \infty$, and $x \in M$.

(3) $\exists$ a subring $K \subset A \subset L$ such that $\dim_K(A) < \infty$ and $x \in A$.

Proof. We already know (2) $\iff$ (3) $\Rightarrow$ (1) by the previous lemma, so it suffices to show that (1) $\Rightarrow$ (3). Suppose x is algebraic. Then $\exists a_i$ such that

$$x^d + a_{d-1}x^{d-1} + \cdots + a_0 = 0$$

Let

$$A = \text{span}_K(1, x^2, x^3, \ldots, x^{d-1})$$

Clearly $\dim_K(A) < \infty$, and is closed under multiplication by the existence of the polynomial above. The result follows. □

Math 594: Algebra II **Winter 2019**

Lecture 14: March 14th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

14.1 More on Field Extensions

Recall Lemma 14.70 from last class. We used this to prove the following corollary:

Lemma 14.71. *Let $x, y \in L/K$ be algebraic over K. Then $x + y, xy, x^{-1}$ are all algebraic over K.*

The proof is omitted, but is a simple symbol push. This allows us to define an extension of K (and subfield of L) consisting of all elements in L that are algebraic over K. As an example,

$$\overline{\mathbb{Q}} := \{x \in \mathbb{C} \mid x \text{ is algebraic over } \mathbb{Q}\}$$

is defined as the ***field of algebraic numbers.***

14.1.1 Generating Sets of Extensions

Let L/K denote an extension, and $S \subset L$. Then, $\exists$ a smallest subfield of L containing both S and K. We denote this the ***subextension of*** L/K ***generated by*** S. If $S = \{a_1, \ldots, a_n\}$, we denote this field $K(a_1, \ldots, a_n)$. L/K is said to be ***finitely generated*** if it is generated by a finite set of elements.

Suppose, for L/K an extension, $K(a)$ is the extension generated by some $a \in L$. We have two possibilities. If $[K(a) : K] < \infty$, then a is algebraic. If not, then a is transcendental. We let $[K(a) : K]$ denote the ***degree*** of a.

14.1.2 Minimal polynomials

If a is algebraic over L/K, then $\exists f \in K[T]$ monic (the first coefficient is 1) such that $f(x) = 0$. We claim that there exists a unique polynomial satisfying this condition that is of degree equal to $\deg(a)$. This is the ***minimal polynomial*** of a. We now prove existence and uniqueness:

Lemma 14.72. *For any a algebraic over L/K, there exists a minimal polynomial, and it is unique.*

Proof. let $n = \deg(a) = \dim_K(K(a))$. Then, $1, \ldots, a^n$ are linearly dependent, since a is algebraic. Furthermore, a does not satisfy a polynomial (meaning, there does not exist an f such that $f(a) = 0$) of degree $m < n$. If there did exist such a polynomial, it is easy to see that then $\deg(a) = m < n$, a contradiction. Since $1, \ldots, a^n$ are linearly dependent, $\exists b_i$ such that $b_n a^n + \cdots + b_0 = 0$. We now have a minimal polynomial, that is monic with coefficients b_i/b_n, and has degree $\deg(a) = n$.

For uniqueness, observe that if two such polynomials existed, say f, g, then $f(a) = g(a) = 0 \Rightarrow (f - g)(a) = 0$. But $\deg(f - g) < n$, so $f = g$ by minimality. □

14.1.3 Algebraic Extensions

We now prove some simple results about extensions. Let $M/L, L/K$ be extensions (these are often denoted in tower notation, like so:

$$\begin{array}{c} M \\ | \\ L \\ | \\ K \end{array}$$

But we won't do that here.

Lemma 14.73. *For M, L, K as above, $[M : K] = [M : L][L : K]$.*

Proof. Let $\{x_1, \ldots, x_n\}$ denote a K basis for L, and $\{y_1, \ldots, y_m\}$ denote a L basis for M. I claim that $\{x_i y_j \mid i \in [1, n], j \in [1, m]\}$ is a K basis for M. This would complete the proof, as this set has cardinality mn. First, we check that this spans.

Let $z \in M$. Since y_j's form an L basis for M, we have that $z = \alpha_1 y_1 + \ldots \alpha_m y_m$. for some $\alpha_i \in L$. Since x_i's are a K basis for L, it follows that every $\alpha_i = \beta_{i_1} x_1 + \cdots + \beta_{i_n} x_n$ for some $\beta_{i_j} \in K$. It follows that

$$z = \sum_{i,j=1}^{m,n} \beta_{i_j} x_j y_i$$

Completing the proof.

To conclude, we check linear independence. Suppose

$$0 = \sum_{i,j=1}^{n,m} \beta_{i_j} x_i y_j$$

(Note here that we switched our indexing) We want to show that $\beta_{i_j} = 0 \ \forall i, j$. Well,

$$\sum_{i,j=1}^{n,m} \beta_{i_j} x_i y_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \beta_{i_j} x_i \right) y_j$$

And by linear independence of the y_j's in L, $\left(\sum_{i=1}^{n} \beta_{i_j} x_i\right) = 0 \ \forall j$. Well, by linear independence of the x_i's, it follows that $\beta_{i_j} = 0 \ \forall i, j$. $\square$

We say L/K is an ***algebraic extension*** if all elements of L are algebraic over K. Otherwise, we say that L/K is a ***transcendental extension***. From the above lemma, we can easily conclude the following two results.

Lemma 14.74. *Let M/L,L/K be extensions. If these are both algebraic extensions, then M/K is an algebraic extension.*

Lemma 14.75. *let L/K be an extension. Then, the following are equivalent.*

1) $[L : K] < \infty$

2) L is generated by finitely many algebraic elements.

Math 594: Algebra II **Winter 2019**

Lecture 15: March 19th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

15.1 Stem Fields

Suppose K/F and L/F are extensions. We define an ***F-homomorphism*** $K \to L$ to be a field homomorphism which is the identity on elements of F. An ***F-isomorphism*** is a bijective F-homomorphism.

Let $f \in F[x]$ be an irreducible polynomial. Then, a ***stem field*** for f is a pair $(E/F, \alpha)$ where

- E/F is an extension.
- α is a root of f.
- $E = F(\alpha)$.

Two things we may want to know about stem fields are their existence and uniqueness. We give an explicit construction of a stem field below, then show that two stem fields of the same polynomial are isomorphic.

Lemma 15.76. *Let $f \in F[x]$ be irreducible, for a field F. Let $L = F[x]/(f)$.*

(1) L is a field, and $(L/F, x)$ is a stem field for f.

(2) If $(E/F, \alpha), (E'/F, \alpha')$ are two stem fields for f, then $\exists!$ F-isomorphism $E \to E'$ such that $\alpha \mapsto \alpha'$.

Proof. We first prove (1). L is a field because an ideal generated by an irreducible element is maximal over a PID (which any polynomial ring over a field is). To see why, note that if (f) was not maximal, then $\exists$ an ideal (g) such that $(f) \subsetneq (g) \subsetneq (1)$. But then $g|f$, a contradiction to irreducibility. Since the quotient of a ring by a maximal ideal is a field, it follows that $L = F[x]/(f)$ is a field. $f(x) = 0$ in L because it is in the quotient, so x is a root of f. It follows then that $(L/F, x)$ is a stem field of f.

We now prove (2). Without loss of generality, let $E = F[x]/(f)$, and $\alpha = x$, and let $(E'/F, \alpha)$ be some other stem field of f. $\exists$ a unique F-homomorphism of rings $\varphi : F[x] \to E$ which sends $x \to \alpha'$. Because φ is an F-homomorphism, $f \in \ker(\varphi)$. Thus, φ induces a map $\overline{\varphi} : F[x]/(f) \to E'$. φ is a field homomorphism, and thus injective. It is surjective because $\mathrm{im}(\overline{\varphi})$ contains both F and α', and they generate E'. Thus,

$$E = F[x]/(f) \cong E'$$

□

We also have a mapping property of stem fields:

Lemma 15.77. *Let $(E/F, \alpha)$ be a stem field for F, and let K/F be another extension. Then, we have a bijection*

$$\{F\text{-homomorphisms } E \to K\} \cong \{\text{roots of } f \text{ in } K\}$$

Where

$$\varphi \mapsto \varphi(\alpha)$$

Proof. We first check well definedness. If $\varphi : E \to K$ is a F-homomorphism, then $0 = \varphi(f(\alpha)) = f(\varphi(\alpha))$, since coefficients of f are in F, and $\varphi = \text{Id}$ on F. This implies that $\varphi(\alpha)$ is a root of f, as desired. We now check that this is a bijection.

