510A Lecture Notes

Contents

Part I

Group theory

Chapter 1

Groups

1.1 Lecture 1: Basic notions

Before getting started, I wanted to make some comments about prerequisites. Here are some things that you should be familiar with.

- Sets - I assume you have some working idea of the notion of a set and functions between them. Furthermore, I assume you know about basic operations that may be performed on sets: unions, intersections, Cartesian products, etc.
- Groups - I assume you have seen the notion of a group before and know a few examples (cyclic groups, symmetric groups)
- Arithmetic - I assume you know about basic facts from elementary number theory, e.g., gcd, divisibilty results for integers, etc.

1.1.1 Groups and homomorphisms

I will present the definition of a group in a rather formal way.

Definition 1.1.1.1. A quadruple $(G, \cdot, (-)^{-1}, e)$ consisting of a set G, a function $\cdot : G \times G \to G$ (called multiplication), a function $(-)^{-1} : G \to G$ (called inversion) and a distinguished element $e \in G$ is called a *group*, if the following diagrams commute:

i) (Associativity)

$$\begin{tikzcd} G \times G \times G \arrow[r, "\cdot \times id"] \arrow[d, "id \times \cdot"] & G \times G \arrow[d, "\cdot"] \\ G \times G \arrow[r, "\cdot"] & G. \end{tikzcd}$$

ii) (Units)

$$\begin{tikzcd} G \arrow[r, "e \times id"] \arrow[dr, "id"] & G \times G \arrow[d, "\cdot"] & \text{and} & G \arrow[r, "id \times e"] \arrow[dr, "id"] & G \times G \arrow[d, "\cdot"] \\ & G, & & & G. \end{tikzcd}$$

iii) (Inverses)

$$\begin{tikzcd} G \arrow[r, "(-)^{-1} \times id"] \arrow[dr, "e"] & G \times G \arrow[d, "\cdot"] & \text{and} & G \arrow[r, "id \times (-)^{-1}"] \arrow[dr, "e"] & G \times G \arrow[d, "\cdot"] \\ & G, & & & G, \end{tikzcd}$$

where the function $G \to G$ denoted e is the constant function with value $e \in G$.

If $(G, \cdot, (-)^{-1}, e)$ and $(G', \cdot, (-)^{-1}, e')$ are two groups, then a function $f : G \to G'$ is a *group homomorphism* if f preserves multiplication, i.e., the diagram

$$\begin{tikzcd} G \times G \arrow[r, "\cdot"] \arrow[d, "f \times f"] & G \arrow[d, "f"] \\ G' \times G' \arrow[r, "\cdot"] & G' \end{tikzcd}$$

commutes.

As mentioned in Appendix A.1.1, groups and group homomorphisms form a category $\mathbf{Grp}$ (objects are groups, morphisms are group homomorphisms).

Remark 1.1.1.2. The definition of group we have given is not "minimal": the notion of group can be specified with less data. You can, instead, specify only a function $m : G \times G \to G$ corresponding, in the notation above, to $(x, y) \mapsto xy^{-1}$ and reformulate the axioms of a group in terms of this function.

Remark 1.1.1.3. For notational and linguistic convenience, we will speak of the group G instead of always carting around all the baggage of the quadruple. Nevertheless, it is important to remember that a group structure is *additional data* on a given set.

Group objects in a cateogry

The above definition of group has the benefit of being easily transplanted to other settings: it can be used in any context where one can make sense of "products". For example, we may speak of *group objects in a category* $\mathscr{C}$ (see Definition A.1.1.1 for the definition of a category and basic properties.

Example 1.1.1.4 (Topological groups). If X is a topological group, then we can talk about what it means to have a group structure compatible with the topology: repeat Definition 1.1.1.1 and simply replace G by a topological space X, e by a point of X, require that $\cdot : X \times X \to X$ is a continuous function (we give $X \times X$ the product topology!) and require that $()^{-1}$ be a continuous map $X \to X$ and impose all the axioms in the definition.

Example 1.1.1.5 (Lie groups). Similarly, a "Lie group" is a manifold with compatible group structure: repeat Definition 1.1.1.1 and replace the set G by a smooth manifold M, e by a point of M, assume $\cdot$ is a smooth map of manifolds, and assume inversion is a smooth map of manifolds, once more assuming all additional axioms are satisfied.

Example 1.1.1.6. In greatest generality, we may speak of "group objects in a category $\mathscr{C}$". From the point of view of the above examples, we think of objects of our category equipped with a group structure compatible with whatever structure is present on objects. For example, a topological group is a group object in the category of groups. A Lie group is a group object in the category of smooth manifolds.

Homomorphisms and isomorphisms

Example 1.1.1.7. Any 1 element set has a group structure. If $\{e\}$ is the single element, multiplication is the unique function $\{e\} \times \{e\} \mapsto \{e\}$ and inversion is given by the identity map on the set. We will write 1 for this group. This group structure is unique in a strong sense: given any other 1 element set, there is a unique bijection between the two 1 element sets and this bijection "preserves" all the additional structure. Moreover, if G is any group, there is a unique group homomorphism $1 \to G$ that sends 1 to e.

Definition 1.1.1.8. A group homomorphism $f : G \to G'$ is an *isomorphism* (resp. monomorphism, epimorphism) if f is a *bijection* (resp. injection, surjection). A group homomorphism $f : G \to G'$ is called *trivial*, if the image of f is the identity $e' \in G'$.

Remark 1.1.1.9. Definition 1.1.1.8 is precisely the definition of isomorphism in a category (see Definition A.1.1.8) specialized to the category $\mathbf{Grp}$.

Lemma 1.1.1.10. *If $f : G \to G'$ is an isomorphism of groups, then the inverse function f^{-1} is also an isomorphism.*

Proof. The inverse is a function $f^{-1} : G' \to G$. We need to first show that $f^{-1}(e') = e$. To see this, write $e' = f(e)$. In that case, $f^{-1}(f(e)) = e$ by the definition of an inverse function. Similarly, to see that $f^{-1}(g_1'g_2') = f^{-1}(g_1')f^{-1}(g_2')$, write $g_1' = f(g_1)$ and $g_2' = f(g_2)$. Then, we have $f^{-1}(g_i') = g_i$. Furthermore, $f(g_1)f(g_2) = f(g_1g_2)$ since f is a homomorphism. Then, we see that $f^{-1}(g_1'g_2') = f^{-1}(f(g_1g_2)) = g_1g_2 = f^{-1}(g_1')f^{-1}(g_2')$. □

Types of groups

Definition 1.1.1.11. A group G is called *finite* if the set G is finite and *infinite* if it is not finite. If G is a finite group, the cardinality of G, denoted $|G|$ is called the *order of* G.

Definition 1.1.1.12. Given any group G, we can consider the swap function $sw : G \times G \to G \times G$ given by $(x, y) \mapsto (y, x)$. A group G is called *abelian* if the diagram

$$\begin{tikzcd}
G \times G \arrow[r, "sw"] \arrow[dr, "\cdot"] & G \times G \arrow[d, "\cdot"] \\
 & G \times G
\end{tikzcd}$$

commutes.

Example 1.1.1.13. If G is any group, then we can ask whether the inversion map $()^{-1} : G \to G$ is a homomorphism. Observe that $(gh)^{-1} = h^{-1}g^{-1}$. Thus, in order that inversion be an isomorphism, we require that $h^{-1}g^{-1} = (gh)^{-1} = g^{-1}h^{-1}$ for every $h, g \in G$. In other words, if inversion is homomorphism then G is abelian. Conversely, if G is abelian, then inversion is a homomorphism.

1.1.2 Products

Lemma 1.1.2.1. *If $\{G_i\}_{i \in I}$ is any family of groups, we can form the Cartesian product $\prod_i G_i$ as sets. The Cartesian product $\prod_{i \in I} G_i$ admits the structure of a group with componentwise multiplication, inversion and identity e given by $\prod_i e_i$.*

Proof. Exercise. □

Remark 1.1.2.2. There is a general notion of a product of a set of objects in a category (see Definition A.1.2.20). We may observe that the Cartesian product of groups as in Lemma 1.1.2.1 is a product in $\mathbf{Grp}$ in precisely this sense.

Lemma 1.1.2.3. *If $f : G \to H$ and $f' : G' \to H$ are group homomorphisms, then the fiber product $G \times_{f,H,f'} G'$ consists of those pairs $(g, g') \in G \times G'$ such that $f(g) = f'(g')$. The fiber product is a subgroup of $G \times G'$.*

Proof. Exercise. □

Remark 1.1.2.4. We introduced the category $\mathbf{Grp}$ above, the notion of a group object in a category in Example 1.1.1.6. In particular, you can speak of a group object in $\mathbf{Grp}$. Unwinding the definition, we begin with a group $(A, e, \cdot, ()^{-1})$, and we want to equip *it* with a group structure: we distinguish another element e' in A, specify a function $m : A \times A \to A$, but we require that this function is a group homomorphism for $\cdot$ on A and the product $\cdot \times \cdot$ on $A \times A$); we specify an inversion function $A \to A$ and require that this function is *also* compatible with the group structure on A. For example, in the first case, to say that m is a group homomorphism with respect to $\cdot$ implies that the following diagram commutes:

$$\begin{tikzcd}
(A \times A) \times (A \times A) \arrow[r, "m \times m"] \arrow[d, "\cdot \times \cdot"] & A \times A \arrow[d, "\cdot"] \\
A \times A \arrow[r, "m"] & A,
\end{tikzcd}$$

but there are a number of other compatibilities. In particular, we have a set A equipped, *a priori* with two units, two multiplications and two inversions. It turns out (and you will show on your HW) that a group object in the category of groups is an *abelian group*. More precisely, under the above conditions, the two units actually coincide, the two operations coincide, and they are both commutative! This observation is very useful in topology: it implies, e.g., the fundamental group of a topological group is always an abelian group.

1.1.3 Subgroups

Definition 1.1.3.1. A subset $H \subset G$ is a *subgroup* of G if $e \in H$ and if the composite maps $H \times H \hookrightarrow G \times G \xrightarrow{\cdot} G$ and $H \hookrightarrow G \xrightarrow{()^{-1}} G$ factor through $H \subset G$ (in other words the two listed composites have image contained in H).

Remark 1.1.3.2. Given a subgroup $H \subset G$, we can also define an injective group homomorphism $i : H \to G$. Conversely, any injective group homomorphism defines a subgroup (the image of the homomorphism). Sometimes, we will abusively conflate these notions. More generally, given any homomorphism $f : G \to G'$, the image of f has the structure of a subgroup of G'; we will sometimes write $\operatorname{im}(f)$ for this subgroup.

Lemma 1.1.3.3. *Given any group homomorphism $f : G \to G'$, the subset $\{g \in G | f(g) = e'\}$ has the structure of a subgroup of G; we will call this subgroup* $\ker(f)$.

Proof. Exercise. □

Lemma 1.1.3.4. *A group homomorphism $f : G \to G'$ is a monomorphism if and only if* $\ker(f)$ *is the trivial subgroup.*

Proof. Suppose $f : G \to G'$ is a group homomorphism. To say that f is a monomorphism is to say that f is injective as a function of the underlying sets, i.e., that $f(g) = f(g') \implies g = g'$. However, $f(g) = f(g') \Leftrightarrow f(g)f(g')^{-1} = e'$. Now, you can check that if f is a homomorphism, then $f(g)^{-1} = f(g^{-1})$ for any $g \in G$. Therefore, we can rewrite $e' = f(g)f(g')^{-1} = f(g)f(g'^{-1}) = f(gg'^{-1})$. Thus, the condition that $f(g) = f(g')$ is equivalent to the condition that $gg'^{-1} \in ker(f)$. On the other hand $g = g' \Leftrightarrow gg'^{-1} = e$. Therefore, if $\ker(f) = e$, it follows that f is injective. Conversely, if f is injective, then the non-empty preimages of any element must consist of a single element, and thus $\ker(f) = e$. □

Definition 1.1.3.5. Suppose G is a group. If $g \in G$ is an element, the centralizer $C_G(g)$ is the collection of all elements $h \in G$ such that $hg = gh$. If $S \subset G$ is a subset, then the centralizer of S in G is the collection of all $g \in G$ such that $gh = hg$ for each $h \in S$. The center of G, denoted $Z(G)$, is $C_G(G)$.

Lemma 1.1.3.6. *For any group G and any subset $S \subset G$, the subsets $C_G(S)$ are subgroups.*

Proof. Exercise. □

Lemma 1.1.3.7. *If $\{H_i\}_{i \in I}$ is any collection of subgroups of a group G, then $\cap_{i \in I} H_i$ is a subgroup of G.*

1.2 Lecture 2: Symmetries and group actions

1.2.1 Groups as symmetries

Example 1.2.1.1. Suppose S is a set. Write $Isom(S)$ for the set of bijective functions $f : S \to S$. Note that $Isom(S)$ has a distinguished element $id : S \to S$. There is a natural "multiplication" on $Isom(S)$ given by composition of functions. Since any bijective function has a (unique) inverse, we can define an inversion operation by sending a function f to its inverse function f^{-1}. Associativity of composition and the usual properties of the identity function and inverse of a function show that $Isom(S)$ is a group. In the special case where S is a finite set with n elements, we will write S_n for this group; this is the symmetric group on n elements.

We can also talk about symmetries of sets that "preserve additional structure."

Example 1.2.1.2. An (undirected) graph is a pair (V, E) consisting of a set V (vertices), and a set E of 2 element subsets of V (edges). If a pair $\{v, v'\}$ is an element of E, then v and v' are said to be adjacent. If (V, E) and (V, E') are graphs, then a bijection $f : V \to V$ is an isomorphism of graphs (a.k.a an edge preserving bijection), if v and v' are adjacent if and only if $f(v)$ and $f(v')$ are adjacent. Composites of isomorphisms of graphs are again isomorphisms of graphs. If (V, E) is a graph, and f is a self-isomorphism of (V, E), then its inverse function is again a self-isomorphism. The identity function is a self-isomorphism of (V, E). The set of self-isomorphisms of (V, E) together with composition of functions, inversion of functions, and identity function forms a group $Aut(V, E)$ called the automorphism group of the graph.

Example 1.2.1.3. If X is a topological space, then the homeomorphisms $\varphi : X \to X$ also form a group $\mathrm{Homeo}(X)$ called the group of homeomorphisms of X. If a set S is viewed as a topological space equipped with the discrete topology, then $\mathrm{Homeo}(S) = Isom(S)$. In general, $\mathrm{Homeo}(X) \subset Isom(X)$.

Example 1.2.1.4. If F is a field and V is an F-vector space, then the set of invertible linear transformations $\varphi : V \to V$ forms a group, often denoted $GL(V)$. Note that $GL(V)$ is a subset of $Isom(V)$, where in the latter case we simply view V as a set by forgetting it is a vector space.

Example 1.2.1.5. More generally, if $\mathscr{C}$ is a category and $C \in \mathscr{C}$, then one can define $\mathrm{Aut}(C)$ as the set of isomorphisms of C with itself in $\mathscr{C}$: the unit is given by the distinguished identity element in $\mathrm{Mor}(C, C)$, composition is associative by definition of a category, and the inversion operation is given by assigning to any isomorphism of C with itself, the corresponding inverse isomorphism.

1.2.2 Group actions

Definition 1.2.2.1. Suppose G is a group, and S is a set. An action of G on S is a function $a : G \times S \to S$ such that the following diagrams commute:

i) (Associativity)

$$\begin{tikzcd}
G \times G \times S \arrow[r, "id_G \times a"] \arrow[d, "\cdot \times id_S"] & G \times S \arrow[d, "a"] \\
G \times S \arrow[r, "a"] & S.
\end{tikzcd}$$

ii) (Identity)

$$\begin{tikzcd}
S \arrow[r, "e \times id_S"] \arrow[dr, "id_S"] & G \times S \arrow[d, "a"] \\
& S.
\end{tikzcd}$$

Given an action a of a group G on a set S, any fixed element $g \in G$ gives rise to a function $S \to S$ via $s \mapsto a(g,s)$. This function is a bijection because it has an inverse for which the composite is the identity on S, namely $s \mapsto a(g^{-1},s)$. Granting this, we can obtain the following alternative characterization of actions.

Lemma 1.2.2.2. *If a is an action of G on a set S, the function $G \to Isom(S)$ just described is a group homomorphism. Conversely, any homomorphism $G \to Isom(S)$ determines a (unique) action of G on S.*

Proof. Exercise. □

Based on the Lemma 1.2.2.2, note that if G acts on a set S and $\varphi : H \to G$ is a group homomorphism, then there is an induced action on S: simply consider the composite map $H \to G \to Isom(S)$. On the other hand, given two sets S and S', actions of G on S and S' and a function $f : S \to S'$, we would like to make sense of what it means for the function f to be compatible with the action. The following definition combines these two notions.

Definition 1.2.2.3. Suppose given a homomorphism $\varphi : G \to H$, and action a of G on a set S, and an action b of H on a set S'. A function $f : S \to S'$ intertwines the actions if the following diagram commutes:

$$\begin{tikzcd} G \times S \arrow[r, "a"] \arrow[d, "\varphi \times f"] & S \arrow[d, "f"] \\ H \times S' \arrow[r, "b"] & S'. \end{tikzcd}$$

In the special case where φ is the identity, we will say that f is a *G-equivariant function*.

In practice, if a set S is equipped with additional structure (e.g., it is a vector space, a group itself etc.) then one can consider actions that preserve that additional structure.

Example 1.2.2.4. If F is a field, and V is an F-vector space, then an action of G on V by invertible linear transformations, i.e., a homomorphism $\varphi : G \to GL(V)$, is called a *representation* of G on V. Since $GL(V) \subset Isom(V)$, any representation is an example of an action. Likewise, if X is a topological space, then a homomorphism $\varphi : G \to \mathrm{Homeo}(X)$ is called an action of G on the topological space X.

Definition 1.2.2.5. If a is an action of a group G on a set S, then we can consider the orbit map

$$o : G \times S \overset{a \times pr_S}{\longrightarrow} S \times S$$

Given any $s \in S$, the orbit of s under G, denoted $\mathcal{O}_s$, is the image of the function $o(\cdot, s) : G \to S$. The stabilizer s under G, denoted $Stab_G(s)$ or G_s, is the set of $g \in G$ such that $a(g,s) = s$.

Definition 1.2.2.6. An action a of a group G on a set S is said to be *free* if the orbit map $o : G \times S \to S \times S$ is injective.