For injectivity, observe that since α generates E over F, and F-homomorphism is defined by where α goes. For surjectivity, If $\beta \in K$ is a root of f, then we have an F-homomorphism

$$F[x]/(f) \to K$$

which maps $x \to \beta$. Combining this with the unique isomorphism

$$(F[x]/(f), x) \cong (E/F, \alpha)$$

gives us the F-homomorphism $E \to K$ we want. □

Computing the degree of stem fields is also easy.

Lemma 15.78. *If $(E/F, \alpha)$ is a stem field for f, then $[E : F] = \deg_F(\alpha) = \deg(f)$.*

15.2 Splitting Fields

Given $f \in F[x]$ and an extension K/F, we say that f ***splits*** over K if f factors into linear factors in $K[x]$ (in other words, K contains all the roots of f).

For $f \in F[x]$ non-constant, An extension E/F is called a ***splitting field*** for f if

- f splits over E.
- E is generated (as an extension of F) by roots of f.

The next natural question, as with stem fields, are if splitting fields exist, and if they are unique up to isomorphism. The answer to both of these questions is yes.

Lemma 15.79. *Any $f \in F[x]$ has a splitting field E/F of degree $\leq \deg(f)!$.*

Proof. Let $K_0 = F$. Let K_1 be the stem field for an irreducible factor of f over K_0. Over K_1, f will factor as $f(x) = f_1(x)(x - \alpha_1)$. We know that $[K_1 : K_0] \leq \deg(f)$, and $\deg(f_1) = \deg(f) - 1$. If f_1 splits over K_1, then K_1 is our splitting field. If not, we construct K_2 similarly. Observe that $[K_2 : K_1] \leq \deg(f_1) = \deg(f) - 1$. If K_2 is our splitting field, then we're done. If not, we continue this process up to some K_n (this process eventually halts, since the degree of f_i will always decrease). Observe that

$$[K_n : K_0] = [K_1 : K_0][K_2 : K_1] \dots [K_n : K_{n-1}] \leq \deg(f)(\deg(f)-1)(\deg(f)-2)\cdots = \deg(f)!$$

And K_n is clearly generated by roots of f, so K_n is our splitting field of f. □

Lemma 15.80. *Let $f \in F[x]$ be some nonconstant polynomial over a field F. Let E/F be an extension generated by roots of f, and let K/F be an extension over which f splits. Then,*

(1) $\exists$ an F-homomorphism $E \to K$.

(2) The number of such F-homomorphisms $E \to K$ is $\leq [E : F]$.

(3) If f has distinct roots over K, then the number of such F-homomorphisms $E \to K$ is exactly equal to $[E : F]$.

Proof. Let $E = F(\alpha_1, \dots, \alpha_n)$ for α_i roots of f. I claim there exists an F-homomorphism $F(\alpha_1) \to K$. To show this, let g be the minimal polynomial for α_1 over F. $g|f$, so g splits into linear factors over K. $F(\alpha_1)$ is a stem field for g, and by the mapping property of stem fields, there exists an F-homomorphism $F(\alpha_1) \to K$. Furthermore, the number of roots of g in K has size $\leq \deg(g) = [F(\alpha_1) : F]$ (with equality if and only if f has distinct roots).

Fix an F-homomorphism $i_1 : F(\alpha_1) \to K$. let g be the minimal polynomial of α_2 over $F(\alpha_1)$. $g|f$, so g splits over K, and $F(\alpha_1, \alpha_2)/F(\alpha_1)$ is a stem field of g. We continue the above process and find that the number of F-homomorphisms $F(\alpha_1, \alpha_2) \to K$ extending i_1 is at least 1, at most $[F(\alpha_1, \alpha_2) : F(\alpha_1)]$, and is exactly $[F(\alpha_1, \alpha_2) : F(\alpha_1)]$ if f has distinct roots.

Continuing this process for each α_i, we have that the number of F-homomorphisms $F(\alpha_1, \dots, \alpha_n) \to K$ is at least 1, at most $[E : F]$, and equal to $[E : F]$ if f has distinct roots. □

This result has the important corollary that any two splitting fields of f are isomorphic as fields.

Lemma 15.81. *Any two splitting fields of f are isomorphic.*

Proof. Let E/F and K/F be two splitting fields of f. f has finitely many roots, so E and K are finite extensions of F. We know that $[E : F] \leq [K : F]$ and $[K : F] \leq [E : F]$ by our lemma above, so $[E : F] = [K : F]$. We also know these exists a F-homomorphism $E \to K$. Since all field homomorphisms are injective and E, K have equal degree, it follows that this F-homomorphism is an F-isomorphism. □

Do observe that (usually) two splitting fields are not canonically isomorphic.

15.3 Algebraic Closure

A field K is ***algebraically closed*** if every polynomial $f \in K[x]$ splits in K. To show a field is algebraically closed, it is enough to show that every non-constant polynomial $f \in K[x]$ has a root in K (then you can just factor out roots).

For F a field, The ***algebraic closure*** of F is an algebraic extension K/F where K is algebraically closed.

As with the previous kinds of field extensions, it is important to check that these exist, and that they are unique up to isomorphism. These both are true, and we will prove the first statement today, and the second statement in the next lecture.

Lemma 15.82. *For any field F, there exists an algebraic closure.*

Proof. Let

$$S = \{f \in F[x] \mid f \text{ monic and irreducible}\}$$

For each $f \in S$, let K_f/F be a splitting field for f. Say $K_f = F(\alpha_{f,1}, \ldots, \alpha_{f,n(f)})$. Then we have a surjection

$$F[x_{f,1}, \ldots, x_{f,n(f)}] \to K_f$$

where $x_{f,i} \mapsto \alpha_{f,i}$. Let I_f be the kernel of this map. Let $R = F[x_{f,i}]_{f \in S, 1 \leq i \leq n(f)}$ be an infinite polynomial ring, and let $I \subset R$ be the ideal generated by all the I_f terms.

We now check that $I \neq (1)$. To check this, suppose it does. Then $1 = \sum_{i=1}^{n} a_i b_i$ for $a_i \in R < b_i \in I_{f_i}, f_1, \ldots, f_n \in S$. Let $g = f_1 f_2 \ldots f_n$, and let E/F be a splitting field of g. Let $R \to E$ be a F-homomorphism taking $x_{f,j}$ to the j^{th} root of f_i in E. The other x terms can be sent anywhere.

The map $R \to E$ takes $F[x_{f,1} \ldots, x_{f,n(f)}] \to K \to E$, and everything else anywhere else. This implies that each $b_i \to 0$, implying that $1 = 0$, a contradiction.

Since $I \neq (1)$, $\exists$ a maximal ideal M containing I. Consider $L = R/M$. This is a field extension of F, and is the algebraic closure of F. To see why, note that any polynomial over F splits in L. This is sufficient for L to be algebraically closed, by homework 8 problem 3. $\square$

Math 594: Algebra II **Winter 2019**

Lecture 16: March 21st

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

16.1 More on Algebraic Closure

Lemma 16.83. *Let F be a field, and let Ω/F be its algebraic closure. Let K/F denote an algebraic extension. Then $\exists$ an F-homomorphism $K \to \Omega$.*

Proof. First, suppose that $K = F(\alpha)$, and let f be the minimal polynomial for α in F. Since f factors into linear factors over Ω, it has at least 1 root in Ω. By Lemma 16.77, since the set of roots in Ω is nonempty, the set of F-homomorphisms from $K \to \Omega$ must be nonempty, so such a map must exist.

Now consider the case where $K = F(\alpha, \beta)$. We can think of this as a stem field over $F(\alpha)$. By the previous case, there exists an $F(\alpha)$ homomorphism $F(\alpha, \beta) \to \Omega$, which is just an F-homomorphism. Continuing this process, we know that if $K = F(\alpha_1, \alpha_2, \dots)$ for a countable number α_i, then there exists an F-homomorphism $K \to \Omega$. In general, consider the following set

$$S = \{(L/F, i) \mid F \subset L \subset K, i : L \to \Omega \text{ an } F\text{-homomorphism}\}$$

We define a partial order as follows. We say that $(L, i) \leq (L', i')$ if $L \subset L'$ and if $i'|_L = i$. By construction this is a well defined partial ordering. We need to show that any ascending chain is bounded. Well, If we have an ascending chain $L_1 \subset L_2 \subset \dots$, just let $L = \bigcup_j L_j$, and define i from the i_j's appropriately. It is clear that this is an upper bound.

Thus, by Zorn's Lemma, there exists a maximal element $(L, i) \in S$. I claim that $L = K$. This is because if not, $\exists \alpha \in K \backslash L$, and we have an L-homomorphism $j : L(\alpha) \to \Omega$, contradicting maximality, as $L(\alpha)$ is strictly larger than L and contained in S. □

If you're reading closely, you may be confused about how we're using L-homomorphism here. We only defined L-homomorphisms where L is a subfield of something. However, in general, if there exist field homomorphisms $L \to F, L \to K$, then an L-homomorphism is just a map which is compatible with them.

Lemma 16.84. *Suppose Ω is algebraically closed, and Ω'/Ω is an extension. then $\Omega = \Omega'$.*

Proof. Let $\alpha \in \Omega'$, and define f to be its minimal polynomial. Since Ω is algebraically closed, f splits over Ω. However, f is irreducible, so this implies that $\deg(f) = 1$. Thus, $f(x) = x - \alpha$, so $\alpha \in \Omega$. Thus we have that $\Omega' \subset \Omega$, and the result follows. □

We're now ready to prove that the algebraic closure of a field is unique up to isomorphism.

Lemma 16.85. *Let F be a field, and Ω, Ω' be two algebraic closures of F. Then, $\exists$ an F-isomorphism $\Omega \to \Omega'$. In fact, any F-homomorphism $\Omega \to \Omega'$ is an isomorphism.*

Proof. We already know there exists an (injective) F-homomorphism $i : \Omega \to \Omega'$. Observe that $F \subset i(\Omega) \subset \Omega'$, so $\Omega'/i(\Omega)$ is a field extension. By Lemma 17.84, it follows that $i(\Omega) = \Omega'$, so i is surjective, and thus an isomorphism. □

Algebraic closures on their own are fairly cumbersome, but their existence simplifies much of the "root-hunting" we've been doing thus far. As a sample application, let Ω/F be an algebraic closure, and take $f \in F[x]$. The splitting field of f is the subfield of Ω generated over F by the roots of f in Ω. In the case of $\mathbb{R}, \mathbb{C}$, this is clear. Take any polynomial over $\mathbb{R}$, factor it over $\mathbb{C}$, then adjoin those roots to $\mathbb{R}$. This will give you your splitting field, and is a much easier method of construction than the usual way of taking nested extensions and quotienting by maximal ideals repeatedly.

16.2 Irreducible Polynomials and Repeated Roots

Let $F = \mathbb{F}_p(t)$ (the rational functions over $\mathbb{F}_p$). Let $f(x) = x^p - t$. Recall that in characteristic p, $(x+y)^p = x^p + y^p$. Let $K = F(t^{1/p})$ be a stem field. Then $f(x)$ factors into $f(x) = (x - t^{1/p})^p$. So f is irreducible, but all of its factors are the same! Why is it irreducible? Well, Suppose that $g|f$. Then $g(x) = (x - t^{1/p})^k$ for some $k < p$. But this is a contradiction, as the constant term, $t^{k/p}$ is not in F.

We see two things here. First, is that raising to the p^{th} power in $\mathbb{F}_p$ can bring about some interesting results. In fact, the map $x \mapsto x^p$ is a field homomorphism over characteristic p fields, and is called the ***Frobenius map***. Second, is that irreducible polynomials over a finite field can have a repeated root. This generalizes into a nice theorem:

Theorem 16.86. *let F be a field, and let $f \in F[x]$ be an irreducible polynomial. Then the following are equivalent:*

(a) f has a repeated root it its splitting field.

(b) $\gcd(f, f') \neq 1$.

(c) F is characteristic p, and $f(x) = g(x^p)$ for some g.

(d) Every root of f is repeated.

Before proving this theorem, we first define what f' means in this context (It is what you think it is) and prove a small preceding lemma. f' is the ***derivative*** of the polynomial f, defined in the usual way. $f' = \frac{d}{dx} f$, where

$$\frac{d}{dx}\left(\sum_{i=1}^{d} a_i x^i\right) = \sum_{i=1}^{d} i a_i x^{i-1}$$

$$\frac{d}{dx}(\alpha f + \beta g) = \alpha \frac{d}{dx} f + \beta \frac{d}{dx} g$$
$$\frac{d}{dx}(fg) = f\frac{dg}{dx} + \frac{df}{dx} g$$

Note that if F is characteristic p, then

$$\frac{d}{dx} x^{kp} = \frac{d}{dx} g(x^p) = 0$$

Now we prove a simple but useful lemma:

Lemma 16.87. *Let K/F be an extension of F, and let $f, g \in F[x]$. Then,*

$$\gcd_{F[x]}(f, g) = \gcd_{K[x]}(f, g)$$

Proof. Let $h = \gcd_{F[x]}(f, g), h' = \gcd_{K[x]}(f, g)$. $h|f, g \in K[x]$, so $h|h'$ in $K[x]$. We also know that $\exists a, b \in F[x]$ such that $af + bg = h$. $h'|af, h'|bg \Rightarrow h'|h$. Thus, $h' = h$, and we conclude. □

We now prove the theorem above.

Proof. $(d) \Rightarrow (a)$ is trivial, so it suffices to show that $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d)$. First we show that $(a) \Rightarrow (b)$. Let K/F be an extension in which f has a repeated root α. Then $f(x) = g(x)(x - \alpha)^n$, and

$$\frac{df}{dx} = g'(x)(x - \alpha)^n + ng(x)(x - \alpha)^{n-1}$$

So $x - \alpha | f'$ and $x - \alpha | f$, implying that $\gcd_{K[x]}(f, f') \neq 1$, so $\gcd_{F[x]}(f, f') \neq 1$ by Lemma 17.87. We next check $(b) \Rightarrow (c)$. Note f is irreducible, and $\deg(f') < \deg(f)$. Thus f', f cannot have a common factor. But, $\gcd(f, f') \neq 1$, so $f' = 0$. This immediately implies that F has characteristic p. Furthermore, it implies that $f(x) = \sum a_i x^i$ where $a_i = 0$ unless $p|i$. This immediately implies that $f(x) = g(x^p)$ for some g.

Finally we check $(c) \Rightarrow (d)$. Suppose that we are working within characteristic p, and $f(x) = g(x^p)$ for some g. We work in the algebraic closure of F, denoted Ω. Here every polynomial splits, so

$$g(x) = \prod_{i=1}^{d} (x - \alpha_i)$$

And

$$f(x) = \prod_{i=1}^{d} (x^p - \alpha_i) = \prod_{i=1}^{d} (x - \beta_i)^p$$

For β_i the p^{th} root of α_i. It follows then that all roots of f are repeated. □

16.3 Perfect and Separable Fields

We use the concept of repeated roots to formulate some new types of fields.

- An irreducible polynomial is ***separable*** if it does not have repeated roots in its splitting field.
- An algebraic element $x \in K/F$ is separable if its minimal polynomial is separable.
- An algebraic extension K/F is separable if all $x \in K/F$ are separable.
- A field F is called ***perfect*** if all finite extensions are separable.

Lemma 16.88. *Let F be a field. If F has characteristic 0, it is perfect. If F is characteristic p, then F is perfect $\iff$ all elements of F are p^{th} powers.*

Proof. If F is characteristic 0, then it is clear that all irreducible polynomials over F are separable, so we move on to the case where F is characteristic p. Suppose all elements are p^{th} powers. Consider K/F a finite extension, and let $x \in K$. Now take f to be the minimal polynomial of x. If f is not separable, then $f(x) = g(x^p)$ for some $g \in F[x]$, by Theorem 17.86. then $g(x) = \sum_{i=0}^{d} a_i x^i$ for some $a_i \in F$. By hypothesis, we can write $a_i = b_i^p$. Thus, we have that

$$g(x^p) = \sum_{i=0}^{d} a_i x^{pi} = \sum_{i=0}^{d} b_i^p (x^i)^p = \left(\sum_{i=0}^{d} b_i x^i \right)^p = f(x)$$

So f can be factored, but it is irreducible? This is a contradiction.

We now tackle the other direction. Suppose that F contains an element that is not a p^{th} power, called α. Then $F(\alpha^{1/p})$ is an inseparable extension of F, so F is not perfect, a contradiction. □

We've shown that characteristic 0 fields are all perfect. It turns out that the same result holds for any finite field.