Lemma 1.2.2.7. *The orbit map is injective if and only if for any $s \in S$, G_s is trivial.*

Proof. Suppose $o : G \times S \to S \times S$ is injective. This means that, for every $(g,s) \in G \times S$, $o(g,s) = o(g',s') \Rightarrow (g,s) = (g',s')$. However, by definition $o(g,s) = (g \cdot s, s)$, while $o(g',s') = (g's', s')$. Therefore, $(gs,s) = (g's',s')$. This, in turn, means that $s = s'$ and thus $gs = g's$. So the condition reads: $gs = g's \Rightarrow g = g'$, which is equivalent to ${g'}^{-1}gs = s \Rightarrow {g'}^{-1}g = e$. Since g and g' are arbitrary, this implies that $G_s = 1$, but since s was arbitrary, the result follows. The other direction is an exercise. □

Example 1.2.2.8. If G is any group, then we can define the *conjugation action* of G on itself by means of the function $c_g(g') = g^{-1}g'g$. It is worth pointing out that defining $c'_g(g') = gg'g^{-1}$ does not define an action by our definition because $c'_{g_1}c'_{g_2} = c'_{g_2g_1}$. For this reason, sometimes one distinguishes two kinds of actions (our definition corresponds to a "left" action, while the formula for c'_g corresponds to a "right" action). The left multiplication action of G on itself is given by the function $\ell_g(g') = g^{-1}g'$. Similarly, the right multiplication action of G on itself is given by $r_g(g') = g'(g)$.

Theorem 1.2.2.9 (Cayley's theorem)**.** *Any group G is a subgroup of a symmetric group and any finite group is a subgroup of S_n for some integer n.*

Proof. Consider the function $\ell : G \to Isom(G)$ sending $g \in G$ to $\ell_g(-)$. The function $\ell_g : G \to G$ is a bijection, since it has an inverse given by $\ell_{g^{-1}}$. Thus, we obtain a function $G \to Isom(G)$. First, we claim that the resulting function is a group homomorphism. Indeed, ℓ_e is the identity function on G by the unit axiom. On the other hand $\ell_{gh}(x) = gh(x) = \ell_g(\ell_h(x))$ so the resulting function preserves multiplication by the definition of composition of functions.

It remains to show that this function is injective, i.e., we have to show that $\ell_g = \ell_{g'} \Rightarrow g = g'$. However, to say that two functions are equal, means that for any $x \in G$ we have $\ell_g(x) = \ell_{g'}(x)$. Taking $x = e$, we see that $g = g'$. It follows that G is isomorphic to its image under ℓ, which is what we wanted to prove.

For the second statement, observe that if G is finite of order n, then $Isom(G)$ is a finite group of order $n!$. □

1.2.3 Addendum: actions on subsets

If a group G acts on a set S, then there are a number of auxiliary actions that one may consider. For example, let $P(S)$ be the power set of S, i.e., the set of all subsets of S. There is an induced action of G on $P(S)$ as follows: given a subset $T \subset S$, set $gT = \{g \cdot t | t \in T\}$. One checks that this actually defines an action. Similar statements can be made for other sets built out of S (e.g., the set of n-element subsets of S for some natural number n).

Example 1.2.3.1. Consider Example 1.2.2.8. The conjugation and left and right multiplication actions of G on itself induce actions on the power set $P(G)$. The stabilizer of a subset $S \in P(G)$ with respect to the action induced by conjugation by G consists of those $g \in G$ such that $g \cdot S = S$, i.e., $gSg^{-1} = S$. The normalizer $N_S(G)$ of a subset $S \subset G$ is, by definition, the preceding stabilizer, i.e., the set of $g \in G$ such that $gSg^{-1} = S$.

In this lecture, we begin introduce some tools to quantify how complicated a group is. One way to study a group G is to study homomorphisms from an arbitrary group to G and homomorphisms from G to an arbitrary group. In a sense that will be made precise later, a group G is completely determined by knowing all homomorphisms from an arbitrary group to it. Note that if H is a group, then any homomorphism $\varphi : H \to G$ factors through the $im(\varphi)$, so knowing homomorphisms $\varphi : H \to G$ in particular involves study of all subgroups of G. We will return to this issue later. In this lecture, we will instead study homomorphisms *out* of a group G.

1.3 Lecture 3: Automorphisms, conjugation and normality

1.3.1 Automorphisms and conjugation

Example 1.3.1.1. If G is any group, we write $Aut(G)$ for the set of isomorphisms $f : G \to G$. The identity function $id : G \to G$ is an automorphism and, as we observed above, if f is an isomorphism of groups, then f^{-1} is also an isomorphism of groups. The axioms insure that $Aut(G)$ with composition and inversion as operations and identity function as distinguished element is a group.

Example 1.3.1.2. If G is any group, any $g \in G$ is any element $c_g(\cdot) : G \to G$ is an isomorphism. The inverse of $c_g(\cdot)$ is the function $c_{g^{-1}}(\cdot)$. Conjugation by the identity element is simply the identity function. Note that $c_g(c_h(\cdot)) = c_g(h - h^{-1}) = gh - h^{-1}g^{-1} = c_{gh}(-)$. Thus, conjugation determines a homomorphism $G \to Aut(G)$.

Definition 1.3.1.3. If G is a group, and $H \subset G$ is a subgroup, then the image of H under c_g is a subgroup of G called the conjugate of H by g.

Definition 1.3.1.4. An automorphism f of G of the form $c_g(-)$ for some $g \in G$ is called an *inner* automorphism. An automorphism that is not an *inner* automorphism is called an *outer* automorphism.

Example 1.3.1.5. The homomorphism $G \to Aut(G)$ need not be either a monomorphism or an epimorphism. Indeed, if A is an abelian group, then conjugation by any element is the identity map. Therefore, the homomorphism $A \to Aut(A)$ is the trivial homomorphism, i.e., the only inner automorphism is the identity. On the other hand, inversion gives a non-trivial automorphism of G, which is, in general, not the identity.

Lemma 1.3.1.6. *If G is a group acting on a set S, and if s and s' are two elements of S lying in the same G-orbit, then the subgroups G_s and $G_{s'}$ are conjugate.*

1.3.2 Cosets and orders

Definition 1.3.2.1. If G is a group and H is a subgroup of G, the left cosets of H in G are the subsets of the form $gH := \{gh | h \in H\}$. The collection of left cosets of H in G will be denoted G/H (this is just a set!).

The following result shows that the cosets of a group form a partition of G into disjoint subsets all of the same cardinality.

Lemma 1.3.2.2. *If gH and $g'H$ are two left cosets of H in G, then either $gH = g'H$ or $gH \cap g'H = \emptyset$.*

Proof. Suppose $x \in gH \cap g'H$. We claim that $gH \subset g'H$ and conversely. Indeed, any two elements of gH differ by a unique element of H in the sense that if gh_1 and gh_2 are elements, then $gh_2 = gh_1h_1^{-1}h_2$. Thus, it follows that $xH = gH$ and likewise that $xH = g'H$. □

Corollary 1.3.2.3 (Lagrange's theorem)**.** *If G is a finite group, and H is a subgroup, then $|G| = |H| \cdot |G/H|$. In particular, $|H|||G|$.*

Corollary 1.3.2.4 (Orbit-stabilizer formula)**.** *If G is a finite group acting on a set S, then for any $s \in S$, $|G| = |\mathcal{O}_s||G_s|$.*

Proof. The elements of $\mathcal{O}_s$ are precisely the elements of the form $g \cdot s$. We claim that the choice of the element s gives rise to a function $G/G_s \to \mathcal{O}_s$. Indeed, we have the function $\varphi : G \to \mathcal{O}_s$ defined by $\varphi(g) = g \cdot s$. Observe that $\varphi(g) = \varphi(g') \Leftrightarrow gg'^{-1} \in G_s$. Thus, the assignment $\varphi'(gG_s) = \varphi(g)$ yields a well-defined function. The function φ is surjective by construction and therefore so is the function φ'. The defining formula for φ' shows that it is injective as well. (Alternatively, one can define an inverse function). The result now follows from Lagrange's theorem. □

1.3.3 Normal subgroups

Lemma 1.3.3.1. *If $f : G \to G'$ is a group homomorphism, then $K := \ker(f)$ is a subgroup of f that is stable under conjugation by G, i.e., given any $g \in G$ and $k \in K$, $gkg^{-1} \in K$.*

Proof. Suppose $g \in G$ and $k \in K$ are arbitrary. We just need to show that $f(gkg^{-1}) = e$. However, $f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)ef(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = e'$. □

Definition 1.3.3.2. A subgroup $N \subset G$ is called a *normal subgroup* of G if N is stable by conjugation, i.e., for every $g \in G$ and every $n \in N$, $gng^{-1} \in N$. We will write $N \trianglelefteq G$ if N is a normal subgroup of G.

Example 1.3.3.3. The trivial subgroup $e \subset G$ is always a normal subgroup, and G is a normal subgroup. A normal subgroup $H \subset G$ such that $H \neq G$ is called a proper normal subgroup.

Example 1.3.3.4. Since conjugation is trivial in an abelian group, any subgroup of an abelian group is normal.

Remark 1.3.3.5. A group that has the property that every subgroup is normal is called a *Dedekind group*. We just saw that abelian groups are Dedekind, but there are non-abelian groups that are Dedekind as well. For example, the quaternion group of order 8 is a Dedekind group that is not abelian.

Definition 1.3.3.6. A group G is called *simple* if it has no non-trivial proper normal subgroups.

Example 1.3.3.7. Any finite group of prime order is simple. Indeed, if G is such a group, and H is any subgroup, then $|H|||G|$ by Lagrange's theorem. This means that either $|H| = 1$, i.e., H is the trivial group, or $|H| = p$. It follows from the counting formula that $H = G$.

1.4 Lecture 4: More on normal subgroups, and generators

1.4.1 Normal subgroups II

Given any two subsets S, S' of G, their product $S \cdot S'$ is the subset of G consisting of elements of the form $s \cdot s'$. Of course, any coset is itself an example of this form.

Lemma 1.4.1.1. *If $N \trianglelefteq G$, then the product of two left cosets is again a left coset. More precisely, $gN \cdot g'N = gg'N$ as subsets of G.*

Proof. We will show that $gN \cdot g'N \subset gg'N$ and conversely. For the first inclusion, take $gn \in gN$ and $g'n' \in g'N$. Then, $gng'n' = gg'{g'}^{-1}ng'n'$. Since N is normal, ${g'}^{-1}ng' \in N$. Thus, ${g'}^{-1}ng'n' \in N$ as well since N is a subgroup. Moreover, this element lies in the coset $gg'N$. Since n and n' were arbitrary elements of N, the relevant containment follows. Conversely, given any element $gg'n \in gg'N$, we can write it as $geg'n$, which is in the product $gNg'N$. □

The identity coset is the coset eN. Define inversion of cosets by $gN \mapsto g^{-1}N$.

Corollary 1.4.1.2. *If $N \trianglelefteq G$ is a normal subgroup, then G/N equipped with multiplication coming from multiplication of cosets, inversion of cosets and identity given by eN is a group.*

Proof. I leave to you the exercise of checking associativity of the above product, which follows from associativity in G. The formula in the previous lemma shows that eN is an identity and also that $g^{-1}N$ is an inverse. □

If N is a normal subgroup of G, then we have just defined a group G/N called the quotient of G by N. Observe that the function $f : G \to G/N$ defined by $f(g) = gN$ is a well-defined group homomorphism and the kernel of f is precisely N. Furthermore, f is surjective by construction. Thus, if $N \subset G$ is a normal subgroup, then not only do we obtain a new group G/N, there is an explicit surjective group homomorphism $G \to G/N$ with kernel N called the *quotient map*.

Suppose $\varphi : G \to G'$ is a surjective group homomorphism. In that case, $\ker(\varphi)$ is a normal subgroup of G, and the construction above yields a quotient $G/\ker(\varphi)$ and a surjective homomorphism $G \to G/\ker(\varphi)$. We would like to compare this quotient group to G', and in order to do this we need to construct a homomorphism between the $G/\ker(\varphi)$ and G'.

In fact, φ gives rise to a comparison homomorphism. In more detail, since $\varphi(\ker(\varphi)) = e_{G'}$ by definition, it follows that φ actually is constant on left cosets for $\ker(\varphi)$, i.e., $\varphi(g\ker(\varphi)) = \varphi(g)$. Moreover,

$$\varphi(g_1\ker(\varphi)g_2\ker(\varphi)) = \varphi(g_1g_2\ker(\varphi)) = \varphi(g_1g_2)$$

since $\ker(\varphi)$ is normal. These formulas show that $\varphi : G \to G'$ actually defines a homomorphism $\bar{\varphi} : G/\ker(\varphi) \to G'$ such that the composite

$$G \longrightarrow G/\ker(\varphi) \xrightarrow{\bar{\varphi}} G'$$

coincides with φ. Note that $\bar{\varphi}$ is surjective by construction since φ has the same property. We can ask if the comparison map is actually an isomorphism. This observation, in slightly greater generality, is the content of the next result.

Theorem 1.4.1.3 (First isomorphism theorem)**.** *If $f : G \to H$ is a group homomorphism, with kernel K, then K is a normal subgroup of G and the homomorphism f factors through an isomorphism $G/K \xrightarrow{\sim} \mathrm{im}(f)$.*

Proof. As above, define a function $\bar{f} : G/K \to H$ by means of the formula $\varphi(gK) = f(g)$. This formula is well-defined by repeating the discussion before the theorem statement. Since $f : G \to im(f) \subset H$ is surjective by definition, the argument for surjectivity described above yields the surjectivity of $\bar{f}$. Now, we show that $\bar{f}$ is injective. To this end, suppose $f(gK) = f(g'K)$. In that case, we know that $f(g) = f(g')$, which means that $f(gg'^{-1}) = e$, which means that $gg'^{-1} \in K$, which means that $gK = g'K$, as desired. □

As the name "first isomorphism theorem" indicates, there are other isomorphism theorems, which can be thought of as expressing additional compatibilities about the isomorphism in Theorem 1.4.1.3. In general, examples shows that it can be the case that normality is not transitive, i.e., even if K is normal in H and H is normal in G, then K need not be normal in G. Thus, general compatibility statements will require additional hypotheses on the groups in question. For example, suppose we are given a sequence $K \subset H \subset G$ with K and H normal in G. In that case, K is automatically normal in H. Moreover, we may form the three quotients $H/K, G/K$ and G/H. The quotient homomorphism $G \to G/H$ is constant on left K-cosets and thus factors through a homomorphism $G/K \to G/H$. The third isomorphism theorem states that the kernel of this homomorphism is identified with H/K

Theorem 1.4.1.4 (Third isomorphism theorem)**.** *If $K \subset H \subset G$ are subgroups, where both K and H are normal in G, then the quotient morphism $G \to G/H$ factors through a surjective group homomorphism $G/K \to G/H$. The inclusion $H \subset G$ induces a homomorphism $H/K \to G/K$ making H/K a normal subgroup of G/K and the homomorphism $G/K \to G/H$ factors through an isomorphism $(G/K)/(H/K) \cong G/H$.*

Proof. Exercise. □

Theorem 1.4.1.5 (Second isomorphism theorem)**.** *If N and T are subgroups of G with N a normal subgroup, then $N \cap T$ is normal in T, and $T/(N \cap T) \cong NT/N$.*

Proof. Exercise. □

The following setup arises over and over in the above, so we will give it a special name.

Definition 1.4.1.6. A short exact sequence of groups, written

$$1 \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow 1$$

is a sequence of group homomorphisms such that $K \to G$ is injective, $G \to H$ is surjective, and K is the kernel of $G \to H$. Equivalently, we will say that G is an extension of H by K.

Remark 1.4.1.7. Note that any normal subgroup gives rise to a short exact sequence. One particularly imporant example is the "trivial extension". If K and H are any two groups, then $K \times H$ is a group. There is a homomorphism $K \to K \times H$ given by $k \mapsto (k, e_H)$. On the other hand, there is the projection homomorphism $K \times H \to H$ sending $(k, h) \mapsto h$. Note that the kernel of the projection homomorphism is precisely K, so there is a short exact sequence of the form

$$1 \longrightarrow K \longrightarrow K \times H \longrightarrow H \longrightarrow 1;$$

this short exact sequence is called the trivial extension of H by K. More generally, given a short exact sequence

$$1 \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow 1$$

since the right hand homomorphism is surjective, we can always choose a function $s : H \to G$ (not, in general, a group homomoprhism!) such that the composite $H \to G \to H$ is the identity on H. Thus *as a set* G can be identified with $K \times H$, and an extension can be thought of as the set $K \times H$ equipped with a twisted multiplication. The problem of deciding when we may build an extension of H by K is the *extension problem*.

If G is a group, then we can try to study it inductively as follows: pick a normal subgroup and look at the quotient. We may then investigate the normal subgroup and the quotient in the same way. Eventually we will obtain groups where we may no longer find proper normal subgroups, i.e., a simple groups. If, for example, G is a finite group, then this process must terminate after a finite number of steps. We may therefore break up the problem of determining all finite groups up to isomorphism in two steps: (i) determine all finite simple groups, and (ii) determine all the ways of building short exact sequences of groups as in Definition 1.4.1.6, i.e., "solve" the extension problem.

1.4.2 The universal property of quotients

We can abstract the properties of the quotient homomorphism and some of the content of the isomorphism theorems. Indeed, suppose $\varphi : G \to G'$ is any group homomorphism, and suppose $N \subset G$ is any subgroup that is contained in $\ker(\varphi)$. Pictorially, these homomoprhism are organized into the diagram:

$$\begin{tikzcd}
N \arrow[r] & G \arrow[r, "\varphi"] \arrow[d] & G' \\
& G/N &
\end{tikzcd}$$

where the vertical map is the quotient homomorphism. Since N is contained in φ, the arguments provided above show that φ is constant on left N-cosets and thus factors through a homomorphism $\bar{\varphi} : G/N \to G'$. In fact, this observation gives a characterization of the group G/N, and the discussion so far proves the following statement (I leave it as an exercise to sort out exactly what is being used where).

Theorem 1.4.2.1. *Suppose $N \subset G$ is a normal subgroup. There exists a (unique up to isomorphism) pair $(G/N, q)$ consisting of a group G/N, and a surjective homomorphism $q : G \to G/N$ (called the canonical quotient map) such that for any homomorphism $\varphi : G \to G'$ such that N is contained in* $\ker(\varphi)$*, there exists a unique homomorphism $\bar{\varphi} : G/N \to G'$ with $\varphi = \bar{\varphi} \circ q$.*

1.4.3 Internal direct products

Definition 1.4.3.1. A group G is the internal direct product of two subgroups H_1 and H_2 if $H_1 \cap H_2$ is the trivial subgroup, and $H_1H_2 = G$, and every element of H_1 commutes with H_2.