Lemma 16.89. *Every finite field is perfect.*

Proof. Say F is a finite field of characteristic p. Consider $\varphi : x \mapsto x^p$ the Frobenius map. φ is a field homomorphism, so it is injective. Since the domain and target are both F, it is an isomorphism. This implies that all elements are p^{th} powers, so we can conclude that F is perfect by the previous Lemma. □

Math 594: Algebra II **Winter 2019**

Lecture 17: March 26th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

17.1 Transcendental Extensions

We conclude our study of Fields by discussing transcendental extensions. When studying such extensions, it may be useful to consider the analogy between transcendental extensions and linear algebra. As you'll soon see, many of the theories of transcendental extensions are very similar to ones you have seen before in Linear Algebra. We introduce a notion of algebraic independence and span (analogous to linear independence and span), then use those to construct transcendence bases (analogous to bases of vector spaces) and define a transcendence degree (analogous to the dimension of a vector space).

17.1.1 Algebraic Independence

Let Ω/F denote a field extension, and take $A \subset \Omega$. We say that A is ***Algebraically Dependent*** if there exists distinct elements $a_1, \ldots, a_n \in A$ and a nonzero polynomial $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$. If A is not algebraically dependent, we say that A is ***Algebraically Independent***.

Lemma 17.90. *For $a_1, \ldots, a_n \in \Omega$, Let $F[a_1, \ldots, a_n]$ be a subring of Ω. Then, the following are equivalent:*

(1) $\{a_1, \ldots, a_n\}$ is algebraically independent.

(2) The F-homomorphism $\varphi : F[x_1, \ldots, x_n] \to \Omega$ which maps $x_i \to a_i$ is an isomorphism onto $F[x_1, \ldots, x_n]$

Proof. Note that $f \in \ker(\varphi)$ if and only if $f(a_1, \ldots, a_n) = 0$. Thus, $\ker(\varphi) \neq 0 \iff$ $a_1, \ldots, a_n$ are algebraically dependent. □

If there exists an isomorphism from $F[x_1, \ldots, x_n] \to F[a_1, \ldots, a_n]$, then by localizing we have an isomorphism $F(x_1, \ldots, x_n) \to F(a_1, \ldots, a_n) \subset \Omega$, which is a field extension of F. An extension of this form is called a ***Purely Transcendental Extension***.

17.1.2 Algebraic Span

For $A \subset \Omega$, the ***Algebraic Span*** is the set of all elements of Ω that are algebraic over $F(A) \subset \Omega$ (F with all elements of A adjoined). A ***Algebraically Spans*** (or is an ***Algebraic Spanning Set***) if $F(A) = \Omega$.

17.1.3 Transcendence Bases

We define a ***Transcendence Basis*** to be a set $A \subset \Omega$ such that A is algebraically independent and A spans. As one might expect, we have the following equivalence.

Theorem 17.91. *For $A \subset \Omega$, the following are equivalent.*

(1) A is a transcendence basis.

(2) A is a minimal algebraic spanning set.

(3) A is a maximal algebraically independent set.

Proof. First we check that (1) $\Rightarrow$ (2). Fix A a transcendence basis. By definition, A algebraically spans. We need to show that no proper subset of A algebraically spans. We proceed by contradiction; suppose a set B does, and take $x \in A \backslash B$. Because B is an algebraically spanning set, x is algebraic over B. Thus, $\exists c_i \in F(B)$ such that

$$x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0$$

There exists $b_1, \ldots, b_m \in B$ such that for each c_i

$$c_i = \frac{g_i(b_1, \ldots, b_m)}{h_i(b_1, \ldots, b_m)}$$

Clearing denominators, we have that

$$x^n + c'_{n-1}x^{n-1} + \cdots + c'_0 = 0$$

for $c'_i = f_i(b_1, \ldots, b_m)$. But then, we define

$$f(x_1, \ldots, x_m, X) := f'_n(x_1, \ldots, x_m)X^n + f'_0(x_1, \ldots, x_m)$$

Observe that $f(b_1, \ldots, b_m, x) = 0$, but $b_1, \ldots, b_m, x \in A$, implying that A is algebraically dependent, a contradiction.

We now prove (2) $\Rightarrow$ (1). A is a minimal spanning set; we check that A is a basis. It is sufficient to show that A is algebraically independent. We proceed by contradiction, and suppose not, taking $\{a_1, \ldots, a_n\}$ as the minimal algebraically dependent subset of A.

We claim that a_n is algebraic over $F(a_1, \ldots, a_{n-1})$. Choose $f \in F[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$ (this exists by hypothesis). Note that

$$f(x_1, \ldots, x_{n-1}, Y) = \sum_{i=0}^{d} g_i(x_1, \ldots, x_{n-1}) Y^i$$

where all g_i are not zero. Note that

$$0 = f(a_1, \ldots, a_n) = \sum_{i=1}^{d} g_i(a_1, \ldots, a_{n-1}) a_n^i$$

Every $g_i(a_1, \ldots, a_{n-1})$ is not zero, by minimality of $a_1, \ldots, a_n$. Now take $B = A \backslash \{a_n\}$. $F(B)/F$ is an algebraic extension by construction, and $F(A)/F(B)$ is an algebraic extension by our claim. Finally, $\Omega/F(A)$ is algebraic because A algebraically spans. This implies that Ω is an algebraic extension of $F(B)$, implying B is an algebraic spanning set, contradicting the minimality of A.

Next we show (1) $\Rightarrow$ (3). Take A a transcendence basis. This implies that A is algebraically independent; we must show that A is the maximal such set. Let $b \in \Omega \backslash A$, and let $B = A \cup \{b\}$. It is sufficient to show that B is algebraically dependent.

Well, A is algebraically spanning, so $\Omega = F(A)$. Thus, $\exists c_i \in F(A)$ such that $\sum_{i=1}^{d} c_i b^i = 0$. By clearing denominators as in the first case, this proves that b is algebraically independent.

We conclude by showing that (3) $\rightarrow$ (1). Let A be a maximal algebraically independent set; we want to show that A spans. Well, suppose not, then $\Omega/F(A)$ is not an algebraic extension. Let $b \in \Omega$ be transcendental over $F(A)$. Then, $A \cup \{b\}$ is algebraically independent, a contradiction. □

As in the linear algebra case, we have the following result about transcendental bases.

Theorem 17.92. *Transcendental bases always exist.*

The proof is an easy application of Zorn's Lemma.

17.1.4 An Exchange Lemma

Recall that in linear algebra, the Steinitz Exchange Lemma allows you to extend the basis of a vector subspace to a basis of the whole space. A similar result holds for transcendence bases and field extensions.

Lemma 17.93. *(Exchange Lemma)Let Ω/F be a field extension, and $a_1, \ldots, a_k \in \Omega$. Let $b \in \text{span}(a_1, \ldots, a_k)$, but $b \notin \text{span}(a_1, \ldots, a_{k-1})$. Then, $a_k \in \text{span}(a_1, \ldots, a_{n-1}, b)$*

Proof. b is algebraic over $F(a_1, \ldots, a_k)$, implying that there exists $c_i \in F(a_1, \ldots, a_k)$ such that

$$c_d(a_1, \ldots, a_k) b^d + \cdots + c_0(a_1, \ldots, a_k) = 0$$

Consider

$$f(x_1, \ldots, x_k, Y) := c_d(x_1, \ldots, x_k)Y^d + \cdots + c_0(x_1, \ldots, x_k) \in F[x_1, \ldots, x_k, Y]$$

b satisfies $f(a_1, \ldots, a_k, Y)$, and a_k satisfies $f(a_1, \ldots, a_{n-1}, x_k, b)$. This polynomial is nonzero because $b \notin \text{span}(a_1, \ldots, a_{n-1})$, which then shows that $a_k \in \text{span}(a_1, \ldots, a_{n-1}, b)$ as intended. □

Lemma 17.94. *Given $a_1, \ldots, a_n, b_1, \ldots, b_m \in \Omega$ such that $\{a_1, \ldots, a_n\}$ is algebraically independent and $a_i \in \text{span}(b_1, \ldots, b_m)$, then $n \leq m$.*

Proof. Let k be maximal such that $a_1, \ldots, a_k \in \{b_1, \ldots, b_n\}$. let these be denoted $b_1, \ldots, b_k$. Thus, we have that

$$a_k \in \text{span}(a_1, \ldots, a_k, b_{k+1}, b_j)$$

for $j \leq m$ minimal. Then, $a_{k+1} \notin \text{span}(a_1, \ldots, a_k, b_{k+1}, \ldots, b_{j-1})$. By the exchange lemma, $b_j \in \text{span}(a_1, \ldots, a_{k+1}, b_{k+1}, \ldots, b_{j-1})$, implying that

$$\text{span}(b_1, \ldots, b_m) = \text{span}(a_1, \ldots, a_{k+1}, b_{k+1}, \ldots, \overline{b_j}, \ldots, b_m)$$

where $\overline{b_j}$ denotes omission. We continue this process, until $k = n$, and $k \leq m$ by construction. □

17.1.5 Transcendence Degree

This lemma quickly implies the following theorem:

Theorem 17.95. *All finite transcendence bases of a given extension have the same cardinality.*

This gives rise to a notion of "dimension" for transcendental extensions. The ***Transcendence Degree*** of Ω/F, denoted $\text{trdeg}(\Omega/F)$, is the size of the extension's transcendence bases.