Lemma 1.4.3.2. *If G is the internal direct product of two subgroups H_1 and H_2, then the product map $H_1 \times H_2 \to G$ sending $(x, y) \mapsto xy$ is an isomorphism.*

Proof. The condition that every element of H_1 commutes with H_2, then it is straightforward to check that the product map $H_1 \times H_2 \to G$ is a homomorphism. The map $H_1 \times H_2 \to G$ is surjective since $H_1H_2 = G$. The kernel of the product map consists of those pairs (x, y) such that $xy = e$. However, this equality implies $x = y^{-1}$, i.e., $x \in H_1 \cap H_2$ and $y \in H_1 \cap H_2$. Since the intersection is trivial, it follows that $x = y = 1$. □

Remark 1.4.3.3. The above result has a converse: if $G = H_1 \times H_2$, then G is the internal direct product of H_1 and H_2.

1.4.4 Generators

If G is a group, and $g \in G$ is any element, then we can define the element g^i for any $i \in \mathbb{Z}$; by convention $g^0 = e$ and the power law $g^a g^b = g^{a+b}$ holds. The subset $\langle g \rangle$ of G consisting of g^i, $i \in \mathbb{Z}$ is a subgroup of G; it is called the subgroup of G generated by g. Here is an alternative characterization.

Lemma 1.4.4.1. *If G is a group and $g \in G$ is an element, then $\langle g \rangle$ is the smallest subgroup of G that contains g.*

Proof. We have shown that $\langle g \rangle$ is a subgroup of G containing g, and therefore it contains the smallest subgroup of G containing g. On the other hand, if $g \in G$, then all the g^i must be in the smallest subgroup as well, so $\langle g \rangle$ is contained in the smallest subgroup containing g as well. □

More generally, given a subset S of G, we can consider the smallest subgroup of G containing S; we will write $\langle S \rangle$ for this subgroup. Since the collection of all such subgroups is non-empty (it contains G), and since the intersection of any two subgroups is again a subgroup, it follows that $\langle S \rangle$ actually exists.

Example 1.4.4.2. The subgroup generated by the empty set is the trivial subgroup.

Definition 1.4.4.3. If G is a group and $S \subset G$ is a subset, then say G is *generated by S* (or that S is a generating set for G) if $\langle S \rangle = G$. Say that G is *finitely generated* if it has a finite generating set.

Remark 1.4.4.4. Note that every group G has a (possibly infinite) generating set (namely, the set G itself). In particular, every finite group is finitely generated.

1.5 Lecture 5: Free groups

1.5.1 Free groups: definitions

If G is generated by S, in general there will be many ways to write elements of G as products of elements of S. We now study the "simplest" such group.

Consider a set S (for the moment, we will call the elements of S an alphabet). Define a set S^{-1} whose elements are expressions of the form s^{-1} with $s \in S$. Set $T = S \coprod S^{-1}$. A word on S is a (possibly empty) finite string $w_1 \cdots w_n$ where each w_i is in T. Two words $w_1 \cdots w_i w_{i+1} \cdots w_n$ and $w_1 \cdots w_{i-1} w_{i+2} \cdots w_n$ are elementarily equivalent if either $w_i = s$ and $w_{i+1} = s^{-1}$ or $w_i = s^{-1}$ and $w_{i+1} = s$. Say two words are equivalent if they are equivalent for the equivalence relation generated by elementary equivalence. The integer n is called the length of the word, and we will say that a word is *reduced* if it is not equivalent to a word of smaller length. With some work, one may show that every word is equivalent to a *unique* reduced word, which we will refer to as its reduction. We may then define a product on words by concatenation followed by reduction. Given any word $w_1 \cdots w_n$, we can define an inverse by $w_n^{-1} \cdots w_1^{-1}$, where by convention if $w_i = s^{-1}$, then $w_i^{-1} = s$. I hope the following result makes intuitive sense.

Theorem 1.5.1.1. *If S is a set, then the set of reduced words on S with product given by concatenation (followed by reduction), inverse given by the inversion formula, and identity given by the empty word is a group.*

Definition 1.5.1.2. If S is a set, the group $F(S)$ is called the free group on the set S.

Example 1.5.1.3. The free group on a 1 element set x is isomorphic to $\mathbb{Z}$. The reduced words are precisely the expressions $x \cdots x = x^n$, $x^{-1} \cdots x^{-1} = x^{-m}$ or the empty word. To define the isomorphism, we send x to ± 1.

This definition has the benefit of being explicit: we know how to describe elements of free groups and compute with them. However, the downside of this is that it does not, in any sense, tell us the sense in which $F(S)$ is "free". To explain the sense in which $F(S)$ is free, we will take a more abstract (and non-constructive) point of view.

1.5.2 Free groups: universal properties

If S is a set, and $F(S)$ is the free group on S whose costruction was sketched earlier, then by construction note that there is a function $i_S : S \to F(S)$ sending a letter of the alphabet S to the corresponding element of $F(S)$. While the construction/definition we had before had the benefit of being explicit it does not provide a useful way to "recognize a free group if you see one", i.e., a property that characterizes the free group on a set S amongst all groups. The key characterizing property of free groups is the following.

Definition 1.5.2.1. Assume S is a set. A free group on S is a pair $(i_S, F(S))$ consisting of a group $F(S)$ and a function $i_S : S \to F(S)$ such that, given any group G and a function $f : S \to G$, there is a unique homomorphism $\varphi_f : F(S) \to G$ factoring f, i.e., $f = \varphi_F \circ i_S$.

This definition shows that a free group on a set S, if it exists, is in fact uniquely determined (up to isomorphism) by the above property.

Example 1.5.2.2. From the universal property, it follows that the free group on the empty set is the trivial group. Indeed, if S is the empty set, then there is a unique function $\emptyset \to G$. By the universal property, this function extends uniquely to a a group homomorphism $F(\emptyset) \to G$ for any group G.

Assuming free groups exist, the universal property also shows that assigning to a set S the free group $F(S)$ extends to a functor **Set** $\to$ **Grp** in the sense of Definition A.1.2.1. Indeed, suppose S and S' are any pair of sets and $g : S \to S'$ is any function. In that case, the function $i_{S'} : S' \to F(S)$ yields a function $S \to S' \to F(S')$. Taking $G = F(S')$ in the above definition, there is a unique homomorphism $F(S) \to F(S')$ factoring $S \to F(S')$.

In Example A.1.2.3, we observed that there is a "forgetful" functor **Grp** $\to$ **Set** that assigns to a group G its underlying set and to a group homomorphism the underlying function of sets. Since any function $S \to G$ is simply a function to the underlying set of G (forgetting the group structure) we can recast Definition 1.5.2.1 as a relationship between the forgetful functor and the "free group" functor as the following identification:

$$\mathrm{Hom}_{\mathbf{Grp}}(F(S), G) = \mathrm{Hom}_{\mathbf{Set}}(S, G).$$

This kind of an identification is an example of a pair of *adjoint functors* between categories (see Definition A.1.2.15).

If a group G is generated by a set $S \subset G$, then the universal property of the free group shows that there is a homomorphism $F(S) \to G$ extending $S \to G$; moreover, the fact that G is generated by S amounts to the fact that the homomorphism $F(S) \to G$ is *surjective*. In fact, these abstract observations suggest an alternative way to *construct* the free group on a set S, obviating our previous approach.

Theorem 1.5.2.3. *If S is a set, then a free group on S exists, i.e., there exists a group $F(S)$ and a function $i_S : S \to F(S)$ having the property mentioned in* Definition 1.5.2.1.

Proof. The idea to build S is encoded in our previous paragraph: the group $F(S)$ is generated by the set S and it is the "first" such group with this property. Therefore, consider the collection of isomorphism classes of groups G that may be generated by a set of cardinality at most $|S|$. We claim that this is a set; this is a cardinality count that we will discuss below. Assuming this for the time being, let us proceed.

Let $\mathfrak{D}$ be the collection of all pairs (G, ψ), consisting of a group G and $\psi : S \to G$ whose image generates G. By what we just saw, this is a set, and therefore we may form

$$\hat{F} := \prod_{(G,\psi)\in\mathfrak{D}} G$$

by appeal to Lemma 1.1.2.1.

By construction there is a function $S \to \hat{F}$. Define F to be the subgroup of $\hat{F}$ generated by the image of $S \to \hat{F}$ (i.e., the intersection of all subgroups of $\hat{F}$ whose image contains S) and let $i : S \to F$ be the map obtained by restricting S to its image.

We claim that F is a free group on the set S. To see this, it suffices to check the characterizing property. Thus, let H be any group, and suppose $f : S \to H$ is a function. Let $G \subset H$ be the subgroup generated by the image of S and let $f : S \to G$ be the resulting function. Note that the pair (G, f) must lie in $\mathfrak{D}$, and thus we obtain a unique homomorphism $\hat{F} \to G$, i.e, the projection onto the factor corresponding to (G, f). The desired homomorphism is obtained by restricting to $F \subset \hat{F}$, and the uniqueness statement is immediate by unwinding the definitions.

To finish the proof, we simply need to explain the cardinality argument suggested above: there is a set consisting of isomorphism classes of groups generated by at most $|S|$ elements. If G is a group generated by a set S, note that if $|S|$ is infinite, then $|G|$ is at most $|S|$. Indeed, every element of G may be written as a finite product of elements of S. Thus, if S is finite let T be a countably infinite set and if S is infinite, let T be a set of the same cardinality as S. To finish, it remains to observe that a group stucture is given by a pair of functions $\varphi : G \times G \to G$ and $inv : G \to G$. Thus, we may consider the set of group structures on subsets of T in either case, and this yields the result. □

Remark 1.5.2.4. It is worth pointing out one thing that has been swept under the rug here: while we have shown that free groups exist, we have not yet established that they may be manipulated in the way discussed in Theorem 1.5.1.1. In other words, while we may simply refer to elements of the group $F(S)$ as words, we don't know that the product on $F(S)$ is precisely the same as that from Theorem 1.5.1.1. Instead, to show the two constructions agree, one must first construct a group as suggested in the previous lecture and then show that it satisfies the universal property of the free group, in which case it must be isomorphic to the free group as constructed above. Thus in contrast to the previous discussion, while it's "easy" (from a certain point of view) to see that free groups exist by this procedure, it is by no means explicit.

1.5.3 Addendum: Proof of Theorem 1.5.1.1

Here, we show that the free group as described in terms of words actually coincides with the free group constructed abstractly above. To this end, the key step is establishing uniqueness of reductions of words. Recall that if w is a word, then an elementary reduction of w is a word w' obtained by deleting a subword of the form ss^{-1} or $s \in S \sqcup S^{-1}$. Given a word, there can be many possible reductions. We will write $w \to w_1 \to \cdots \to w_n$ for a reduction process (since w is a finite string, there are only finitely many possible reductions). If we cannot perform elementary reductions on w_n, then w_n will be called a reduced form of w.

Lemma 1.5.3.1. *If w is a word, and w_1 and w_1' are two elementary reductions of w, then there exist elementary reductions $w_1 \to w_2$ and $w_1' \to w_2$.*

Proof. Let $w \to w_1$ and $w \to w_1'$ be two elementary reductions of w. We treat two cases: either the two elementary reductions are disjoint or they "overlap". More precisely, in the disjoint case, we may write $w = u_1ss^{-1}u_2s's'^{-1}u_3$ for suitable words u_1, u_2 and u_3. In this case, $w_1 = u_1u_2s's'^{-1}u_3$ and $w_1' = u_1ss^{-1}u_2u_3$ and we take $w_2 = u_1u_2u_3$. The other possibility is the "overlapping" case, i.e., $w = u_1ss^{-1}su_2$, $w_1 = u_1su_2 = w_1'$ and we take $w_2 = w_1 = w_1'$. □

Proposition 1.5.3.2. *If w is a word, then there is a unique reduced word w that may be obtained by w by a finite sequence of elementary reductions.*

Proof. We induct on the length of w. If $|w| = 0$, then there is nothing to check. Thus, assume $|w| \geq 1$. Suppose $w \to w_1 \to \cdots \to w_m$ and $w \to w_1' \to \cdots \to w_n'$ are two strings of elementary reductions with w_m and w_n' reduced words. We want to show that $w_m = w_n'$. Consider the reductions $w \to w_1'$ and $w \to w_1$. Note that $|w_1| < |w|$ and $|w_1'| < |w|$. By Lemma 1.5.3.1, we may find w_2'' such that $|w_2''| < |w|$ and w_2'' is a common reduction of w_1 and w_1'. By the induction hypothesis, w_1, w_1' and w_2'' have a unique common reduction, which is what we wanted to show. □

Proof of Theorem 1.5.1.1. It suffices to establish associativity of product. Granted associativity, the other facts follow immediately from the definitions. Suppose u, v and w are words. For any word x, write $\overline{x}$ for the unique reduced word associated with x, which exists by Proposition 1.5.3.2. Then, we defined $u \cdot v = \overline{uv}$ and $v \cdot w = \overline{vw}$. So we want to show that $\overline{\overline{uv}w} = \overline{u\overline{vw}}$. Each of these reduced words is obtained from uvw by a sequence of elementary reductions. Thus, it suffices to apply Proposition 1.5.3.2 to uvw to conclude. □

Finally, we want to conclude that if S is a set, then $F(S)$ as defined by Theorem 1.5.1.1 satisfies the property of Definition 1.5.2.1. To this end, suppose S is a set, G is a group, and $f : S \to G$ is a function. For any word $w \in F(S)$, we can write $w = w_1 \cdots w_n$ with $w_i \in S \sqcup S^{-1}$. Define the homomorphism φ by $\varphi(\emptyset) = 1$. If $w_i \in S$, then set $\varphi(w_i) = f(w_i)$. If $w_i \in S^{-1}$, then ${w_i}^{-1} \in S$ and set $\varphi(w_i) = f(w_i^{-1})^{-1}$.

Then, define $\varphi(w) = \varphi(w_1) \cdots \varphi(w_n)$. That φ is a group homomorphism is immediate, and the universal property is thus satisfied.

1.5.4 Relations and presentations

If G is a group, and S is a generating set, then we can consider the homomorphism $\varphi : F(S) \to G$. The kernel of $K := \ker(\varphi)$ is a normal subgroup of $F(S)$. The elements of K arise in the following fashion: since φ is surjective, if we have two elements x and y such that x and y are sent to the same element of G (i.e., we have two different expressions of some element in G as a reduced word), then xy^{-1} (or yx^{-1} or $x^{-1}y$ or $y^{-1}x$) is an element of the kernel. The expression xy^{-1} can be thought of as an identification of the two different words, i.e., it is a "relation." Thus, the elements of K are precisely the relations among the generators.

In general, we can choose a generating set for K; if this set can be chosen to be finite, then G is called *finitely related*. If both S and a generating set for K can be chosen to be finite, then G is called *finitely presented*. Of course, one could keep going and consider relations among relations and so on, but most ways in which this is studied today rely on topological notions.

Now, we would like to go in the other direction: given a generating set S, we would like to describe a group as the quotient of $F(S)$ by some relations. In the previous paragraph, the relations form a group K, which was a normal subgroup of $F(S)$ so that $F(S)/K$ is actually a group. If we were just to specify some generators for a subgroup of $F(S)$, it would not be clear that the resulting subgroup is normal so that a quotient group even exists. For that reason, the next best thing is to take the smallest normal subgroup of $F(S)$ containing the chosen generators of K. Let us formalize this process.

Definition 1.5.4.1. If G is a group and $S \subset G$ is a subset, then the *normal closure* of S in G, denoted $N(S)$, is the smallest normal subgroup of G containing S.

Lemma 1.5.4.2. *If G is a group and $S \subset G$ is a subset, then the normal closure of S exists.*

Proof. The set of normal subgroups of G containing S is non-empty (it contains G). Moreover, if H and H' are two normal subgroups of G that contain S, then their intersection $H \cap H'$ is also a normal subgroup of G (since it must also be stable under conjugation) that contains S. □

Definition 1.5.4.3. A presentation of a group G is a pair $\langle S|R\rangle$ where S is a generating set for G and R is a subset of $F(S)$ such that $F(S)/N(R) \cong G$.

Lemma 1.5.4.4. *Finite groups are finitely presented.*

Proof. Intuitively, this follows from the fact that if G is a finite group, then we can simply write down the entire multiplication table for G to understand all possible relations. In fact, we can turn this intuitive idea into a formal proof.

Let $G = g_1, \ldots, g_n$ be the distinct elements of G. Then, multiplication is given by the formula $g_i g_j = g_k$ for suitable k. We can view $S = \{g_1, \ldots, g_n\}$ as a set of generators and consider the homomorphism $\pi : F(S) \to G$. The elements $g_i g_j g_k^{-1}$ all lie in the kernel of π, and write R_0 for the set of all such elements; thus, $R_0 \subset \ker(\pi)$. If N is the normal closure of R_0 in $F(S)$, then $N \subset \ker(\pi)$ as well and thus the sequence of inclusions $N \subset \ker(\pi) \subset F(S)$ yields a surjective homomorphism $F(S)/N \to F(S)/\ker(\pi) = G$.

Set $\tilde{G} = F(S)/N$. Write $\tilde{g}_i$ for the images of the elements of S in $\tilde{G}$. Since these elements generate $\tilde{G}$ by definition, it follows that $|\tilde{G}| \geq |G|$. On the other hand, since N is defined to impose precisely the multiplication rules in G, it follows that the collection of elements $\{\tilde{g}_i\}_{i \in I}$ is closed under multiplication in $\tilde{G}$ (i.e., $\tilde{g}_i \tilde{g}_j = \tilde{g}_k$). Therefore, $|\tilde{G}| \leq |G|$. Thus, we conclude $|G| = |\tilde{G}|$ and since $\tilde{G} \to G$ is a bijective group homomorphism, it must be an isomorphism. □

Definition 1.5.4.5. Given two groups G_1 and G_2 with presentations $G_1 = \langle S_1 | R_1 \rangle$, and $G_2 = \langle S_2 | R_2 \rangle$, the coproduct $G_1 * G_2$ is the group $\langle S_1 \cup S_2 | R_1 \cup R_2 \rangle$.

Remark 1.5.4.6. Sometimes this is called the *free product with amalgamation* or *the amalgamated sum*; we prefer the sum terminology for reasons we will explain shortly.

More generally, we have the following definition.

Definition 1.5.4.7. Suppose $\varphi : F \to G$ and $\psi : F \to H$ are two group homomorphisms. Suppose we have presentations of G and H. The amalgamated free product $G *_F H$ is the quotient of $G * H$ by the normal subgroup generated by the elements $\{\varphi(f)\psi(f)^{-1} | f \in F\}$.

1.6 Lecture 6: Orders of elements

1.6.1 Subgroups of free groups

Lemma 1.6.1.1. *Every subgroup of the free group on a single generator is free. More precisely, if we fix an isomorphism $F(e) \cong \mathbb{Z}$, then every subgroup of $\mathbb{Z}$ is of the form $\langle m \rangle$ for some $m \in \mathbb{Z}$.*

Proof. Suppose $H \subset \mathbb{Z}$ is a subgroup. Because $\mathbb{Z}$ is ordered, H is ordered. Now, either $H = 0$ or there is a smallest non-zero integer $m \geq 0$ such that $m \in H$. We claim that $H = m\mathbb{Z}$. If $m = 1$, then $H = \mathbb{Z}$, and there is nothing to check. Therefore, assume $m \geq 2$. If $h \in H$, then $h = n$ for some integer n. Now, since H is a subgroup, multiplying n by multiples of m (i.e., subtracting am from n for some integer a) we see that $n - am$ is also an element of H for every integer a. Now, for suitable choice of a, we have $0 \leq n - am < m$. If $n - am \neq 0$, this contradicts the minimality of m. Therefore, $n = am$.

If $m \neq 0$, the subgroup $m\mathbb{Z}$ is equal to the subgroup generated by m, so $m\mathbb{Z}$ is itself free. If $m = 0$, recall that the trivial group is the free group on the empty set. □

Example 1.6.1.2. It follows from this result that every element has an order. If G is any group, and $g \in G$ is an element, then there is a homomorphism $\mathbb{Z} \to G$ defined by sending $1 \in \mathbb{Z}$ to $g \in G$. The kernel of this group homomorphism is, by the previous lemma, either trivial or equal to the subgroup $m\mathbb{Z}$ for some positive integer m. If the integer $m = 1$, then the element g is necessarily the identity. If $m = 0$, then the element g is said to have infinite order. If m is an integer ≥ 2, then the element g is said to have order m. Indeed, in this case, the group $\langle g \rangle$ is a subgroup of G of order m. The order of an element $g \in G$ will be denoted $ord(g)$.

Example 1.6.1.3. The quotient groups $\mathbb{Z}/m\mathbb{Z}$ are the cyclic groups of order m. These groups have the presentation $\langle x | x^m \rangle$.

Corollary 1.6.1.4. *If G is a finite group, and $g \in G$, the $ord(G) || G|$.*

Proof. If G is finite, then $\langle g \rangle$ is a subgroup of G, and the result follows from the counting formula. □

Corollary 1.6.1.5. *If p is a prime number, and G is a finite group of order p, then $G \cong \mathbb{Z}/p$.*

Proof. We already saw that every subgroup of G is either the trivial group or the whole group. Thus, if we fix an element $x \in G$, then $\langle x \rangle$ is either the trivial group or the whole group. If $x \neq e$, then $\langle x \rangle = G$ and since G is finite, it follows that $x^p = e$. □

Theorem 1.6.1.6 (Nielsen-Schreier theorem)**.** *Every subgroup of a free group is free.*

Proof. While it is possible to give a "combinatorial" proof of this result, one of the most intuitively satisfying (in my mind) is topological and involves covering space theory. In brief, using the van Kampen theorem, one sees that the free group on some number of generators can be realized as the fundamental group on a wedge sum of circles. The statement that subgroups of free groups are free corresponds to the topological observation that any covering space of a wedge of circles is again a wedge of circles. □

Chapter 2

Abelian groups

2.1 Lecture 6 bis: Free and finite abelian groups

In this lecture, we begin a more detailed analysis of abelian groups. We begin by analyzing simple abelian groups and finite abelian groups. Our eventual goal is to understand finitely generated abelian groups.

2.1.1 Free abelian groups

Just as free groups were characterized above using a universal property, there is a corresponding universal property for maps from a set to an *abelian group*.

Definition 2.1.1.1. If S is a set, then a *free abelian group on* S is a pair $(i, \mathbb{Z}[S])$ consisting of an abelian group $\mathbb{Z}[S]$ and a function $i : S \to \mathbb{Z}[S]$ such that given any abelian group A and a function $f : S \to A$, there is a unique homomorphism $\mathbb{Z}[S] \to A$ factoring f.

As before, it follows immediately from the definition that if free abelian groups exist, then they give rise to a functor $\mathbb{Z}[-]$ from $\mathbf{Set}$ to $\mathbf{Ab}$ (the category of abelian groups). Moreover, one checks exactly as before that this functor is left adjoint to the forgetful functor from abelian groups to sets. To establish the existence of free abelian groups, one may simply repeat the construction of Theorem 1.5.2.3 replacing "group" everywhere by "abelian group." We leave the task of elucidating these results to the reader. Instead, we simply observe that the free abelian group $\mathbb{Z}[S]$ may be constructed as the direct product $\prod_{s \in S} \mathbb{Z}$.

Note, in particular, that if A is any abelian group, then a choice of a set S of generators for A determines a surjection $\mathbb{Z}[S] \to A$. In particular, any finitely generated abelian group is a quotient of a product of finitely many copies of $\mathbb{Z}$. Note that if A is a finitely presented abelian group, then A is the cokernel of a map $\mathbb{Z}^m \to \mathbb{Z}^n$. Thus, the problem of classifying finitely presented abelian groups can be rephrased in terms of normal forms of integer matrices. In fact, we will see that every finitely generated abelian group is automatically finitely presented, and we will also see that subgroups of free abelian groups are automatically free abelian.

2.1.2 Structure of finite abelian groups

Let us begin by trying to understand simple abelian groups.

Lemma 2.1.2.1. *Any simple abelian group is a finite cyclic group.*

Proof. Indeed, suppose A is a simple abelian group and $x \in A$ is a non-identity element. If $x \in A$, then $\langle x \rangle$ is a subgroup of A, which is normal since A is abelian. Since A is simple, the subgroup is either trivial or equal to A. Since x is a non-identity element, it follows that $A = \langle x \rangle$. If $ord(x)$ is infinite, then $A \cong \mathbb{Z}$ and we saw in Lemma 1.6.1.1 that $\mathbb{Z}$ has non-trivial subgroups. Therefore, $ord(x)$ must be finite. □

If G is any group, then we can consider the n-th power function $x \mapsto x^n$. An element $x \in G$ is said to have *exponent* n if $x^n = e$. The exponent of a group G is the smallest natural number n such that $x^n = e$ for every $x \in G$.

The n-th power map is not a homomorphism in general. For $n = 2$, $(xy)^2 = x^2y^2$ if and only if $xy = yx$ for every $x, y \in G$. On the other hand, note that if G is a finite group of exponent m, then the m-th power map *is a homomorphism*. However, if A is an abelian group, then the n-th power map is always a group homomorphism. We introduce two pieces of notation related to the n-th power map on abelian groups.

Definition 2.1.2.2. If A is an abelian group and n is an integer, then the *n-torsion subgroup of A*, denoted ${}_nA \subset A$, is the kernel of the n-th power map. The quotient of A by the image of the n-th power map will be denoted A/nA.

Elementary facts about primeness allow us to separate finite abelian groups into factors depending only on a prime p. If p and q are coprime integers, then consider the cyclic group $\mathbb{Z}/pq$. The multiples of p determine a subgroup isomorphic to $\mathbb{Z}/q\mathbb{Z}$ and the multiples of q determine a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z}$. We may define a map $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z}$ by sending $(1, 1)$ to 1. This map is evidently surjective and one may construct an explicit inverse by observing that since p and q are coprime, we may find integers x and y such that $px + qy = 1$. The generalization of this fact for an arbitrary (not necessarily cyclic) finite abelian group is the following lemma.

Lemma 2.1.2.3. *If A is a finite abelian group of order m and $m = rs$ with r and s coprime, then the product map ${}_rA \times {}_sA \to A$ is an isomorphism.*

Proof. The product map is a group homomorphism since A is abelian. Thus to prove that the map is an isomorphism, it suffices to check that it is bijective.

First, let us observe that the intersection of the two subgroups in question is precisely the trivial group since r and s are coprime. From this, we deduce that the product map is injective. Indeed, if (x, y) is an element of the product such that $xy = e$, then $x = y^{-1}$, which means that both x and y lie in the intersection (which is a subgroup).

Second, we show that the product map is surjective, i.e., given any element of A, we may write A as the product of an r-torsion or s-torsion element. Now, if $x \in A$, the order d of x divides m. Since $d \leq m$ and since $d|m$, either $d = m$ or $d < m$ and d divides either r or s (but not both). In the latter case, the element x lies in the r-torsion subgroup or the s-torsion subgroup and therefore it lies in the image of the product map.

Thus, it remains to treat the case where $d = m$. In that case, $\langle x \rangle$ generates a cyclic subgroup of order m and we may appeal to the discussion before the proof. Observe that x^r is an s-torsion element and x^s is an r-torsion element. Then, we choose a and b such that $ar + bs = 1$. It follows that $x^{ra}(x^s)^b = x^{ar}x^{bs} = x^{ar+bs} = x$ and we thus obtain a lift of x. □

Writing the order of an abelian group A as a product of prime powers and applying inductively to the preceding lemma, one immediately deduces the following result.

Corollary 2.1.2.4. *If A is a finite abelian group of order m and $m = q_1 \cdots q_n$ where $q_i = p^{a_i}$ are the distinct prime powers appearing in a factorization, then the product map*

$$\prod_i {}_{q_i}A \longrightarrow A$$

is an isomorphism.

This result is sometimes referred to as *primary* decomposition of A, and the factors that appear are called the p-primary components. Since any finite abelian group can be decomposed as a product of factors, each of which has prime power order, it remains to analyze groups of prime power order. Observe that the groups ${}_{q_i}A$ can, in general, be further decomposed since ${}_{q_i}A$ could itself be a product of groups of different powers of a fixed prime (e.g., $\mathbb{Z}/4 \times \mathbb{Z}/2$).

2.2 Lecture 7: Mostly finitely generated groups

In this lecture, we'll prove a few refinements of the result we stated at the end of last class.

2.2.1 Finite abelian groups

At the end of the last lecture, we established primary decomposition for finite abelian groups. We also note that, in general, the p-primary components may be further refined. For abelian groups, the direct product is also a coproduct in the categorical sense, so when we speak of abelian groups, we can speak of direct sums instead of direct products.

Theorem 2.2.1.1. *Suppose A is a finite abelian group, then A is a direct sum of cyclic groups.*

There are several ways to think about this result. First, suppose we pick generators for A, i.e., we write A is a quotient of a finite-rank free abelian group $\mathbb{Z}^{\oplus n}$. The idea of the proof of Theorem 2.2.1.1 is simple: we pick an arbitrary generating set of A and we would like to modify this generating set in a suitable way to obtain the cyclic decomposition of A. The kernel of this homomorphism is a normal subgroup of $\mathbb{Z}^{\oplus n}$, for which we may again choose generators (in fact, this subgroup is again free, and, moreover, as we will see, is also finitely generated). Thus, the homomorphism can be viewed as the cokernel of a suitable matrix with integer coefficients. Thus, the theorem above amounts to a "normal form" for matrices with integer coefficients. Note that if A is an abelian group, we write $+$ for the group operation and 0 for the identity element. The m-th power map is a homomorphism, and we write ma for the m-th power of A. With this notation, and based on the linear algebra analogy, we introduce the following notion (which is a direct parallel of the notion of a basis of a vector space).

Definition 2.2.1.2. If A is an abelian group, a subset $x_1, \ldots, x_n$ of A is called *a basis* of A if

- $\langle x_1, \ldots, x_n \rangle = A$, and
- given an equation of the form $\sum_i m_i x_i = 0$, with $m_i \in \mathbb{Z}$, it follows that $m_i x_i = 0$ for each i.

The following result is essentially an exercise in unwinding the definitions.

Lemma 2.2.1.3. *If A has a basis $x_1, \ldots, x_n$, then $A \cong \langle x_1 \rangle \times \cdots \times \langle x_n \rangle$.*

Proof. As before, the product map $\langle x_1 \rangle \times \cdots \times \langle x_n \rangle \to A$ is a group homomorphism. It is surjective because $x_1, \ldots, x_n$ generate A. It is injective because of the definition of a basis. □

We now establish a lemma about changing bases.

Lemma 2.2.1.4. *Suppose A is generated by $x_1, \ldots, x_n$. For any $c_1, \ldots, c_n$ with $gcd(c_1, \ldots, c_n) = 1$, there exist generators $y_1, \ldots, y_n$ of A with $y_1 = c_1 x_1 + \cdots + c_n x_n$.*

Proof. Without loss of generality, we may assume $c_i \geq 0$ (replacing x_i by its inverse if necessary). We argue by induction on $c_1 + \cdots + c_n = s$. If $s = 1$, then at most c_1 is non-zero and the result is immediate. Thus, assume $s > 1$. In that case, at least 2 of the c_i are non-zero and by reordering the x_i if necessary, without loss of generality we may assume $c_1 \geq c_2 > 0$. Now, observe that $\{x_1, x_1 + x_2, x_3, \ldots, x_n\}$ also generates A, $gcd(c_1 - c_2, c_2, c_3, \ldots, c_n) = 1$ and $(c_1 - c_2) + c_2 + \cdots + c_n < s$.

Thus, by induction, there exist generators $y_1, \ldots, y_n$ such that

$$\begin{aligned} y_1 &= (c_1 - c_2)x_1 + c_2(x_1 + x_2) + c_3 x_3 + \cdots + c_n x_n \\ &= c_1 x_1 + \cdots + c_n x_n, \end{aligned}$$

which is precisely what we wanted to show. □

Proof of Theorem 2.2.1.1. The following argument is apparently due to Kronecker, though I learned it from Milne's notes. We argue by induction on the number of generators. If A has a single generator, then we already showed that any quotient of $\mathbb{Z}$ is cyclic. Thus, assume that A has a generating set consisting of some fixed number $r > 1$ generators. Consider the collection of all generating sets $\{x_1, \ldots, x_r\}$ for A with exactly r elements (by assumption, there is at least 1). Among these, there is a generating set for which the order of x_1 is as small as possible. We will show that $A \cong \langle x_1 \rangle \oplus \langle x_2, \ldots, x_r \rangle$. This will complete the proof since $\langle x_2, \ldots, x_r \rangle$ is generated by fewer elements, and the induction hypothesis guarantees that it is isomorphic to a finite direct product of cyclic groups.

Assume to the contrary that A is not the direct sum of $\langle x_1 \rangle$ and $\langle x_2, \ldots, x_k \rangle$. This means that the intersection of $\langle x_1 \rangle$ and $\langle x_2, \ldots, x_k \rangle$ in A is non-empty. In other words, there exist integers $m_1, \ldots, m_r$ such that $m_1 x_1$ can be written as $\sum_{i=2}^{r} m_i x_i$ with $m_1 \neq 0$, or equivalently (after changing the sign of m_i if necessary), there exists a relation in A of the form

$$m_1 x_1 + \cdots + m_r x_r = 0$$

with $m_1 x_1 \neq 0$. After replacing some of the x_i by their inverses if necessary (which does not affect whether $x_1, \ldots, x_r$ generates A), we may suppose that $m_i > 0$ for every i. Without loss of generality, we may also suppose that $m_1 < ord(x_1)$.

Let $d = gcd(m_1, \ldots, m_r) > 0$, and let $c_i = \frac{m_i}{d}$ (note that $gcd(c_1, \ldots, c_r) = 1$). We claim that, in this case, there exists a generating set $y_1, \ldots, y_r$ such that $y_1 = c_1 x_1 + \cdots + c_r x_r$ (we prove this in Lemma 2.2.1.4). Assuming this, observe that

$$dy_1 = dc_1 x_1 + \cdots dc_r x_r = m_1 x_1 + \cdots + m_r x_r = 0.$$

However, $d \leq m_1 < ord(x_1)$. Thus, we have obtained a generating set $y_1, \ldots, y_r$ where y_1 has order smaller than $ord(x_1)$, which contradicts the minimality assumption regarding the order of x_1. Thus, there can exist no relation in A of the stated form. □

Remark 2.2.1.5. In particular, applying the above result to the p-torsion summand of a finite abelian group, we conclude that any finite abelian group of prime power order is a direct sum of cyclic groups of prime power order.

One major downside of this proof is that it is non-constructive: if you start with a given collection of generators, it is unclear how to turn it into a basis; this deficiency can be eliminated with some more work. One benefit of our proof of Theorem 2.2.1.1 is that applies essentially verbatim to arbitrary finitely generated abelian groups (one need only contemplate what happens if $ord(x_1)$ is infinite). You will likely come back to this question in 510B. The above result may also be refined to tell you something about uniqueness of the resulting decomposition.

Theorem 2.2.1.6. *Every finitely generated abelian group is the product of cyclic groups.*

2.2.2 Infinitely generated abelian groups I: divisible groups

Many abelian groups that are not finitely generated appear in nature. For example, the abelian group underlying the field of rational numbers $\mathbb{Q}$ is not a finitely generated abelian groups, or any infinite direct product of cyclic groups (thus, the same holds for the abelian group underlying any field having characteristic 0). New phenomena appear in the structure of infinitely generated abelian groups.

Lemma 2.2.2.1. *The addtive group of rational numbers $\mathbb{Q}$ is not isomorphic to a direct product of cyclic groups.*

Proof. To establish this result, we begin by isolating a key property of the additive group of rational numbers. For any $r \in \mathbb{Q}$, and any non-zero natural number n, the equation $r = nr'$ has a unique r' as solution: namely r/n. Equivalently, the n-th power map is a bijection for any non-zero natural number n.

On the other hand, if A is a cyclic group, then the n-th power map is not always a bijection. For example, when $A = \mathbb{Z}$ the n-th power map is not surjective (though it is injective), and if $A = \mathbb{Z}/m\mathbb{Z}$, then the n-th power map need not be either surjective or injective in general. More generally, the n-th power map in an arbitrary direct product of cyclic groups, being defined componentwise, has the same property. □

We turn the divisibility property into a definition.