17.1.5.1 Examples:

- Take $\Omega = F(x_1, \ldots, x_n)$. $x_1, \ldots, x_n$ forms a transcendence basis, so $\text{trdeg}(\Omega/F) = n$.
- Let $f(x, y) \in F(x, y)$ be some irreducible polynomial. Then, $R = F[x, y]/(f)$ is a domain. Let Ω be the field of fractions of R, which is an extension of R. $\{x\}$ and $\{y\}$ are both transcendental bases of Ω, so $\text{trdeg}(\Omega/F) = 1$.

As one might expect, for algebraically closed extensions, we have the following result.

Lemma 17.96. *Two algebraically closed extensions are isomorphic if and only if they have the same transcendence degree.*

Math 594: Algebra II **Winter 2019**

Lecture 18: March 28th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

18.1 An Introduction to Galois Theory

We now proceed to the 4th and final part of the course, covering Galois theory and its applications. We first prove the main theorem of Galois theory, relating intermediate extensions to subgroups of a field's automorphism group, then use this to prove the unsolvability of the quintic.

18.1.1 Galois Groups

For E a field, an ***automorphism*** of E is a field isomorphism $E \to E$. The set of all these form a group, called the ***automorphism group*** of E, denoted $\mathrm{Aut}(E)$. If E is a field extension of the form E/F, an F***-automorphism*** of E is an automorphism on E that is the identity on F. The set of these automorphisms is called the ***Galois Group*** of E/F and is denoted as $\mathrm{Gal}(E/F)$ or $\mathrm{Aut}(E/F)$ dependent on context.

18.1.1.1 Examples:

- If E is of characteristic p, then the Frobenius map $x \mapsto x^p$ is a field homomorphism. It is an automorphism if and only if E is perfect.
- For $E = \mathbb{C}$, $\tau : E \to E$ defined by $a + ib \mapsto a - ib$ (the conjugation map) is a field automorphism which fixes $\mathbb{R}$. τ clearly has order 2. In fact, we have that $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \tau\} \cong \mathbb{Z}/2\mathbb{Z}$, a fact which clearly follows from the fact that $1, i$ generate $\mathbb{C}$ over $\mathbb{R}$.
- $\mathrm{Aut}(\mathbb{Q})$ is trivial.
- $\mathrm{Aut}(\mathbb{F}_p)$ is also trivial.
- $\mathrm{Aut}(\mathbb{R})$ is also trivial, since $\mathrm{Aut}(\mathbb{Q})$ is trivial, and automorphisms preserve order, and $\mathbb{Q}$ is dense in $\mathbb{R}$.
- Consider $\tau : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ which takes $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ (calling this τ was intentional). This is an automorphism, and by similar logic to $\mathbb{C}/\mathbb{R}$, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \tau\} \cong \mathbb{Z}/2\mathbb{Z}$.
- $\mathrm{Aut}(\mathbb{C})$ is very big! Let x_i denote a transcendental basis for $\mathbb{C}/\mathbb{Q}$ for $i \in I$ some indexing set. We have that $\mathbb{C} \cong \overline{\mathbb{Q}(x_i)_{i \in I}}$.

- Let F be a field. We want to see the structure of $\mathrm{Gal}(F(x)/F)$. In general, any F-homomorphism has the form $f(x) \mapsto f(g(x))$. This means that maps like $f(x) \mapsto f(ax+b)$ (for $a \neq 0$) define a field automorphism. In general, $f(x) \mapsto f\left(\frac{ax+b}{cx+d}\right)$. These are fractional linear transformations (which you may have seen in a complex analysis course, and are very widely known. For example, any fractional linear transformation can be taken as a matrix $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ where $\det(A) \neq 0$ (i.e. the matrix is invertible). From here, we find that
$$\mathrm{Gal}(F(x)/F) \cong \mathrm{PGL}_2(F)$$
where $\mathrm{PGL}_2(F) := \mathrm{GL}_2(F)/F^\times$ for $F^\times$ the diagonal scalars of the identity matrix.

- In a similar fashion we can compute $\mathrm{Gal}(F(x,y)/F)$. This is denoted the ***Cremona Group***.

- Let $F = \mathbb{Q}(\sqrt[3]{2})$. What does $\mathrm{Gal}(F/\mathbb{Q})$ look like? Well, $\sqrt[3]{2}$ is the root of $x^3 - 2$, with roots $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$ for ζ the 3rd root of unity. Automorphisms send roots to roots, but only 1 root of the polynomial is in F, Thus, Automorphisms fix 1 and $\sqrt[3]{2}$, but these generate F. Thus, $\mathrm{Aut}(F/\mathbb{Q})$ is trivial.

- Let $F = \mathbb{F}_p(T)$, and $E = \mathbb{F}_p(T^{1/p})$. We have the minimal polynomial $X^p - T = 0$, which factors modulo p as $(X - T^{1/p})^p = 0$, and has p identical roots. Since automorphisms permute roots, and all the roots are the same, all permutations are trivial, so all automorphisms are trivial. Thus, $\mathrm{Gal}(E/F)$ is trivial.

18.1.2 Galois Extensions

Lemma 18.97. *Suppose E/F is the splitting field of a separable polynomial. Then, $\#\mathrm{Gal}(E/F) = [E : F]$.*

Proof. By an earlier proposition, we know that the number of F-homomorphisms $E \to E$ is exactly $[E : F]$. Field homomorphisms are always injective, and any F-homomorphism $E \to E$ is an isomorphism because it is an injection onto a finite dimensional F-vector space of same dimension. □

As an example, consider $E = \mathbb{Q}(\zeta, \sqrt[3]{2})$, the splitting field of $X^3 - 2$. We know that $[E : \mathbb{Q}] = 6$, so via the proposition, $\mathrm{Gal}(E/Q)$ has order 6. Any automorphism permutes 3 roots, so it is a subset of S_3. Since $\mathrm{Gal}(E/\mathbb{Q})$ has order 6, it follows that $\mathrm{Gal}(E/\mathbb{Q}) = S_3$.

In general, if a splitting field E/F of a polynomial f has degree $(\deg(f))!$, then $\mathrm{Gal}(E/F) \cong S_{\deg(f)}$.

Let E/F be a finite extension. We say that E/F is ***normal*** if it is the splitting field of some polynomial. E/F is a ***Galois Extension*** if it is normal and separable. Galois Extensions have a remarkable structure, that we will discuss for the remainder of the term. First and foremost, we have a theorem relating intermediate extensions of Galois Extensions to subgroups of its Galois group.

18.2 The Fundamental Theorem of Galois Theory

Theorem 18.98. *Let E/F be a Galois Extension, and set $G = \mathrm{Gal}(E/F)$. Then, the set of intermediate fields between F and E are in bijection with the subgroups of G. Moreover, this bijection is explicit. $\Phi : H \mapsto E^H$, or the fixed field under the action of H (via automorphism evaluation) on E. $\Psi : K \mapsto \mathrm{Gal}(E/K)$, and these maps are each others inverses.*

This bijection is order reversing with respect to inclusion. That is, For $H, H' \subset G$, $H \subset H' \iff \Phi(H') \subset \Phi(H)$.

In addition, For K an intermediate extension, K/F is Galois if and only if $\Phi(K) = \mathrm{Gal}(E/K)$ is a normal subgroup of G. In this case, $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$.