Definition 2.2.2.2. If p is a prime number, an abelian group A is called *p-divisible*, *p-torsion free*, or *uniquely p-divisible* if the p-th power map $A \to A$ is surjective, injective, or bijective. More generally, if S is a set of prime natural numbers, then A is called *(uniquely) S-divisible*, if it is (uniquely) p-divisible for every $p \in S$ or *S-torsion free*, if it is p-torsion free for every $p \in S$. In the special case where $S = P$ is the set of all prime natural numbers, (uniquely) P-divisible groups are called *(uniquely) divisible* and P-torsion free groups are called *torsion free*.

Example 2.2.2.3. The rational numbers are uniquely divisible by this definition.

Example 2.2.2.4. Any product of copies of $\mathbb{Z}$ provides a torsion free group that is not divisible.

We now give some examples of divisible groups that are *not* torsion free.

Example 2.2.2.5. There is an injection $\mathbb{Z} \hookrightarrow \mathbb{Q}$. The quotient group $\mathbb{Q}/\mathbb{Z}$ is sometimes called the additive group of rationals "modulo 1". Observe that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order. Indeed pick a representative of $\bar{r} \in \mathbb{Q}/\mathbb{Z}$ by a fraction $r = \frac{p}{q}$ in lowest terms. In that case $qr = p$, which is an integer and therefore lies in the coset $e + \mathbb{Z}$, i.e., is 0 in $\mathbb{Q}/\mathbb{Z}$. The group $\mathbb{Q}/\mathbb{Z}$ is divisible. Indeed, given $\bar{r}$ and an element r as above lifting it, then the coset $\bar{r}' := r/n + \mathbb{Z}$ gives a class with $n\bar{r}' = \bar{r}$. An analogous argument can be used to show that any quotient of a divisible group is divisible.

Example 2.2.2.6. Fix a prime number p, and let $\mathbb{Z}[1/p]$ denote the subgroup of $\mathbb{Q}$ consisting of rational numbers whose denominators are a power of p. Again, there is an inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[1/p]$, and we write $\mathbb{Z}[1/p]/\mathbb{Z}$ for the quotient. Note that $\mathbb{Z}[1/p] \subset \mathbb{Q}$, and therefore, $\mathbb{Z}[1/p]/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$. Since the denominators of $\mathbb{Z}[1/p]$ are powers of p, it follows that every element of $\mathbb{Z}[1/p]/\mathbb{Z}$ has order p^n for some integer n. In fact, we may identify $\mathbb{Z}[1/p]/\mathbb{Z}$ as the p-torsion subgroup of $\mathbb{Q}/\mathbb{Z}$. Thus, there exists a chain of subgroups

$$_p\mathbb{Z}[1/p]/\mathbb{Z} \subset {}_{p^2}\mathbb{Z}[1/p]/\mathbb{Z} \subset \cdots \subset {}_{p^n}\mathbb{Z}[1/p]/\mathbb{Z} \subset \cdots .$$

Each inclusion here is strict as we can always find an element that has order p^n but not p^{n-1} by taking a representative with denominator p^n.

In fact, we can be more precise. The subgroup $_p\mathbb{Z}[1/p]/\mathbb{Z}$ is a cyclic subgroup of order p generated by $\frac{1}{p}$, and, more generally, $_{p^n}\mathbb{Z}(p^\infty)$ is a cyclic subgroup of order p^n generated by $\frac{1}{p^n}$. In any case, we get an ascending chain of (finite) subgroups which never terminates. The group $\mathbb{Z}[1/p]/\mathbb{Z}$ is thus p-divisible but evidently not p-torsion free. In fact, one can show that $\mathbb{Z}[1/p]/\mathbb{Z}$ is divisible.

2.3 Lecture 8: Infinitely generated groups continued: torsion and divisibility

2.3.1 Sums and products

Earlier, we defined the Cartesian product of an arbitrary set of groups (Lemma 1.1.2.1 and the surrounding discussion). We now observe that there is a "smaller" subgroup that is frequently useful; this construction makes sense in the category of abelian groups.

Lemma 2.3.1.1. *If I is a set, and A_i is a family of abelian groups indexed by I, then the subset of $\prod_{i \in I} A_i$ consisting of elements $(a_i)_{i \in I}$, where all but finitely many a_i are equal to the identity element is a subgroup.*

Definition 2.3.1.2. If I is a set, and A_i is a family of abelian groups indexed by I, then the direct sum $\bigoplus_{i \in I} A_i$ is the subgroup of $\prod_{i \in I}$ consisting of elements $(a_i)_{i \in I}$, where all but finitely many a_i are equal to the identity element.

Remark 2.3.1.3. Of course, if I is a finite set, the inclusion of the direct sum into the direct product is an isomorphism. The difference between the two notions appears when I is infinite. When we investigate infinitely generated groups in more detail, the difference between the two notions will be important.

Example 2.3.1.4. The direct sum of abelian groups is a coproduct in the category $\mathbf{Ab}$ in the sense of Definition A.1.2.24.

One use for the notion of direct sum of abelian groups is the following result, which formalizes and generalizes an observation we've used repeatedly.

Lemma 2.3.1.5. *Suppose A is a group, and $\{A_i\}_{i \in I}$ is a family of subgroups of A. The function sending $(a_i)_{i \in I}$ to $\prod_{i \in I} a_i$ gives rise to a homomorphism $\bigoplus_{i \in I} A_i \to A$.*

Proof. The product homomorphism makes sense because of the very definition of $\bigoplus_{i \in I} a_i$: only finitely many elements are non-zero. □

Remark 2.3.1.6. Observe that there is no corresponding construction when we consider infinite products because it does not in general make sense to take the product of infinitely many elements of an (abelian) group!

2.3.2 Structure theory for torsion groups

Lemma 2.3.2.1. *If A is an abelian group, then given any two elements x and y of finite order, the product xy also has finite order (equal to the least common multiple of the orders of x and y).*

As a consequence, the subset of A consisting of elements of finite order is necessarily a subgroup of A. If p is a prime number, then the subset of A consist of elements whose order is a power of p is also a subgroup of A.

Definition 2.3.2.2. If A is an abelian group, then A_{tor} is the subgroup consisting of all elements of finite order. An abelian group A is called a *torsion group* if $A = A_{tor}$, i.e., every element has finite order. If p is a prime number, then the subset $A_p \subset A$ consisting of elements whose order is a power of p is called the p-primary subgroup of A. An abelian group is called *p-primary* if $A = A_p$, i.e., every element of A has order that is a power of p.

Example 2.3.2.3. The notion of torsion group is most interesting when A is not finitely generated. Indeed, any finitely generated torsion group is necessarily a finite group.

Lemma 2.3.2.4. *If A is an abelian group, then A/A_{tor} is a torsion free abelian group.*

In the case where A is no longer finitely generated, we saw in Example 2.2.2.6 that the order of elements can grow without bound. Nevertheless, primary decomposition as in Corollary 2.1.2.4 may be salvaged.

Theorem 2.3.2.5. *If A is a torsion abelian group, then A is a direct sum of p-primary groups.*

Proof. Let A be an abelian group, and for every prime p, consider the p-primary subgroup $A_p \subset A$. We shall now prove that A is isomorphic to the direct sum of the subgroups A_p. First, observe that the product map $\oplus_p A_p \to A$ is a group homomorphism by Lemma 2.3.1.5 (this is the first place where we use the fact that we work with the direct sum since the product of infinitely many elements does not make sense in general).

We now show that the product map is a surjection. To this end, it suffices to show that A is the union of the subgroups A_p. Take any $x \in A$, say of order n. Factor n into prime powers: $n = p_1^{r_1} \cdots p_k^{r_k}$ and write $n_i = \frac{n}{p_i^{r_i}}$. Thus, $n_1, \ldots, n_k$ have greatest common divisor 1 and so there exist integers $a_1, \ldots, a_k$ with $a_1 n_1 + \cdots a_k n_k = 1$. Then,

$$x = a_1 n_1 x + \cdots + a_k n_k x.$$

Now $n_i x$ has order $p_i^{r_i}$ and so it is in A_{p_i}. Thus, the above equation is the desired expression of x as a sum of (finitely many) elements of the A_p.

To establish injectivity, it suffices to establish uniqueness of the expression just found (this amounts to showing that the intersection of the p-primary subgroups is the trivial subgroup). To this end, suppose $x = y_1 + \cdots + y_k$ and $z_1 + \cdots + z_k$, where $y_i, z_i \in A_{p_i}$. Consider the equation

$$y_1 - z_1 = (z_2 + \cdots + z_k) - (y_2 + \cdots + y_k).$$

We know that $y_1 - z_1$ has order a power of p_1. On the other hand, the right hand side is an element whose order is a product of powers of $p_2, \ldots, p_k$. This is only possible if $y_1 - z_1 = e$, i.e., $y_1 = z_1$. Similarly, $y_i = z_i$ for each i. □

2.3.3 Divisible subgroups are direct summands

Having described some structural results for torsion groups, we now analyze the structure of divisible groups in greater detail. The following result describes a feature of divisible groups that is not shared by abelian groups in general. In general, given a short exact sequence of abelian groups

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A/A' \longrightarrow 0$$

there is no reasonable way to identify A/A' as a subgroup of A, i.e., to describe a map $A/A' \to A$ such that the composite $A/A' \to A \to A/A'$ is the identity (such a map is called a *splitting* of the short exact sequence). For example, consider $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ where the map from $\mathbb{Z}$ to itself is multiplication by 2. Since every element of $\mathbb{Z}$ has infinite order, there is no non-trivial homomorphism $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ and in particular, no splitting of the relevant short exact sequence. The situation for divisible groups is different. For example, consider the inclusion $\mathbb{Z}[1/p]/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ we described before. The former consists of p-primary torsion in the latter and we can naturally identify the quotient with the *prime to* p-torsion in $\mathbb{Q}/\mathbb{Z}$. The following result is a vast generalization of this observation.

Theorem 2.3.3.1. *A divisible subgroup of an abelian group is a direct summand, i.e., if A is an abelian group, and $D \subset A$ is a divisible subgroup, then there exists a subgroup $K \subset A$ such that the multiplication map $D \oplus K \to A$ is an isomorphism. In particular, the composite map $K \to A \to A/D$ is an isomorphism and the short exact sequence $0 \to D \to A \to A/D \to 0$ is split.*

Proof. Let A be an abelian group, and suppose $D \subset A$ is a divisible subgroup. We use additive notation, so we write 0 for the unit in A. Our goal is to find a subgroup $K \subset A$ such that $D \cap K = 0$ and such that $DK = A$ (we abuse terminology and write DK instead of $D + K$ for the image of the product homomorphism $D \oplus K \to A$).

To construct the subgroup suggested in the previous paragraph, let us begin by trying to construct a subgroup K of A that is disjoint from D, i.e., such that $D \cap K = 0$. Consider the set S of all subgroups L of A that satisfy $D \cap L = 0$. The set S is non-empty because it contains the trivial subgroup. Note also that the set S is partially ordered with respect to set-theoretic inclusion. The key new idea in this proof is to use Zorn's lemma: if S is a partially ordered set in which every chain has a least upper bound, then S has a maximal element.

To apply Zorn's lemma, we will show that every chain in S has a least upper bound. Suppose $\{L_i\}$ is a chain of subgroups in S. Take the set-theoretic union of $\cup_i L_i \subset A$ and call it H. We have to show that (i) H is a subgroup, (ii) $H \cap D = 0$, and H is the least upper bound of the L_i. The final statement follows immediately from the previous two. For (i), i.e., to see that H is a subgroup, take x and y in H: it suffices to show that $x - y$ lies in H (since then H is closed under both addition and inversion). Now, to say that x is in H is to say that there is some L_i with $x \in L_i$ and likewise, $y \in L_j$. However, we know that $L_i \subset L_j$ (or vice versa), so either both x and y are in L_i or both are in L_j. Thus, $x - y \in L_i$ (or L_j). To see that $D \cap H = 0$, simply observe that since any $x \in H$ lies in some L_i, it follows also that if $x \in D \cap H$, then $x \in D \cap L_i = 0$.

The hypotheses of Zorn's lemma being satisfied, we know that the set S has a maximal element, and we write K for the maximal subgroup of A that is disjoint from D. To complete the proof, it suffices to show that $DK = A$. Since A is abelian, it is straightforward to check that DK is itself a subgroup of A that contains D and K.

Assume to the contrary that $DK \neq A$, i.e., there exists an element $x \in A$ such that $x \notin DK$. Since D and K are subgroups of DK, it follows that x is neither in D nor in K. Since x does not lie in K, we can form the subgroup K_1 generated by K and x. By construction, K is a proper subgroup of K_1 consisting of elements of the form $k + nx$ where $k \in K$ and $n \in \mathbb{Z}$.

Since K is maximal with respect to the property of being disjoint from D, we know that $D \cap K_1$ must contain a non-zero element d. The element $d = k + nx$, i.e., $nx = d - k$. Since $k \in K$ and $d \in D \cap K_1 \subset D$, this means $nx \in DK$.[1] Since we know that $nx \in DK$ for some $n \in \mathbb{Z}$, we can pick the smallest positive such n. Since x is not in DK by assumption, we can assume that $n > 1$ without loss of generality. Therefore, there exists a prime number p dividing n. Fixing such a prime p, we set $y = (n/p)x$. By minimality of n, we conclude that y also must not lie in DK. On the other hand, $py = nx = d - k$ does lie in DK. Since D is divisible, we can write $d = pd'$ for some $d' \in D$. Thus, $py = pd' - k$, i.e., $p(d' - y) = k$. Set $z = d' - y$. If $z \in DK$, then $z - d' \in DK$ as well, so y would also lie in DK, so we conclude that z does not lie in DK, though $pz \in K$.

Now, we repeat the argument: consider the subgroup K_2 of A generated by K and z. Every element of this subgroup is of the form $k + mz$ for $k \in K$ and $m \in \mathbb{Z}$. Again, the fact that K is maximal with respect to the property of being disjoint from D and the fact that K_2 contains K as a proper subgroup implies that $K_2 \cap D$ must contain a non-trivial element d''. Write $d'' = k' + mz$ where $k' \in K$. If m is divisible by p, then since $k' \in K$, and $d'' = k' + mz = k' + (m/p)pz \in K$, which contradicts our definition of d'', so we may assume m is coprime to p. If m is coprime to p, then we may find integers a and b such that $am + bp = 1$. Then, $z = amz + bpz$. However, $mz = d'' - k'$ and is therefore in DK while $bpz = b(k)$,

[1] The last statement can be rephrased as follows: given any element x in A lying outside of DK, there exists an integer n such that nx is trivial in the quotient A/DK. So far, divisibility has not been used (!), and what we have proven can be summarized as this: given any subgroup H of an abelian group A, then: (i) there exists a subgroup K of A that is maximal with respect to the property of being disjoint from H (i.e., $H \cap K = 0$), and (ii) the quotient A/HK is a torsion group.

which is also in K. Thus, we conclude that z was in DK to begin, which is a contradiction. Since we only assumed that $DK \neq A$ to construct z, we conclude that $DK = A$, which is what we wanted to prove. □

2.3.4 Properites of divisible groups

Lemma 2.3.4.1. *Suppose G and H are abelian groups.*

i) If G is divisible and H is a subgroup of G, then G/H is divisible; more generally, any homomorphic image of a divisible group is divisible.

ii) If H is a divisible subgroup of G, then $G \cong G/H \times H$.

iii) If H is a divisible subgroup of G, J is any abelian group, and $\varphi : H \to J$ is any homomorphism, then φ extends to a homomorphism $\hat{\varphi} : G \to J$.

iv) Any product of divisible groups is divisible; any sum of divisible groups is divisible. Conversely, a product (or sum) of groups is divisible only if the factors are divisible.

v) If G is torsion free and divisible (i.e., uniquely divisible), then G has the structure of a $\mathbb{Q}$-vector space.

Proof. For (i), if $f : G \to G'$ is a homomorphism with G divisible, then given $\bar{x} \in im(f)$, we can pick $x \in G$ lifting x. Since G is divisible, given any integer n, we can find $y \in G$ with $ny = x$. Then, since f is a homomorphism, it follows that $\bar{x} = f(ny) = nf(y)$, and $\bar{y} = f(y)$ witnesses the divisibility of $\bar{x}$.

For (ii), we already know that H is a summand of G by appeal to Theorem 2.3.3.1, i.e., $G \cong H \oplus K$ for some subgroup $K \subset G$. Now, observe that the inclusion map $K \to H \oplus K \cong G \to G/H$ yields a homomorphism $K \to G/H$, and the isomorphism theorems imply that this map yields the required isomorphism.

For (iii), observe that $G \cong H \oplus G/H$ by (ii) and $H \oplus G/H \cong H \times G/H$. Therefore, any homomorphism $H \to J$ can be extended by means of the composite $H \oplus G/H \to H \to J$.

For (iv), a witness to divisibility can be constructed by "dividing" component-wise. If one of the factors is not divisible, then the product cannot be divisible.

For (v), given a uniquely divisible group, we need to define scalar multiplication by $r \in \mathbb{Q}$. Express r as p/q (in lowest terms). Then, given $x \in G$, there is a unique x' such that $qx' = x$. We then define rx as px'. We now check that scalar multiplication distributes over addition. Again, uses uniqueness of the element witnessing divisibility: if $x = x_1 + x_2$, then since there are unique elements x_1' and x_2' such that $qx_1' = x_1$ and $qx_2' = x_2$; the result then follows because the p-th power map is a homomorphism. The other axioms can be checked similarly. □

Lemma 2.3.4.2. *Every abelian group is a subgroup of a divisible group.*

Proof. Write $G = F/R$ where F is free abelian. Now, F is a direct sum of copies of $\mathbb{Z}$ and therefore embeds in the corresponding direct sum of copies of $\mathbb{Q}$. Now, R is embedded in a direct sum of copies of $\mathbb{Q}$ and it follows that G embeds in the quotient of this sum of copies of $\mathbb{Q}$ by R. Since any quotient of a divisible group is divisible, this provides the required embedding. □

Corollary 2.3.4.3. *A group G is divisible if and only if it is a direct summand of any group in which it is contained.*

Proof. One direction is the theorem established last time. For the other direction, assume G is a direct summand of any group in which it is contained. Embed G in a divisible group D (this can be accomplished by means of the previous lemma). Then, since G is a summand of D, it follows that G is divisible, since any summand of a divisible group is divisible. □

2.4 Lecture 9: Divisibility and Injectivity

2.4.1 The structure theorem for divisible groups

Lemma 2.4.1.1. *Suppose D is a divisible abelian group. The following statements hold:*

- *D_{tor} and the p-primary components of D are divisible subgroups of D;*
- *$D \cong D_{tor} \times D/D_{tor}$ and D/D_{tor} is uniquely divisible.*

Proof. For (i): given $x \in D_{tor}$, and $n \in \mathbb{Z} \neq 0$ we can find $x' \in D$ such that $x = nx'$. If $ord(x) = m$, then $mx = 0$. Then, $m(nx') = mn(x') = 0$, which means that x' is also in the torsion subgroup. Now, any torsion group is a direct sum of its p-primary components by Theorem 2.3.2.5. Therefore, since direct summands of divisible groups are divisible by Lemma 2.3.4.1(iv), we also conclude that all p-primary subgroups of D are divisible.