We prove this theorem in the next lecture. As a toy example of its application, we consider $E = \mathbb{Q}(\zeta, \sqrt[3]{2})$ from before. Subfields of E corresponds with subgroups of S_3 in the following way:

$$\begin{aligned} E &\longleftrightarrow 1 \\ \mathbb{Q}(\zeta^2\sqrt[3]{2}) &\longleftrightarrow \langle (1\ 2) \rangle \\ \mathbb{Q}(\zeta\sqrt[3]{2}) &\longleftrightarrow \langle (1\ 3) \rangle \\ \mathbb{Q}(\sqrt[3]{2}) &\longleftrightarrow \langle (2\ 3) \rangle \\ \mathbb{Q}(\zeta) &\longleftrightarrow A_3 \\ \mathbb{Q} &\longleftrightarrow S_3 \end{aligned}$$

Math 594: Algebra II **Winter 2019**

Lecture 19: April 2nd

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

19.1 Basic results about Galois Extensions

Lemma 19.99. *Let E be a field, and G a finite subgroup of $\mathrm{Aut}(E)$. Then, $[E : E^G] = \#G$ and $G = \mathrm{Aut}(E/E^G)$.*

Proof. Let $n = \#G$, and $G = \{\sigma_1, \ldots, \sigma_n\}$. Say $\alpha_1, \ldots, \alpha_m \in E$, and $m > n$. We want to show that $\alpha_1, \ldots, \alpha_m$ are linearly dependent over E^G. Well, set

$$\sigma_i(\alpha_1)X_1 + \cdots + \sigma_i(\alpha_m)X_m = 0$$

There are n equations and m unknowns, with $m > n$. Thus, $\exists$ a nonzero solution $(c_1, \ldots, c_m) \in E^G$. Choose this vector such that it has the maximum number of zeroes; we then normalize so that $c_1 = 1$.

We claim that $c_i \in E^G$ for all i. To see why, choose $\tau \in G$. Then,

$$(\tau\sigma_i\alpha_1)(\tau c_1) + \cdots + (\tau\sigma_i\alpha_m)(\tau c_m) = 0$$

But τ just permutes the terms when applied to the σ_i terms, implying that

$$(\sigma_i\alpha_1)(\tau c_1) + \cdots + (\sigma_i\alpha_m)(\tau c_m) = 0$$

So $(\tau c_1 \ldots, \tau c_m)$ is a solution, so $(\tau c_1 - c_1, \ldots, \tau c_m - c_m)$ is a solution. Well, this will have more zeroes $(c_1, \ldots, c_m)$, so they all must be zero by construction. Thus, $\tau c_i = c_i \; \forall i$, for any $\tau \in G$, so c_i is fixed by G, and $c_i \in E^G$.

This shows that $[E : E^G] \leq G$. Well, $G \subset \mathrm{Aut}(E/E^G) \Rightarrow \#G \leq \#\mathrm{Aut}(E/E^G)$. This implies that $[E : E^G] = G$, which implies that $G = \mathrm{Aut}(E/E^G)$ immediately. □

Lemma 19.100. *Let E/F be a field extension. Then, the following are equivalent:*

(1) E is a splitting field of a separable polynomial over $F[T]$.

(2) F is the fixed field of the Galois Group (i.e. $F = E^{\mathrm{Gal}(E/F)}$) and $[E : F] < \infty$.

(3) $F = E^G$ for some finite $G \subset \mathrm{Gal}(E/F)$.

(4) E/F is a Galois Extension.

Proof. First we show (1) $\Rightarrow$ (2). (1) immediately implies that $[E : F] < \infty$, and by the previous lemma,

$$[E : E^{\mathrm{Gal}(E/F)}]\#\mathrm{Gal}(E/E^{\mathrm{Gal}(E/F)}) = \#\mathrm{Gal}(E/F) = [E : F]$$

Since $F \subset E^{\mathrm{Gal}(E/F)}$, by a simple degree argument we have that $F = E^{\mathrm{Gal}(E/F)}$.

(2) $\Rightarrow$ (3) is obvious (just take $G = \mathrm{Gal}(E/F)$) so we proceed to proving (3) $\Rightarrow$ (4). By the previous lemma, we know that E/F is a finite extension, so it is sufficient to show that it is normal and separable. Let $\{\alpha_1, \ldots, \alpha_n\}$ be orbit for some $\alpha \in E$ under G. Consider $f(T) = \prod(x - \alpha_i)$. For $\sigma \in G$, Let $\sigma f(T)$ denote the polynomial obtained by applying σ to each α_i. In other words,

$$\sigma f(T) = \prod(T - \sigma\alpha_i)$$

This just permutes the roots, so it is clear that $\sigma f(T) = f(T)$, and the coefficients of $f(T)$ are fixed by G, so the coefficients of f are in $E^G = F$.

Observe that $f(T)$ is the minimal polynomial of $\alpha \in F$. If it wasn't, and a polynomial $h(T)$ was, then h divides f. Well, then the roots of h are a subset of the roots of f, but G acts transitively on $\{\alpha_1, \ldots, \alpha_n\}$, so each α_i needs to be a root of h, so $h = f$, a contradiction. Thus, each $\alpha \in E$ is separable, implying that E/F is a separable extension. Normality also follows, so E/F is a Galois Extension.

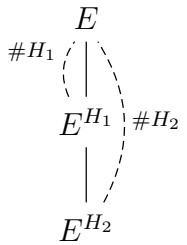
To conclude we prove (4) $\Rightarrow$ (1). Since E/F is normal, we know that it is the splitting field of some polynomial f over $F[T]$. Let f' denote the polynomial with the same roots as f, but no repeated roots. It follows from the separability of E that E is still the splitting field of f'. □

19.2 Proof of the Fundamental Theorem of Galois Theory

We use the tools from above to prove the main theorem.

Proof. First, take an intermediate extension $F \subset K \subset E$. We claim that E/K is Galois. To show this, Choose $f \in F[T]$ such that E is the splitting field for f (which we can do by the previous result. $f \in K[T]$ as well, and is still separable, implying that E/K is Galois by the previous result, and that $E = E^{\mathrm{Gal}(E/K)}$, the latter of which actually shows that the correspondence defined is in fact a bijective correspondence.

We now show that the bijection is order reversing with respect to inclusion. Choose $H_1 \subset H_2 \subset G$. We want to show that $[H_2 : H_1] = [E^{H_1} : E^{H_2}]$. If H_1 is trivial, then this statement resolves to showing $H_2 = [E : E^{H_2}]$, which was already proved. When H_1 is not trivial, we have the following tower of extensions:



Thus, the degree of E^{H_1}/E^{H_2} must be $[H_2 : H_1]$.

It's also important to show that this correspondence is G-equivariant. To show this, let $K = E^H$. We want to show that $\sigma K = E^{\sigma H \sigma^{-1}}$. Choose $x \in K$, $\tau \in H$. $(\sigma\tau\sigma^{-1})(\sigma x) = \sigma(x)$, implying that $\sigma(x) \in E^{\sigma H \sigma^{-1}}$, implying that $\sigma K \subset E^{\sigma H \sigma^{-1}}$. $\sigma K, E^{\sigma H \sigma^{-1}}$ have the same degree, so $\sigma K = E^{\sigma H \sigma^{-1}}$ as desired.

Finally, we show that K/F is a Galois extension if and only if its corresponding subgroup H is normal in G. In this case, $\mathrm{Gal}(K/F) \cong G/H$.

$$
\begin{aligned}
&K/F \text{ is Galois} \\
&\Rightarrow K/F \text{ the splitting field of some } f \in F[T] \\
&\Rightarrow \text{Every } \sigma \in G \text{ permutes the roots of } f \\
&\Rightarrow \text{every } \sigma \text{ maps } K \text{ to itself} \\
&\Rightarrow \sigma K = K \\
&\Rightarrow K = \sigma K = E^{\sigma H \sigma^{-1}} \\
&\Rightarrow H = \sigma H \sigma^{-1} \\
&\Rightarrow H \text{ is normal}
\end{aligned}
$$

Conversely,

$$
\begin{aligned}
&H \text{ is normal} \\
&\Rightarrow G/H \text{ acts on } K = E^H \\
&\Rightarrow (E^H)^{G/H} = E^G = F \\
&\Rightarrow K^{G/H} = F \\
&\Rightarrow K/F \text{ is Galois with group } G/H
\end{aligned}
$$

This completes the proof. □

Be warned! If E/F is a Galois extension, and $F \subset K \subset E$ is an intermediate extension, then E/K is ALWAYS Galois, but K/F is ONLY galois if H, the subgroup corresponding to K under the correspondence above, is normal.

Math 594: Algebra II **Winter 2019**

Lecture 20: April 4th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

20.1 Solving Equations by Radicals

One of the most well known (simple) applications of Galois Theory is proving the unsolvability of the quintic.

Any high school student knows that for any polynomial of the form $ax^2 + bx + c = 0$, one can solve for x in terms of a, b, c. Namely,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

In the 16th century, mathematicians proved that there is a formula for cubic expressions as well. Not long after, a quartic formula was found. It was not until the 19th century, via the Abel-Ruffini Theorem, that mathematicians proved that no quintic formula exists.

The underlying question is, for a polynomial f, can we find roots of f using only radicals and basic arithmetic operations?

Fix a base field F, characteristic 0. Let $f \in F[T]$, with splitting field K. We say that f is ***Solvable by Radicals*** if there exists a tower of fields

$$\begin{array}{c} K \subset F_n \\ | \\ F_{n-1} \\ | \\ \vdots \\ | \\ F_1 \\ | \\ F = F_0 \end{array}$$

Such that $F_i = F_{i-1}(a_i^{1/d_i})$ for some $d_i \geq 1$, $a_i \in F_{i-1}$. Essentially, each successive extension just adds some radical or root. It is easy to see how having a closed form solution to a polynomial equation in terms of radicals and basic arithmetic operations is analogous to this.

Let $\mathrm{Gal}(K/F)$ denote the Galois group of f (note: A Galois group of a function is just the Galois group of the splitting field. It is often denoted $\mathrm{Gal}(f)$). Furthermore, adjectives used to describe a Galois group can be used to describe its corresponding extension. For example, if an extension has cyclic Galois group, we say that it is a ***cyclic extension***. Similar definitions hold for solvable and abelian extensions.

We first check the following proposition:

Proposition 20.101. *Given $a \in F$, $F(a^{1/n})$ is a Galois Extension, and the Galois group is cyclic with order dividing n.*

Proof. We prove this in the case where F contains a primitive nth root of unity, for some fixed n. Let $\zeta_n \in F$ denote the nth root of unity, and let $\mu_n \subset F$ denote the set of all nth roots of unity. Note that $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$. Thus, μ_n is a subgroup of order n, suggesting that n divides the order of $\mathrm{Gal}(F(a^{1/n})/F)$. □

For any $a \in F$, we can then conclude that $F(a^{1/n})$ is the splitting field of $T^n - a$, and is thus a Galois extension. This is because we've supposed that $\zeta_n \in F$, and roots of $T^n - a$ are of the form $\zeta_n^k \cdot a^{1/n}$ for $0 \leq k < n$.

Given $\sigma \in \mathrm{Gal}(F(a^{1/n})/F)$, we can define a function $f : \mathrm{Gal}(F(a^{1/n})/F) \to \mu_n$ such that $\sigma(a^{1/n}) = f(\sigma)a^{1/n}$ (this construction is well defined as σ fixes F), and field automorphisms map roots to roots). f is in fact a group homomorphism, as shown below:

$$f(\sigma\tau)a^{1/n} = (\sigma \circ \tau)(a^{1/n}) = \sigma(\tau(a^{1/n})) = \sigma(f(\tau)a^{1/n}) = f(\tau)\sigma(a^{1/n}) = f(\tau)f(\sigma)a^{1/n}$$

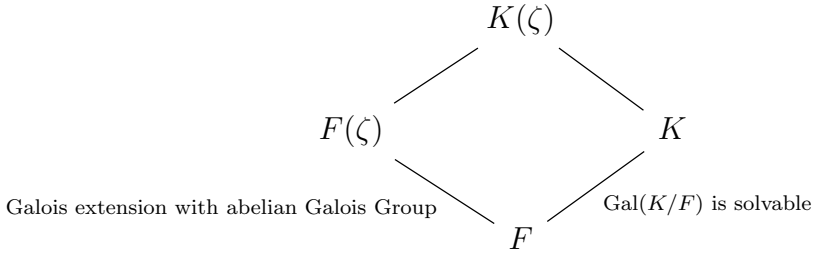
Suggesting that $f(\sigma\tau) = f(\tau)f(\sigma)$. As $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ is abelian, the result follows. f is also clearly injective, as if $\sigma \in \ker(f)$, then $\sigma(a^{1/n}) = f(\sigma)a^{1/n} = a^{1/n}$, so $\sigma = \mathrm{Id}$.

What does this suggest? Well suppose K/F is some Galois extension and $\mathrm{Gal}(K/F) \cong \mathbb{Z}/n\mathbb{Z}$. f is thus an injective morphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, so it is an isomorphism. In particular, we can use f to construct $a \in F$ such that $K = F(a^{1/n})$.

We now prove the main theorem, checking the reverse case first.

Theorem 20.102. *f is solvable by radicals $\iff$ $\mathrm{Gal}(f)$ is a solvable group.*

Proof. (Reverse case) Let K denote the splitting field of F, and suppose that $\mathrm{Gal}(K/F)$ is solvable. Suppose that $d = \deg(f)$ and ζ is a primitive $d!$ root of unity. We get the following field extensions:



From the Proposition 22.101, we know that $\mathrm{Gal}(F(\zeta)/F)$ is cyclic with order dividing n (and in particular, a Galois extension), suggesting that it is the splitting field of some $g \in k[T]$. Thus, $K(\zeta)$ is the splitting field of fg from the tower above, suggesting that $K(\zeta)/F$ is a Galois extension. The Fundamental Theorem of Galois Theory gives us homomorphisms

$$\mathrm{Gal}(K(\zeta)/F) \to \mathrm{Gal}(K/F)$$
$$\mathrm{Gal}(K(\zeta)/F) \to \mathrm{Gal}(F(\zeta)/F)$$

Using the universal property of products, these maps lift to a morphism

$$i : \mathrm{Gal}(K(\zeta)/F) \to \mathrm{Gal}(K/F) \times \mathrm{Gal}(F(\zeta)/F)$$

With the image being the product of the images of the above two induced morphisms. i is, as the name suggests, injective, as if $i(\sigma) = 1$, then σ fixes K and $F(\zeta)$. As these generate $K(\zeta)$, it follows that σ fixes $K(\zeta)$, and is thus the identity map, suggesting that $\ker(i) = \{\mathrm{Id}\}$, and i is injective. Thus, we have an inclusion

$$\mathrm{Gal}(K(\zeta)/F) \hookrightarrow \mathrm{Gal}(K/F) \times \mathrm{Gal}(F(\zeta)/F)$$

$\mathrm{Gal}(K/F)$ is solvable, and $\mathrm{Gal}(F(\zeta)/F)$ is abelian, and the product of an abelian group and solvable group is solvable. As $\mathrm{Gal}(K(\zeta)/F) \cong \mathrm{im}(i)$ for $\mathrm{im}(i)$ a subgroup of a solvable group, we can conclude that $\mathrm{Gal}(K(\zeta)/F)$ is indeed solvable, suggesting that $\mathrm{Gal}(K(\zeta)/F(\zeta))$ is solvable, as it is a subgroup of $\mathrm{Gal}(K(\zeta)/F)$.

Take a composition series $1 = G_1 \subset \ldots \subset G_n = \mathrm{Gal}(K(\zeta)/F(\zeta))$ and let $E_i = K(\zeta)^{G_i}$. We get the tower of extensions

$$\begin{array}{c} E_1 = K(\zeta) \\ | \\ \vdots \\ | \\ E_{n-2} \\ | \ \mathrm{Gal}(E_{n-2}/E_{n-1}) = G_{n-1}/G_{n-2} \\ E_{n-1} \\ | \ \mathrm{Gal}(E_{n-1}/F(\zeta)) = G_n/G_{n-1} \\ E_n = F(\zeta) \\ | \\ F \end{array}$$

Observe that $\mathrm{Gal}(k(\zeta)/E_i) = G_i \supset G_{i-1} = \mathrm{Gal}(K(\zeta)/E_{i-1})$. Furthermore, we know that G_i/G_{i-1} is cyclic, so each of these extensions are cyclic. From the result immediately succeeding Proposition 22.101, we know that cyclic extensions E_{i-1}/E_i can be written as $E_i(a^{1/d_i}$ for some $d_i \in \mathbb{N}, a \in E_i$. Therefore, f is solvable by radicals. Proving the forward case will require some extra machinery, which we will flesh out next lecture. $\square$

Math 594: Algebra II **Winter 2019**

Lecture 21: April 9th

Lecturer: Andrew Snowden *Scribe: Vignesh Jagathese*

21.1 Solving Equations by Radicals (Continued)

Before we finish the proof of Theorem 22.102 we introduce the notion of Galois closure, then use it to prove the forward direction.