Since D_{tor} is a divisible subgroup of D, it follows that $D \cong D_{tor} \times D/D_{tor}$ by Lemma 2.3.4.1(ii). On the other hand, D/D_{tor} is torsion free by Lemma 2.3.2.4 and divisible by Lemma 2.3.4.1(i). We conclude by observing that uniquely divisible groups are precisely torsion free divisible groups by definition. □

We already know that D/D_{tor} is a $\mathbb{Q}$-vector space by Lemma 2.3.4.1(v). By choosing a basis, we see that D/D_{tor} is a direct sum of (possibly infinitely many) copies of $\mathbb{Q}$; thus D/D_{tor} is fairly well understood. To better describe D_{tor}, we proceed to analyze its p-primary subgroups in greater detail.

2.4.2 Prufer groups: the structure theorem completed

Recall the group $\mathbb{Z}[1/p]/\mathbb{Z}$ described in Example 2.2.2.6; this group is frequently called the *Prufer p-group* or the *p-quasicyclic group*. We now give some equivalent descriptions of this group.

Proposition 2.4.2.1. *Let p be a fixed prime. The following groups are isomorphic:*

i) The group $\mathbb{Z}[1/p]/\mathbb{Z}$.

ii) The group, under multiplication, of (p^n)th roots of unity for all $n \in \mathbb{N}$.

iii) The abelian group with presentation $\langle x_1, x_2, \ldots, |px_1 = 0, px_{i+1} = x_i \forall i \geq 1\rangle$.

Remark 2.4.2.2. Recall that $\mathbb{Z}[1/p]/\mathbb{Z}$ is an increasing union of cyclic groups isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. The first isomorphism is essentially given by the exponential map: we can identify $\mathbb{Z}/p^n\mathbb{Z}$ with the subgroup of $p^n - th$ roots of unity by the map $x \mapsto e^{\frac{2\pi i x}{n}}$. If we look at the inclusion $\mathbb{Z}[1/p] \hookrightarrow \mathbb{Q}$, then the map $\mathbb{Z}[1/p]/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ induced by this inclusion is an injection. Again, $\mathbb{Q}/\mathbb{Z}$ can be viewed as a subgroup of $\mathbb{R}/\mathbb{Z}$ by means of the inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$. The identification of $\mathbb{R}/\mathbb{Z}$ with the subgroup of $\mathbb{C}^\times$ of elements of unit norm is exactly given by $x \mapsto e^{2\pi i x}$. The composite of these inclusions thus yields a homomorphism from $\mathbb{Z}[1/p]/\mathbb{Z}$ to the subgroup of p-power roots of unity. The map is an isomorphism, with inverse given essentially by the natural logarithm.

The presentation can be seen similarly. Identify the cyclic subgroup of $\mathbb{Z}[1/p]/\mathbb{Z}$ of order p^n with the subgroup of $\mathbb{Q}/\mathbb{Z}$ generated by $\frac{1}{p^n}$. There is then a homomorphism from the free group on countably many generators $x_1, x_2, \ldots$ to $\mathbb{Z}[1/p]/\mathbb{Z}$ gotten by sending x_n to $\frac{1}{p^n}$. Now, since x_1 is mapped to a cyclic subgroup of order p, it follows that the relation $px_1 = 0$ holds. Likewise, it is immediate that $px_{i+1} = x_i$. Thus, we obtain a homomorphism from the group with the stated presentation to $\mathbb{Z}[1/p]/\mathbb{Z}$.

Proposition 2.4.2.3. *The group $\mathbb{Z}[1/p]/\mathbb{Z}$ is divisible.*

There are a number of ways to prove this result (and you will give two in your HW). We already saw that $\mathbb{Z}[1/p]/\mathbb{Z}$ is p-divisible, and divisibility follows immediately from the following result, which you will also prove on your HW.

Lemma 2.4.2.4. *If p is a prime and G is a p-primary abelian group, then for any integer m coprime to p, G is m-divisible.*

Theorem 2.4.2.5. *Any p-primary divisible group T_p is isomorphic to a direct sum of copies of $\mathbb{Z}[1/p]/\mathbb{Z}$.*

Proof. Fix p and drop it from the notation, i.e., write T for T_p. Consider the set of subgroups of T isomorphic to $\mathbb{Z}[1/p]/\mathbb{Z}$ (this is possibly empty, but we'll come back to this). Let $\mathfrak{B}$ be the set of independent sets of subgroups isomorphic to $\mathbb{Z}[1/p]/\mathbb{Z}$. There is a natural ordering of $\mathfrak{B}$ given by set-theoretic union. We claim that every chain in $\mathfrak{B}$ has a least upper bound (proven in the same fashion as above). Thus, Zorn's lemma guarantees a maximal independent set of subgroups isomorphic to $\mathbb{Z}[1/p]/\mathbb{Z}$, say $\{S_i\}$. Write $S = \sum_i S_i$. We have to show that $S = T$. Since S is a divisible group (as a direct sum of divisible groups), it follows that $T = S \oplus R$. We claim that if $R \neq 0$, then it contains a subgroup isomorphic to $\mathbb{Z}[1/p]/\mathbb{Z}$, by adjoining this subgroup to $\{S_i\}$, we obtain a contradiction, since the enlarged set of subgroups is still independent.

Pick an element $x_1 \in R$ of order p: the group R is an abelian p-torsion group, so such an element always exists). By divisibility of R, we can find elements $x_2, x_3, \ldots$ with $px_2 = x_1$, $px_3 = x_2$ and, in general, $px_{i+1} = x_i$. However, we saw above that this provides a presentation of $Z(p^\infty)$. □

2.4.3 Injectivity and divisibility

Definition 2.4.3.1. An abelian group I is called *injective* if given any injective homomorphism of abelian groups $A \to B$ and a homomorphism $\varphi : A \to I$, there exists a homomorphism $\varphi' : B \to I$ extending φ, i.e., there exists a φ' making the diagram

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[dr] & B \arrow[d, dashed, "\exists\varphi'"] \\
 & I
\end{tikzcd}$$

commute.

Lemma 2.4.3.2. *If D is an abelian group, then D is divisible if and only if it is injective.*

Proof. If D is injective, then divisibility follows easily from the extension property: given any $x \in D$ and $n > 0$, let $\varphi : \mathbb{Z} \to D$ be given by $\varphi(1) = x$. Consider the multiplication by n map $\mathbb{Z} \to \mathbb{Z}$ which is an injective homomorphism of abelian groups. Since D is injective, φ extends to a homomorphism $\varphi' : \mathbb{Z} \to D$ such that $\varphi'(n) = x$. Since n was arbitrary, and since $x = \varphi'(n) = n\varphi'(1)$, we conclude that D is divisible.

Conversely, suppose D is divisible. We want to show that if $f : A \to B$ is any injective homomorphism of abelian groups, then any homomorphism $\varphi : A \to D$ extends to a homomorphism $B \to D$. Consider the set $\mathfrak{D}$ consisting of all pairs (C, ψ) where C is a subgroup of B containing A and $\psi : C \to D$ is a homomorphism extending φ. The set $\mathfrak{D}$ is non-empty since it contains (A, φ) and partially ordered with respect to inclusion, i.e., if (C, ψ) and (C', ψ') are two elements, say $(C, \psi) \leq (C', \psi')$ if $C \subset C'$ and $\psi'|_C = \psi$. If (C_i, ψ_i) is a chain, then one checks as before that $(\cup_i C_i, \cup_i \psi_i)$ is a least upper bound. Thus, Zorn's lemma guarantees that $\mathfrak{D}$ has a maximal element (C, ψ) (abusing notation slightly). We claim $C = B$ and ψ is the desired extension. If $C \subset B$ is a proper subgroup, then there exists $x \in B$ such that $x \notin C$. If xC has finite order in B/C or it has infinite order. In the second case, $x \notin C$ $C \cap \langle x \rangle = 0$ and therefore, $C \to D$ extends to $\langle C \rangle \oplus \langle x \rangle \to D$ by sending x to 0; this contradicts maximality of (C, ψ). If x has finite order in B/C, then write n for that order. Then, nx is the smallest positive integer such that $nx \in C$. In that case, since D is divisible there is an element $z \in D$ such that $nz = \varphi(nx)$. Then, the homomorphism $\psi + h : C \oplus \langle x \rangle \to D$ defined by sending $h(x)$ to z restricts to a homomorphism $\langle C, x \rangle \to D$, again contradicting maximality of (C, ψ), which is what we wanted to prove. □

Remark 2.4.3.3. You can use the above argument to give an alternative proof that a divisible subgroup of an abelian group is a summand: extend the identity homomorphism.

Injectivity and short exact sequences

Suppose $0 \to A' \to A \to A'' \to 0$ is a short exact sequence of abelian groups. If B is another abelian group, then $\mathrm{Hom}_{\mathcal{Ab}}(-, B)$ is a *contravariant* functor $\mathcal{Ab} \to \mathcal{Ab}$. In particular, applying $\mathrm{Hom}_{\mathcal{Ab}}(-, B)$ to our exact sequence above, we obtain a sequence of group homomorphisms

$$\mathrm{Hom}_{\mathcal{Ab}}(A'', B) \longrightarrow \mathrm{Hom}_{\mathcal{Ab}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{Ab}}(A', B).$$

In general, this new sequence of groups is *not* a short exact sequence. Note that $\mathrm{Hom}_{\mathcal{Ab}}(-, B)$ takes the trivial group to the trivial group (since there is only the trivial homomorphism from a trivial group to an arbitrary group). Furthermore, there is an evident map $\cong \mathrm{Hom}_{\mathcal{Ab}}(A, B) \oplus \mathrm{Hom}_{\mathcal{Ab}}(A', B) \to \mathrm{Hom}_{\mathcal{Ab}}(A \oplus A', B)$. Sending (f, g) to $f \oplus g$. A functor on abelian groups that preserves the zero object and direct sums will be called an additive functor, i.e., $\mathrm{Hom}_{\mathcal{Ab}}(-, B)$ is a contravariant additive functor (see Definition A.1.3.12).

Example 2.4.3.4. Consider the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$, and apply $\mathrm{Hom}_{\mathcal{Ab}}(-, \mathbb{Z})$. Note that $\mathrm{Hom}_{\mathcal{Ab}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = 0$ since $\mathbb{Z}$ has no elements of order 2. On the other hand, $\mathrm{Hom}_{\mathcal{Ab}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$: indeed, any homomorphism $f : \mathbb{Z} \to \mathbb{Z}$ is uniquely determined by $f(1) \in \mathbb{Z}$. One checks that $f \mapsto f(1)$ is a homomorphism and thus provides the required isomorphism. Granted these identifications, our the sequence obtained by applying $\mathrm{Hom}_{\mathcal{Ab}}(-, \mathbb{Z})$ reads:

$$\begin{tikzcd}
\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \arrow[d, "\cong"] \\
0 \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Z}.
\end{tikzcd}$$

Since the right horizontal map in the top row is induced by precomposing with the multiplication by 2 map $\mathbb{Z} \to \mathbb{Z}$, and the horizontal arrows are given by evaluation at 1, it follows that the bottom right horizontal map is also the multiplication by 2 map. In particular, this map is not an isomorphism and therefore the sequence is not exact.

Definition 2.4.3.5. We will say that a functor $\mathscr{F} : \mathcal{Ab} \to \mathcal{Ab}$ is *exact* if it is additive and preserves short exact sequences.

Proposition 2.4.3.6. *The following conditions on an abelian group I are equivalent:*

1. *I is injective, and*
2. *$\mathrm{Hom}_{\mathcal{Ab}}(-, I)$ is an exact functor.*

Proof. First, suppose B is any abelian group. If $\varphi : A \to A''$ is a surjective group homomorphism, then let us observe that $\mathrm{Hom}(A'', B) \to \mathrm{Hom}(A, B)$ is always injective. Indeed, suppose $f \in \mathrm{Hom}(A'', B)$ is sent to zero in $\mathrm{Hom}(A, B)$. By definition, this means that the composite of $A \to A'' \to B$ is the zero homomorphism, i.e., sends every element of A to the zero element of B. This immediately implies that f is the zero homomorphism $A'' \to B$, which establishes the required injectivity.

Now, if I is injective, the definition of injectivity can be rephrased as saying applying $\mathrm{Hom}_{\mathcal{A}b}(-, I)$ to an injective group homomorphism $A' \to A$ yields a surjection $\mathrm{Hom}_{\mathcal{A}b}(A, I) \to \mathrm{Hom}_{\mathcal{A}b}(A', I)$. Combining this observation with the discussion of the previous paragraph, we see that if $0 \to A' \to A \to A'' \to 0$ is a short exact sequence, then in the sequence

$$\mathrm{Hom}(A'', I) \longrightarrow \mathrm{Hom}(A, I) \longrightarrow \mathrm{Hom}(A', I)$$

the first homomorphism is injective and the last homomorphism is surjective. It remains to observe that, in this diagram, the image of the left hand morphism is precisely the kernel of the right hand morphism. Given a homomorphism $A'' \to I$, the composite $A \to A'' \to I$ automatically sends A' to 0 so the image is contained in the kernel. On the other hand, given a homomorphism $\varphi : A \to I$ such that the composite $A' \to A \to I$ is trivial, observe that $\varphi : A \to I$ is necessarily constant on cosets of A' in A and thus defines a homomorphism $\bar{\varphi} : A'' \to I$ by identifying $A'' = A/A'$.

We leave the converse as an easy exercise given what we have established above. □

Chapter 3

Symmetric, alternating and general linear groups

3.1 Lecture 9 bis: symmetric groups

We have spent the last few lectures talking about abelian groups and we have discussed a fair amount of the general theory of groups. Let us revisit the symmetric groups and understand their structure in more detail.

3.1.1 Symmetric groups and cycles

Recall that S_n was defined as $Isom(S)$, i.e., the group of self-bijections of S, where S is a set with n elements. It follows immediately from this that S_n has order $n!$. If we fix an identification $S = \{1, \ldots, n\}$, then there is a standard way to represent elements of S_n: if σ is a permutation, we can simply write $\sigma(i)$ below i in a matrix of the form

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n). \end{pmatrix}$$

This notation is cumbersome, but explicit. There is redundancy: for example, if a permutation fixes an integer, then it is still present in the notation. There is standard notation that is slightly more compact and eliminates this redundancy: *cycle* notation.

Definition 3.1.1.1. Suppose $i_1, \ldots, i_r$ are distinct integers with $1 \leq i_j \leq n$. If $\sigma \in S_n$ is a permutation that moves the i_j, fixes the remaining $(n - r)$ integers, and such that $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_r) = i_1$, then σ is called an *r-cycle* and that σ is a cycle of length r. A *transposition* is a cycle of length 2.

Remark 3.1.1.2. A cycle of length 1 is simply the identity, and thus there are many representations of the identity as a cycle.

I like to think of this as the "dynamics of σ" as we're really making two observations: the permutation σ is completely determined by iteration of σ on a single element, i.e., by the sequence $i_1, \sigma(i_1), \sigma^2(i_1), \ldots, \sigma^{r-1}(i_1)$, and σ fixes all integers not appearing in this sequence.

The iterates of an r-cycle σ affect only the elements $i_1, \ldots, i_r$. Another permutation σ' will be called *disjoint* from σ if the iterates of σ' fix $i_1, \ldots, i_r$. Notice that, in this case, the two permutations actually commute.

Definition 3.1.1.3. Two cycles σ and σ' are *disjoint* if every element moved by one is fixed by the other and vice versa. A family $\sigma_1, \ldots, \sigma_r$ of permutations is *disjoint* if each pair is disjoint. More generally, a pair of permutations σ_1 and σ_2 are disjoint, if there S can be written as the disjoint union of two subsets S_1 and S_2 such that σ_i is induced by a permutation of S_i by means of the composite $S \to S_i$.

Lemma 3.1.1.4. *If σ is an r-cycle, then the cyclic subgroup generated by σ has order r.*

Remark 3.1.1.5. Note that the cyclic subgroup generated by a permutation can have order r without σ being a permutation. For example, any product of disjoint cycles of a given order generates a cyclic subgroup of that order.

Proposition 3.1.1.6. *Every permutation is either a cycle or a product of disjoint cycles.*

Proof. The proof is by induction on the number of elements moved by σ. If σ moves nothing, it is the identity, which is a 1-cycle. Assume now that σ moves $n > 1$ elements. Pick i_1 an arbitrary element moved by σ, then set $i_j = \sigma^{j-1}(i_j)$ (by convention $\sigma^0 = id$).

Since the set $\{1, \ldots, n\}$ is finite, there is a first integer r where i_{r+1} is contained in $\{i_1, i_2, \ldots, i_r\}$. If $\sigma(i_r) = i_j$, then since $\sigma(i_{j-1}) = i_j$ as well, it follows that j must be 1 since if $j \geq 2$, then σ is not a bijection. Let $\sigma_1 = (i_1, \ldots, i_r)$. If $r = n$, then $\sigma_1 = \sigma$.

If $r < n$, then we can consider $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_r\}$, which consists of $n - r$ elements. Note that σ induces a permutation σ' of $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_r\}$, and by construction the permutation σ is the product of σ_1 and σ', which are necessarily disjoint. Appealing to the induction hypothesis allows us to finish the proof. □

In the proof above, we arbitrarily fixed an element i_1 and then proceeded to analyze what happened when we repeatedly applied σ. At the end of the procedure, we have written our permutation σ as the product of a collection of cycles. It is natural to ask whether the cycle obtained is unique. At the inductive step, observe that there are always two possibilities: either the permutation σ' fixes the complement or it does not. If the complement is fixed, then the procedure produces 1-cycles equal to the fixed elements. Note also that we have no control over the order of the factors in the permutation, since disjoint permutations necessarily commute. The output of the induction is a product of permutations where there is exactly one 1-cycle for each element fixed by σ; we will call such a factorization complete (as opposed to situations where we suppress 1-cycles).