21.1.1 Galois Closure

Let F be a field (characteristic 0) and K/F is some finite (not necessarily Galois) extension. The ***Galois Closure*** of K is the smallest Galois extension of F containing K. This definition does assume that K is contained in some Galois extension of F, which may not necessarily be true. Well, let's construct such a field as follows. As K/F is finite, suppose $K = F(\alpha_1, \ldots, \alpha_n)$. Take $f_1, \ldots, f_n$ to be the minimal polynomials of $\alpha_1, \ldots, \alpha_n$ respectively. Let $E = \mathrm{Gal}(f_1 \cdot \ldots \cdot f_n)$. E/F is certainly Galois, and $F \subset K \subset E$.

There is no guarantee that E is the smallest such Galois extension, though. If there were smaller such extensions, observe that if $F \subset M_1, M_2 \subset E$ where the M_i are Galois extensions, $M_1 \cap M_2$ is still a Galois extension over F¿ This follows from the Fundamental Theorem of Galois Theory, if M_1, M_2 correspond to normal subgroups H_1, H_2 of $\mathrm{Gal}(E/F)$, it follows that $M_1 \cap M_2$ corresponds to the (normal) subgroup $H_1H_2 \subset \mathrm{Gal}(E/F)$. This is because $M_1 \cap M_2$ is the largest set contained in M_1 and M_2, and as the bijection between extensions and subgroups is order reversing, it corresponds to the subgroup subgroup containing H_1 and H_2, which is precisely H_1H_2. All this suggests that $M_1 \cap M_2$ is Galois.

Therefore, define $K' = \bigcap_{M \in \mathcal{G}} M$ where $\mathcal{G}$ is the set of all field extensions M/F such that $K \subset M \subset E$ and M/F is a Galois extension. Such a construction is clearly unique and well defined, so we say that K' is the Galois Closure of K.

We can also construct K' explicitly. Let K'' be the smallest extension containing all σK for any $\sigma \in \mathrm{Aut}(K/F)$. K'' is clearly Galois, and by the fundamental theorem of Galois Theory, as it is the smallest thing containing all σK, $\mathrm{Gal}(K''/F)$ is the biggest group contained in every $\sigma(\mathrm{Gal}(E/K))\sigma^{-1}$, which is precisely $\bigcap_{\sigma \in \mathrm{Gal}(E/F)} \sigma(\mathrm{Gal}(E/K))\sigma^{-1}$, This is clearly normal, so $\mathrm{Gal}(K''/F)$ is Galois. $K'' \subset K'$ as $K'' \in \mathcal{G}$, and $K' \subset K''$ by construction of K''. Thus, $K'' = K'$, and both are equally valid constructions of Galois Closure. Notice that our construction of K'' shows us that our choice of initial E/F was irrelevant, even though our construction of K' was dependent on that choice.

21.1.2 Finishing the Proof From Last Lecture

Proof. (Theorem 22.101) All that is left to prove is the forward case. Suppose that $f \in F[T]$ is solvable by radicals, and let K/F be its splitting field. We'd like to show that $\mathrm{Gal}(K/F) = \mathrm{Gal}(f)$ is solvable. As f is solvable by radicals, we get the tower

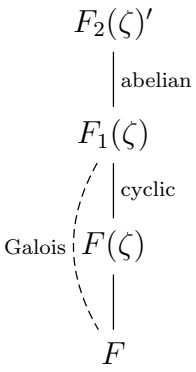
$$\begin{array}{c} K \subset F_n \\ | \\ \vdots \\ | \\ F_3 \\ | \\ F_2 \\ | \\ F_1 \\ | \\ F = F_0 \end{array}$$

Where $F_{i+1} = F_i(a_i^{d_i})$ for $d_i \in \mathbb{N}$, $a_i \in F_i$. Let F_n' be the Galois Closure of F_n/F. Notice that $\mathrm{Gal}(F_n'/F) \to \mathrm{Gal}(K/F)$ is a surjection; thus if $\mathrm{Gal}(F_n'/F)$ were solvable, then it follows that $\mathrm{Gal}(K/F)$ is solvable. Thus, it is sufficient to verify that F_n' is solvable. Let $d = [F_n : F_0]$, and let E/F be a Galois extension containing F_n/F and all dth roots of unity. First, observe that $F_1(\zeta)/F$ is Galois, as $F_1 = F(a^{1/d})$ for some $a \in F$, so $F_1(\zeta)$ is the splitting field for $T^d - a$, suggesting that it is Galois. It immediately follows that $F_1(\zeta)/F(\zeta)$ is a cyclic extension via similar logic to the proof in the reverse case.

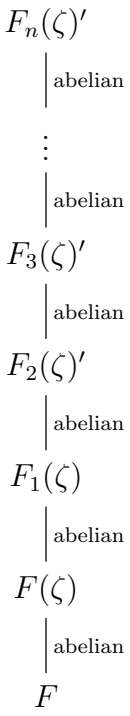
Next, we verify that $F_2(\zeta)'/F_1(\zeta)$ is abelian. We can view $F_2(\zeta)'$ as the minimal field extension of $F_1(\zeta)$ containing all $(\sigma b)^{1/d}$ for $F_2 = F_1(b^{1/d})$ and $\sigma \in \mathrm{Gal}(E/F_1(\zeta))$ for some Galois extension $F_1(\zeta) \subset F_2(\zeta)' \subset E$. Via the fundamental Theorem of Galois Theory, this induces an injection (via similar logic to the reverse case) of the form

$$\mathrm{Gal}(F_2(\zeta)'/F_1(\zeta)) \hookrightarrow \prod_{\sigma \in \mathrm{Gal}(E/F_1(\zeta))} \mathrm{Gal}(F_1(\zeta)((\sigma b)^{1/d})/F_1(\zeta))$$

$\mathrm{Gal}(F_1(\zeta)((\sigma b)^{1/d})/F_1(\zeta))$ is cyclic, so $\mathrm{Gal}(F_2(\zeta)'/F_1(\zeta))$ injects into a product of cyclic groups. It follows that $\mathrm{Gal}(F_2(\zeta)'/F_1(\zeta))$ is Abelian. Thus, we have the tower of extensions



Inducting on n, we find that $F_i(\zeta)'/F_{i-1}(\zeta)'$ is abelian for any $i \leq n$. This gives us the tower



Let $G_k = \mathrm{Gal}(F_n(\zeta)'/F_k(\zeta)')$, take $G_0 = \mathrm{Gal}(F_n(\zeta)'/F(\zeta))$ and $G_{-1} = \mathrm{Gal}(F_n(\zeta)'/F)$. It is clear that $1 = G_n \subset \ldots \subset G_0 \subset G_{-1}$. As $F_k(\zeta)'/F$ is Galois for any k, $G_k \subset G_{k-1}$ is a normal subgroup for any k. In addition, G_i/G_{i+1} is abelian, so we can conclude that $G_{-1} = \mathrm{Gal}(F_n(\zeta)'/F)$ is solvable, completing the proof. $\square$

21.2 The Unsolvability of the Quintic

Theorem 21.103. *There is no formula to solve a general polynomial $f \in F[T]$ for* $\deg(f) \geq 5$.

Proof. Take $E = F(x_1, \ldots, x_n)$ and suppose that S_n acts by variable permutation. Take $K = E^{S_n}$. E/K is Galois with Galois group S_n, suggesting that $[E : K] = n!$. Now consider $f(T) = \prod(T - x_i) \in E[T]$. f is completely invariant under S_n, so it must take coefficients in K, so $f \in K[T]$. Write $f(T) = \sum c_i T^i$ for $c_i \in K$. As $f \in F(c_0, \ldots, c_{n-1})[T]$, it follows that $[E : F(c_0, \ldots, c_{n-1})] \leq n!$, as E is the splitting field of f over $F(c_0, \ldots, c_{n-1})$. As $[E : K] = n!$ and $F(c_0, \ldots, c_{n-1}) \subset K \subset E$, it follows that $[E : F(c_0, \ldots, c_{n-1})] = n!$, and that $[K : F(c_0, \ldots, c_{n-1})] = 1$, so $K = F(c_0, \ldots, c_{n-1})$.

As we know E/F has transcendence degree n by construction, and $c_0, \ldots, c_{n-1}$ span E/F, $c_0 \ldots, c_{n-1}$ are a transcendence basis of E/F, suggesting that they are algebraically independent. Thus, $\mathrm{Gal}(f) = \mathrm{Gal}(E/K) = S_n$, for f a general polynomial of degree n. S_n is only solvable for $n < 5$, so it follows that f is only solvable by radicals for $n < 5$. In other words, there exist formula for polynomials of degree $0, 1, 2, 3, 4$, but there cannot be a general formula for polynomials of degree $n \geq 5$ (i.e. the quintic, as well as higher degree polynomials, are unsolvable). □