Proposition 3.1.1.7. *If $\sigma \in S_n$, and $\sigma = \sigma_1 \cdots \sigma_r$ is a complete factorization of σ as a product of disjoint cycles, then this factorization is unique up to permutation of the factors.*

Proof. We already know there is exactly one factor for each 1-cycle, so it suffices to prove uniqueness for cycles of length ≥ 2. We proceed by descending induction on the number of disjoint cycles. Fix two factorizations $\sigma = \sigma_1 \cdots \sigma_s$ and $\sigma = \sigma'_1 \cdots \sigma'_t$. If σ_s moves i_1, then ${\sigma_s}^r(i_1) = \sigma^r(i_1)$ for all integers r. Now, some σ'_j must move i_1 and we may assume that $\sigma'_j = \sigma'_t$. It follows then that ${\sigma_s}^r(i_1) = (\sigma'_t)^r(i_1)$ for all r and thus $\sigma_s = \sigma'_t$ by construction. By cancellation, it follows that $\sigma_1 \cdots \sigma_{s-1} = \sigma'_1 \cdots \sigma'_{t-1}$ and we thus have a factorization with fewer cycles. □

3.2 Lecture 10: Conjugacy in symmetric groups

3.2.1 The sign homomorphism

Theorem 3.2.1.1. *Every permutation can be written as a product of transpositions.*

Proof. After Proposition 3.1.1.6, it suffices to show that any r-cycle can be written as a product of transpositions. This follows immediately from the following equality:

$$\begin{pmatrix}1 & 2 & \cdots & r\end{pmatrix} = \begin{pmatrix}1 & r\end{pmatrix}\begin{pmatrix}1 & r-1\end{pmatrix}\cdots\begin{pmatrix}1 & 2\end{pmatrix}.$$

□

The decomposition guaranteed by Theorem 3.2.1.1 is no longer unique. For example,

$$(23)(13) = (123) = (13)(12)$$

in S_3. Moreover, even the number of factors can change. However, there are purely combinatorial ways to prove that in any two representations of a permutation as a product of transpositions, the number of transpositions modulo 2 is independent of the presentation. There are many ways to proceed. For example, identify S_n with permutations of the set $1, \ldots, n$ and define $sign(\sigma) = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$. Here, each term in the product takes the value ± 1, and therefore the product takes the values ± 1. It is straightforward to check that $sign$ is a homomorphism and that the sign of a transposition is -1, and the result follows. You can also define the sign homomorphism by its value on transpositions.

Theorem 3.2.1.2. *There is a unique homomorphism $S_n \to \{\pm 1\}$ that takes the value -1 on transpositions.*

Proof. Because the symmetric group is generated by transpositions, it follows that if there exists a homomorphism with the above property, then it is necessarily uniquely specified by the above property. The existence was established before the statement, so we conclude. □

Remark 3.2.1.3. If we write $\mathbb{Z}^{\times}$ for the group of multiplicative units in the ring $\mathbb{Z}$, then the determinant is a homomorphism $GL_n(\mathbb{Z}) \to \mathbb{Z}^{\times} \cong \mathbb{Z}/2$. The function sending an element of S_n to the endomorphism of the free $\mathbb{Z}$-module $Z^{\oplus n}$ with basis $e_1, \ldots, e_n$ specified by $e_{\sigma(1)}, \ldots, e_{\sigma(n)}$ determines an injective homomorphism $S_n \to GL_n(\mathbb{Z})$. The sign homomorphism coincides with the composite $S_n \to GL_n(\mathbb{Z}) \overset{\det}{\to} \mathbb{Z}/2$.

Corollary 3.2.1.4. *If $\sigma \in S_m$ is a permutation and $\sigma = \tau_1 \ldots \tau_n$ and $\tau_1' \ldots \tau_n'$ are two decompositions as products of transpositions, then $n \cong n \mod 2$.*

Definition 3.2.1.5. We define the sign homomorphism $sgn : S_n \to \{\pm 1\}$ as the unique homomorphism given by the above theorem.

Remark 3.2.1.6. If $n = 2$, then the sign homomorphism is an isomorphism (in particular $S_2 = \mathbb{Z}/2$ is simple). For $n \geq 3$, it follows from the existence of the sign homomorphism that S_n is not simple, since the kernel of the sign homomorphism is a non-trivial (proper) normal subgroup. The alternating group A_n is defined to be the kernel of the sign homomorphism.

Example 3.2.1.7. The alternating group A_2 is trivial, A_3 is isomorphic to the cyclic group of order 3, and A_4 is a (non-abelian) group of order 12. The group A_4 arises in nature as the group of orientation preserving symmetries of the regular tetrahedron. Likewise, one can show that the other regular polyhedra have symmetry groups that are alternating of symmetric: the cube and octohedron have S_4 as symmetry group and the icosahedron and dodecahedron have A_5 as group of orientation preserving isometries.

3.2.2 Presentations

Since every element of S_n is a product of transpositions, it follows that S_n is always generated by transpositions; we now analyze relations between these generators to obtain a presentation. We begin by analyzing S_3.

Example 3.2.2.1. In that case there are 3 possible transpositions $(1,2)$, $(1,3)$ and $(2,3)$. However, among these transpositions, there is some redundancy. For example, observe that $(1,3)$ can be written as $(1,2)(2,3)(1,2)$. However, we can also write $(1,3)$ as $(2,3)(1,2)(2,3)$. Let $\sigma_1 = (1,2)$ and $\sigma_2 = (2,3)$. Summarizing the above, we have the relations $\sigma_1^2 = id$, $\sigma_2^2 = id$ and $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$. Using these relations, we see that the elements of S_3 are precisely $1, \sigma_1, \sigma_2, \sigma_1\sigma_2, \sigma_2\sigma_1$ and $\sigma_1\sigma_2\sigma_1$.

Another explicit formula for $(12\cdots r)$ is as the product $(12)(23)(45)\cdots(r-1r)$. Granting this, we see that we may set $\sigma_i = (ii+1)$ and take σ_i, $1 \leq 1 \leq n-1$ as generators. In this case, σ_i and σ_j are disjoint transpositions if $i \neq j \pm 1$ and therefore commute in this case. On the other hand if $i = j+1$, then the elements σ_i and σ_{i+1} can be thought of as generating a subgroup isomorphic to S_3 and thus the relation $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ holds because it holds in S_3. Thus, we conclude that there is a surjection

$$\langle \sigma_1, \ldots, \sigma_{n-1} | \sigma_i^2 = 1, \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } j \neq i \pm 1, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}\rangle \longrightarrow S_n$$

given by sending σ_i to $(ii+1)$. In fact, one may show that this surjection has trivial kernel; we defer the proof of this fact, which can be completed by an induction argument.

Proposition 3.2.2.2. *The symmetric group S_n has a presentation of the form*

$$\langle \sigma_1, \ldots, \sigma_{n-1} | \sigma_i^2 = 1, \sigma_i\sigma_j = \sigma_j\sigma_i \textit{ if } j \neq i \pm 1, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}\rangle$$

Remark 3.2.2.3 (Coxeter presentation). Another way to write the relation $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ is as follows: since $\sigma_i^{-1} = \sigma_i$ it is equivalent to $(\sigma_i\sigma_{i+1})^3 = id$. Likewise, the relation $\sigma_i\sigma_j = \sigma_j\sigma_i$ if $j \neq i \pm 1$ can be rewritten as $(\sigma_i\sigma_j)^2 = id$ if $j \neq i \pm 1$. Finally, we could also observe that $\sigma_i\sigma_i = 1$.

We can define an $(n-1) \times (n-1)$-matrix m_{ij} which takes the value 1 if $i = 2$, is equal to 3 if $i = j \pm 1$, and is equal to 2 if $i \neq j$ or $j \pm 1$. Then all of the above relations can be summarized in terms of the matrix m_{ij} by saying that $(\sigma_i\sigma_j)^{m_{ij}} = 1$. The matrix m_{ij} can be realized as the adjacency matrix of a graph; this is called the Coxeter presentation of the symmetric group.

If we think about the transpositions $x_n := (1,n)$, then we get a presentation again with $(n-1)$ generators $x_2, \ldots, x_n$. Of course $x_i^2 = id$, and straightforward computations show that $(x_ix_j)^3 = (x_ix_jx_ix_k)^2 = id$ for distinct i,j,k. This presentation is, I believe, due to Burnside and Miller. There is an even more symmetric presentation.

Proposition 3.2.2.4 (Guralnick, Kantor, Kassabov, Lubotzky). *The group S_n can be presented as*

$$\langle x_2, \ldots, x_n | x_i^2 = (x_ix_j)^3 = (x_ix_jx_k)^4 = 1 \textit{ for distinct } i,j,k\rangle.$$

There are presentations of S_n that use fewer generators. For example, S_3 can also be generated by the pair of elements $\sigma = \sigma_1$ and $\tau = (1,2,3)$. In this case, the relations $\tau^2 = \sigma^3 = id$ hold, and $(\tau\sigma)^2 = id$ also holds. This presentation can also be generalized. If we take a transposition τ and an n-cycle σ, then $\tau^2 = id$, while $\sigma^n = id$. We must then figure out the relations between powers of σ and τ. I will write down the relations, but I find them rather difficult to remember.

Proposition 3.2.2.5. *The symmetric group of order n has a presentation of the form*

$$\langle \sigma, \tau | \sigma^n = \tau^2 = (\sigma\tau)^{n-1} = (\tau\sigma^{-1}\tau\sigma)^3 = 1 \textit{ and } (\tau\sigma^{-j}\sigma\tau\sigma^j) = 1 \textit{ for } 2 \leq j \leq \lfloor\frac{n}{2}\rfloor\rangle$$

In the previous lecture, we observed that S_n had one normal subgroup, namely A_n. We now proceed to analyze the normal subgroup structure of S_n in greater detail. We begin with some general observations about the relationship between normal subgroups and conjugacy classes.

3.2.3 Conjugacy classes and normality: some concrete computations

Definition 3.2.3.1 (Conjugacy class)**.** If G is a group, and $h \in G$ is an element, then the *conjugacy class* of h is the orbit of h under the conjugation action of G on itself.

By definition, a subgroup N of a group G is normal if, for every $g \in G$, $gNg^{-1} = N$. In particular, if $n \in N$, then $gng^{-1} \in N$ for all $g \in G$, i.e., the conjugacy class of n is contained in N. It follows immediately that a normal subgroup is a union of conjugacy classes. The converse follows easily from the definition of normality and we summarize these observations in the following result.

Lemma 3.2.3.2. *A subgroup $N \subset G$ is normal if and only if $n \in N$ implies every conjugate in G of n is in N.*

The conjugacy class of an element is a subset of G that is typically not a subgroup. To deduce relationships between the size of conjugacy classes and the order of the group, we have to appeal to the orbit-stabilizer formula. The stabilizer of an element $x \in G$ under the conjugation action is by definition the centralizer $C_G(x)$. Assuming G is a finite group, the orbit-stabilizer formula then implies that the number of distinct elements in the conjugacy class is $G/C_G(x)$, i.e., the index of $C_G(x)$ in G. We summarize these observations in the following result.

Lemma 3.2.3.3. *If G is a finite group and $x \in G$, then the number of distinct conjugates of x in G is equal to the index of the centralizer of x in G, i.e., $G/C_G(x)$. In particular, the number of conjugates of x divides $|G|$.*

One variant of the above result is to replace elements of G with more complicated subsets. Consider the set $Sub(G)$ of all subgroups H of G. Since conjugates of subgroups are subgroups, the conjugation action of G on itself defines an action on of G on $Sub(G)$; we will say this is the action "induced by conjugation on G". By construction, the orbits of this action are precisely the conjugates of a given subgroup $H \subset G$. If $H \subset G$ is a subgroup, viewed as an element of $Sub(G)$, then the stabilizer for the conjugation action consists precisely of elements $g \in G$ such that $c_g(H) = H$, i.e., by definition, it is the normalizer $N_H(G)$. Thus, if G is finite, then proceeding in a fashion entirely analogous to the above, we may deduce the following result from the orbit-stabilizer formula 1.3.2.4.

Lemma 3.2.3.4. *Assume G is a finite group and $H \subset G$ is a subgroup. The number of conjugates of H is equal to $|G|/|N_H(G)|$ (which divides $|G|$).*

3.2.4 Conjugacy classes in the symmetric group

To put these results to use, we need to analyze conjugacy classes in the symmetric group. We begin in the simplest case: what are the conjugates of a given r-cycle? Thus, let σ be an r-cycle. If α is an arbitrary permutation, then we may write α as a product of transpositions (possibly non-uniquely), so let us first analyze what happens in that case. We begin with an explicit example.

Example 3.2.4.1. Consider the cycle $(1, 2, 3, 4, 5)$ and the transposition $(1, 2)$. The inverse of any transposition is itself. Observe that if we conjugate $(1, 2, 3, 4, 5)$ by $(1, 2)$, we get another 5-cycle, namely $(2, 5, 1, 3, 4)$. However, cyclically permuting the numbers appearing in a cycle provides an alternate description of the same cycle. Thus, we could just as well write the above cycle as $(1, 3, 4, 2, 5)$. In particular, observe that conjugating a 5-cycle by a transposition yields another 5-cycle. It follows that any conjugate of a 5-cycle is again a 5-cycle.

To generalize this computation we proceed in two steps: first we analyze conjugation of an r-cycle by a transposition, and then we observe that every element of the symmetric group may be written as a product of disjoint cycles. Let us fix our notation involving actions.

As usual, we write S_n for the bijections of the set $\{1, \ldots, n\}$. If $\sigma \in S_n$, then we will write $i \cdot sigma$ for the action of σ on i; this is done to make sure this is an action in the sense we have defined (rather than a "right" action). Now, if σ is the r-cycle $(i_1, \ldots, i_r)$, then by definition $i_j \cdot \sigma = i_{j+1}$ if $j \leq r-1$ and i_1 if $j = r$, while σ fixes all other integers. If τ is a transposition, then $i_j \cdot \sigma\tau = i_{j+1} \cdot \tau$ for $1 \leq j \leq r-1$ and $i_1 \cdot \tau$ for $j = r$. On the other hand, if an integer i is fixed by σ, then $(i \cdot (\sigma\tau)) = i \cdot \tau$ by definition.

In fact, given a formula for τ, we can use the above discussion to evaluate the action of $\tau^{-1}\sigma\tau$. Indeed, for any $i \in \{1, \ldots, n\}$, the following formula holds (using that fact that $\tau^{-1} = \tau$):

$$(i \cdot \tau)\tau\sigma\tau = i \cdot (\sigma\tau)$$

Suppose $\sigma = (i_1, \ldots, i_r)$. Combining these observations, we see that $\tau\sigma\tau$ cyclically permutes the elements $i_j \cdot \tau$ and fixes all other elements. In other words, we have established that

$$\tau(i_1, \ldots, i_r)\tau = (i_1 \cdot \tau, \ldots, i_r \cdot \tau).$$

In particular, it follows that the conjugate of an r-cycle by a transposition is again an r-cycle. Using the fact that every element of S_n may be written as a product of transpositions, by induction on the number of transpositions required to represent an element of S_n, we immediately conclude that the conjugate of an r-cycle is again an r-cycle.

Appealing to Proposition 3.1.1.6, any element of S_n can be written as a product of disjoint cycles (uniquely up to permutation): $\sigma = \beta_1 \cdots \beta_r$. If $\tau \in S_n$, then it follows from the formula

$$\tau^{-1}\sigma\tau = \tau^{-1}\beta_1 \cdots \beta_r\tau = (\tau^{-1}\beta_1\tau)(\tau^{-1}\beta_2\tau) \cdots (\tau^{-1}\beta_r\tau)$$

that two conjugate elements of S_n have the same decomposition into disjoint cycles; in this case we will say that they have the same cycle structure. Thus, our formulas for conjugation of an r-cycle extend immediately to statements about conjugation of arbitrary elements of S_n. We summarize what we have established in the following statement.

Proposition 3.2.4.2. *Conjugate elements of S_n have the same cycle structure.*

We aim to establish a converse to this statement.

3.3 Lecture 11: Alternating groups and general linear groups over finite fields

3.3.1 Conjugacy in S_n continued

Proposition 3.3.1.1. *Two elements of S_n have the same cycle structure if and only if they are conjugate.*

Proof. We have already seen that conjugate elements have the same cycle type in Proposition 3.2.4.2, so it remains to prove the converse. To see this, we simply construct a permutation conjugating a given element with fixed cycle type with any other.

To this end, suppose σ_1 and σ_2 are elements having the same cycle structure. Suppose $\sigma_1 = \alpha_1 \cdots \alpha_r$ and $\sigma_2 = \beta_1 \cdots \beta_r$, where we have reordered the elements if necessary so that α_i and β_i are cycles of the same length. By the discussion in the proof of Proposition 3.2.4.2, it suffices to find an element $\gamma \in S_n$ such that γ maps the numbers permuted by the cycle α_i to the numbers permuted by the cycle β_i. Indeed, write them as

$$\begin{gathered}(i_1(1), \ldots, i_{s_1}(1)) \cdots (i_1(r), \ldots, i_{s_r}(r)) \\ (i'_1(1), \ldots, i'_{s_1}(1)) \cdots (i'_1(r), \ldots, i'_{s_r}(r))\end{gathered}$$

and define γ to be the function that takes $i_j(k)$ to $i_j(k)'$. It is straightforward to check that γ is a bijection. The formula in the construction above guarantees that conjugation by γ takes the permutation σ_1 to σ_2. □

In Lemma 3.2.3.2, we observed that normality could be characterized in terms of conjugacy, and combining that criterion with Proposition 3.3.1.1, we immediately deduce the following fact.

Corollary 3.3.1.2. *A subgroup $H \subset S_n$ is normal if and only if whenever $\alpha \in H$, then every β having the same cycle structure as α lies in H.*

3.3.2 Conjugacy classes and counting

Let us deduce some numerical consequences of the discussion so far; in particular, we will view this discussion as providing a measure of the complexity of the symmetric groups as n grows. If σ is a permutation of n elements, then let us decompose σ into a product of disjoint cycles (and let us include 1-cycles corresponding to fixed elements). The sum of the lengths of the cycles that appear in this decomposition, which are all integers ≥ 1, must be precisely n. A way of writing an integer n as $\sum_i n_i$ with each $1 \leq n_i \leq n$, is called a *partition of n*.

Corollary 3.3.2.1. *The conjugacy classes of elements in S_n are in bijection with partitions of n.*

Remark 3.3.2.2. Partitions of positive integers n are well studied. Let $p(n)$ be the number of integer partitions of n in the sense above; and set $p(0) = 1$ (the reason for this convention will be clear momentarily). One standard way to study these numbers is to consider their generating function $\sum_{n \geq 0} p(n)q^n$. A straightforward exercise involving geometric series shows that

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{i=1}^{\infty} \frac{1}{1-q^i}$$

The above identification of conjugacy classes with partitions is not an accident, and is closely connected with the representation theory of the symmetric group. The number $p(n)$ grows very quickly (see http://oeis.org/A000041 for a list of the first few partitions); one can show that $p(n)$ grows as $\frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}$.

Similarly, it is straightforward to count the number of elements in various different conjugacy classes; we will use this information in conjunction with Corollary 3.3.1.2 to deduce restrictions on the structure of normal subgroups of S_n.

Lemma 3.3.2.3. *If n is a positive integer, then the number of r-cycles in S_n is equal to $\frac{n!}{r(n-r)!}$.*

Proof. To choose an r-cycle, we simply choose elements of an n element set, without replacement, up to cyclic permutations. There are $n(n-1)\cdots(n-r+1)$ choices of the r-elements and to account for cyclic permutation, we divide by r. □

Remark 3.3.2.4. You can write down a similar formula for the number of elements in any conjugacy class: often further symmetries will need to be taken into account in writing the formula. For example, just prior to Lemma 3.3.4.1 we will write down a formula for the number of products of disjoint transpositions in S_n. I leave it as an exercise to write down the general case.

3.3.3 Conjugacy classes in groups of small order

Example 3.3.3.1 (Conjugacy classes in S_4). The symmetric group S_4. In this case, the possible cycle structures are (1) corresponding to the identity element, (12) corresponding to transpositions, (123) corresponding to 3-cycles, (1234) corresponding to the 4-cycle, and $(12)(34)$ corresponding to disjoint transpositions. It is straightforward to count these elements using the formula above. There is a single 1-cycle. There are 6 transpositions, there are 8 3-cycles, there are 6 4-cycles. Finally, regarding products of transpositions: we have 6 choices for the first transposition, and we are allowed to choose the elements of the remaining transposition from a set of size $4-2=2$ (up to cyclic permutation of the elements), which gives an additional $\frac{2\cdot 1}{2}=1$ choices; however, we may permute the two transpositions, so we need to divide the result by 2, i.e., there are 3 cycles whose cycle structure is a pair of disjoint transpositions.

Example 3.3.3.2 (Structure of A_4). The alternating group A_4 is made up of the identity, the 3-cycles and the products of disjoint transpositions (there are 12 of these). The transposition and the 4-cycles all have sign -1 and make up the elements of the other coset of A_4.

The disjoint transpositions that occur here can be represented by $(12)(34)$, $(13)(24)$ and $(14)(23)$ and each has order 2. Observe that $(12)(34)(13)(24)=(14)(23)$. In fact, these 4 elements form a subgroup of A_4 that is isomorphic to $V := \mathbb{Z}/2\times\mathbb{Z}/2$ (generated by any choice of 2 of the products of disjoint transpositions). Since cycle structure is preserved by conjugation, it follows that this subgroup of A_4 is stable by conjugation in S_4 (so it is even normal in S_4) and is therefore normal. Since A_4 has order 12, it follows that A_4/V is a group of order 3 and therefore isomorphic to $\mathbb{Z}/3$ after choice of a generator. In particular, A_4 is not a simple group.

Remark 3.3.3.3. Observe that we have produced a sequence $1\subset V\subset A_4\subset S_4$ of normal subgroups of S_4 where each successive quotient is abelian.

We begin by extending the analysis of conjugacy classes in A_4 to conjugacy classes in A_5 and usins counting arguments, we deduce the simplicity of A_5. Then, we introduce another useful class of finite groups: general linear groups over finite fields.

3.3.4 Simplicity of A_5

We begin by analyzing the structure of conjugacy classes in S_5. Appealing to the formula for counting r-cycles, we conclude that there are 10 transpositions, 20 3-cycles, 30 4-cycles, and 24 5-cycles. Similar counting arguments show that there are

- 15 products of disjoint transpositions: there are 10 choices for the first transposition and 3 choices for the second transposition and we divide by two because we may switch order of the transpositions;
- 20 products of a disjoint 3-cycle and a transposition: there are 20 choices for the 3-cycle, and a unique choice for the disjoint transposition.

The subgroup A_5 consists of the elements that have sign $+1$, i.e., the identity, the 3-cycles, the 5-cycles, and the products of disjoint transpositions. In total there are $1 + 20 + 24 + 15 = 60$ such elements, as expected.

We began our analysis of A_4 by studying the products of disjoint transpositions: in that case we observed that these elements formed an abelian subgroup. As it turns out, this was a low-dimensional accident: the subset of products of disjoint transpositions (together with the identity element) no longer forms a subgroup of A_5. There are several ways to see this. The brute-force method is to simply compute a bunch of examples. For example:

$$((23)(45))((12)(34)) = (13542).$$

However, this can also be argued more abstractly using divisibility properties stemming from Lagrange's theorem: if the subset of disjoint transpositions together with the identity forms a subgroup, then this subgroup contains $15 + 1 = 16$ elements. However, if this subset was a subgroup, then 16 would have to divide 60, which is a contradiction.

Both points of view are useful and both methods generalize. The formula that we wrote down holds in A_n for $n \geq 5$ with no change, so we immediately deduce that the subset consisting of the identity and products of disjoint transpositions will never be a subgroup of A_n for $n \geq 5$. On the other hand, we can also simply compute the number of products of disjoint transpositions in S_n for $n \geq 5$: there are $\frac{1}{2}(\frac{n(n-1)}{2} + \frac{(n-2)(n-3)}{2})$ such elements and they all live in A_n as well. Since A_n has order $\frac{n!}{2}$, one can then check that $\frac{n!}{2}$ is not divisible by $\frac{1}{2}(\frac{n(n-1)}{2} + \frac{(n-2)(n-3)}{2})$ to conclude.

By generalizing these kinds of analyses, we can completely understand the normal subgroup structure of A_5. Since we understand conjugation in S_n the questions is: when are elements conjugate in A_n? The following lemma provides a few different techniques for answering these kinds of questions.

Lemma 3.3.4.1. *All 3-cycles in A_5 are conjugate, and all products of disjoint transpositions in A_5 are conjugate. There are 2 disjoint conjugacy classes of 5-cycles (each consisting of 12 elements).*

Proof. If σ be a 3-cycle in A_5, then it may be conjugated to (123) in S_5 by some permuation π. If $\pi \in A_5$, then our initial 3-cycle is conjugate to (123). Thus, assume that π is not in A_5. In that case, it has sign -1. If we let $\pi' = \pi(45)$, then π' has sign $+1$ and lies in A_5. Since $\pi^{-1}\sigma\pi = (123)$, it follows that

$$(45)\pi^{-1}\sigma\pi(45) = (45)(123)(45) = (123).$$

In other words, ${\pi'}^{-1}\sigma\pi' = (123)$ and we conclude that σ is conjugate in A_5 to (123) as well. Thus, all 3-cycles in A_5 are conjugate.

A similar argument can be made for products of disjoint transpositions. Thus, let σ be a product of disjoint transpositions. The element σ may be conjugated to $(12)(34)$ in S_5 by some element π. If $\pi \in A_5$, then σ is already conjugate in A_5 to $(12)(34)$, so assume $\pi \notin A_5$, i.e., π has sign -1. As before, consider the element $\pi' = \pi(12)$. As before, $\pi'\sigma\pi = (12)(34)$ and $\pi' \in A_5$. Thus, all products of disjoint transpositions are conjugate in A_5.

For the final statement, we proceed in a different fashion and use a counting argument. Recall that, via the orbit-stabilizer formula, the number of distinct conjugates of an element times the order of the centralizer of the element is equal to the order of the group. We begin by analyzing the centralizer in S_5 of a 5-cycle. This centralizer contains the cyclic subgroup generated by the 5-cycle. Since there are precisely

24 5-cycles and they are all conjugate in S_5, we conclude that the centralizer of a 5-cycle is precisely the cyclic subgroup generated by the element.

We can similarly compute the centralizer of a 5-cycle in A_5. As before, the centralizer in A_5 contains the cyclic subgroup generated by the element. You can check that the centralizer is precisely this subgroup (in this case, we can do this by direct computation: simply check that 3-cycles and products of disjoint transpositions do not commute with 5-cycles). Now, since there are 24 distinct 5-cycles and since the order of the centralizer times the number of distinct conjugates must be equal to the order of the group, we conclude that there are 2 distinct conjugacy classes of 5-cycles, each consisting of 12 elements. □

Remark 3.3.4.2. The first two statements are completely general in the sense that the arguments given work in A_n for any $n \geq 5$. Note, however, that the first argument does not work in A_4: there are 3-cycles in A_4 that are not conjugate (though the second argument does work).

Putting everything together, we can now establish the following fact.

Theorem 3.3.4.3. *The group A_5 is simple.*

Proof. Any normal subgroup is a union of conjugacy classes and must contain the identity. Thus, if H is a normal subgroup, then $|H|$ must be 1 plus a sum of the numbers $12, 12, 15$ and 20. By explicit computation, the only such sums that can divide 60 are the number 1 itself and $1 + 12 + 12 + 15 + 20$. □

3.3.5 The groups $GL_n(F)$, when F is a finite field

In the above, we studied various groups of matrices over a field. If F is a finite field, then $GL_n(F)$ is a subset of a finite set $(n \times n)$-matrices over the field, and thus finite itself. We now study the order of $GL_n(F)$ if F is finite.

Lemma 3.3.5.1. *If F is a finite field with q elements, then*

$$|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$$

Proof. The basic fact we use here is: if $v_1, \ldots, v_r$ is a sequence of linearly independent vectors in a vector space V, then a vector $\mathbf{v} \in V$ is linearly independent from that set if it is not contained in the span of $\{v_1, \ldots, v_n\}$. We now use this fact in concert with the definition: elements of $GL_n(F)$ are sequences of n linearly independent elements of $V := F^{\oplus n}$. There are q^n elements on $F^{\oplus n}$. The first column of our matrix must be a non-zero vector in V and there are $q^n - 1$ such elements. The second column must be a vector that lies off the line spanned by the first column. Since there are q multiples of that vector, we have $q^n - q$ choices for the second element and so on. □

Remark 3.3.5.2. For later use, we can rewrite this as follows: factoring a power of q out of all terms except the first, we factor a q out of $q^n - q$, q^2 out of $q^n - q^2$ and so forth to obtain a factor of $q^{1+2+\cdots+(n-1)} = q^{\frac{n(n-1)}{2}}$. The formula above reads:

$$|GL_n(F)| = q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1).$$

Note that $q^i - 1$ is congruent to 1 mod q for all i. Therefore, the product is congruent to 1 mod q as well. Thus, we have factored the order of $GL_n(F)$ as a power of q and a factor coprime to q. Later, we will observe that q must be a power of a prime number p, and thus the above factorization is as the p-part and prime to p part.

Remark 3.3.5.3. The product $(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$ sometimes written $(1 : q)_n$ and called the q-Pochhammer symbol.

Recall that $SL_n(F)$ is the kernel of $\det : GL_n(F) \to F^\times$. The determinant homomorphism is surjective, since the matrix $diag(\lambda, 1, \dots, 1)$ has determinant λ for any $\lambda \in F$. Thus, Lagrange's theorem implies the following result.

Corollary 3.3.5.4. *If F is a finite field with q elements, then*

$$|SL_n(F)| = \frac{(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})}{q-1}.$$

We define:

$$PGL_n(F) := GL_n(F)/Z(GL_n(F)).$$

In linear algebra, one shows that the center of $GL_n(F)$ consists of the non-zero scalar multiples of the identity matrix. It follows that $Z(GL_n(F))$ has order $q-1$, and thus that $|PGL_n(F)| = |SL_n(F)|$.

Similarly, one defines

$$PSL_n(F) := SL_n(F)/Z(SL_n(F)).$$

The center of $SL_n(F)$ can be shown to consist of $n \times n$-matrices X such that $X^n = Id_n$. As a consequence, writing down the order of $PSL_n(F)$ is a slightly more complicated exercise, since it depends on n-th roots of unity in F.

Example 3.3.5.5. Take $n = 2$ and F the finite field with 2 elements. In this case, $SL_2(F)$ has $(2^2 - 1)(2^2 - 2) = 6$ elements. Every element in F is a square, and so $|PSL_2(F)| = 6$. You can construct an isomorphism from the symmetric group on 3 elements to $PSL_2(F)$ by writing down explicit matrices. For example, any shearing matrix has order 2. On the other hand, the matrix

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

has order 3 (it has determinant 1 because we are working in characteristic 2!).

Example 3.3.5.6. The situation in $PSL_2(F)$ with $|F| = 3$ is a little different. In this case, $SL_2(F)$ has order $\frac{1}{2}(3^2-1)(3^2-3) = 24$. The center of $SL_2(F)$ consists of matrices xId_2 with $x^2 = 1$. Note that, in this case, 2^2 is congruent to 1 mod 3, so the center has order 2, which means $|PSL_2(F)| = 12$. The shearing matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

gives an element of order 3 in $SL_2(F)$, which corresponds to an element of order 3 in $PSL_2(F)$. I claim that $PSL_2(F) \cong A_4$. The elements corresponding to products of disjoint transpositions all have order 2 and can be represented by conjugates of the element $diag(1, 2)$.

Chapter 4

Sylow’s theorems and applications

4.1 Lecture 12: The Sylow theorems

In this lecture we will prove the

4.1.1 Subgroups and conjugacy in $GL_n(F)$

The study of conjugacy classes in $GL_n(F)$ amounts to a theory of normal forms for invertible matrices over finite fields (a variant of Jordan normal form called rational canonical form). We will not go into detail about this theory here. For later use, we introduce some standard subgroups of $GL_n(F)$ and study their orders. Write $B(F)$ for the subgroup of $GL_n(F)$ consisting of upper triangular matrices, $U(F)$ for the subgroup of upper triangular matrices with 1s along the diagonal, and $T(F)$ for the subgroup of diagonal matrices.

Lemma 4.1.1.1. *If F is a finite field of order q.*

1. *The group $T(F) \subset GL_n(F)$ has order $(q-1)^n$.*
2. *The group $U(F)$ has order $q^{\frac{n(n-1)}{2}}$, which is the largest power of p dividing $|GL_n(F)|$.*

Proof. For the first point, simply note that each entry of $T(F)$ is a non-zero element of F and there are $(q-1)$ such elements. For the second point, observe that the group $U(F)$ consists of sums of the identity matrix and a strictly upper triangular matrix. A strictly upper triangular matrix has $(n-1)+(n-2)+\cdots+1 = \frac{n(n-1)}{2}$ entries, and these entries are allowed to be arbitrary elements of F. The final statement follows form our computation of the order of $GL_n(F)$ from Lemma 3.3.5.1 and Remark 3.3.5.2. □

4.1.2 Every finite group embeds in a general linear group

Proposition 4.1.2.1. *Suppose F is a field and G is a finite group. There exists an integer n and an injective group homomorphism $G \hookrightarrow GL_n(F)$.*

Proof. We proceed in two steps. First, we observe that S_n embeds in $GL_n(F)$. To this, simply identify S_n with the permutations of the standard basis vectors in $F^{\oplus n}$. By Cayley's theorem, we know that if G is a finite group, then $G \hookrightarrow S_{|G|}$ and combining the two statements we conclude. □

Remark 4.1.2.2. If F is a field, then a homomorphism $G \to GL_n(F)$ is called an F-representation of G. If $G \to GL_n(F)$ is injective, it is called a *faithful* F-representation. Thus, the above corollary shows that every finite group admits faithful F-representations for any F.

4.1.3 Existence of a Sylow subgroup

Earlier, we observed that torsion abelian groups could be studied by breaking them into their p-torsion summands. The examples studied above show that, even if a group G has a subgroup whose order is equal to the largest power of a prime p dividing $|G|$, that subgroup need not be a normal subgroup and thus not even a direct factor. Moreover, it is not even immediately clear that if a finite group G has order $p^n m$ where m is an integer coprime to p, then G has a subgroup of order p^n. Following Sylow, we now turn this into a definition.

Definition 4.1.3.1. Suppose G is a finite group and p is a prime number.

1. If $|G| = p^r$, then G is called a *p-group*.
2. If $|G| = p^n m$ with m coprime to p, then a subgroup $S \subset G$ is called *Sylow p-subgroup* if $|S| = p^n$, i.e., S is a p-group of maximal possible order in G.

Example 4.1.3.2. If F is a finite field of order q, then $q = p^n$ and $GL_n(F)$ has a p-Sylow subgroup, i.e., the subgroup $U(F)$ constructed above.

We now ask: if G is a finite group, then does it have a Sylow p-subgroup? To answer this question: we instead ask the question: if G is a group that we know has a Sylow p-subgroup and H is a subgroup of G, must H also have a Sylow p-subgroup? Of course, if G has a single Sylow p-subgroup, then we can also ask how many does it have? The conjugation action of G on itself allows us to see that if G has a Sylow p-subgroup, then all conjugates of this subgroup are also Sylow p-subgroups. Intuitively, we might expect to get a Sylow p-subgroup of H by simply taking an intersection of one in G with H.

Lemma 4.1.3.3. *Suppose G is a group and S is a p-Sylow subgroup of G. If $H \subset G$ is a subgroup, then H has a p-Sylow subgroup. More precisely, there exists an element $g \in G$ such that $H \cap gSg^{-1}$ is a p-Sylow subgroup of H.*

Proof. Set $X = G/S$. Since S is a p-Sylow subgroup of G, it follows that $|X|$ is coprime to p. Moreover, the stabilizers G_x are, by construction, conjugates of S. Consider the action of H on X induced by inclusion. An analogous computation shows that H_x is of the form $H \cap G_x$, i.e., the intersection of H with a conjugate of S.

The set X is partitioned into H-orbits. Since X has order coprime to p, the sum of the cardinalities of the orbits is equal to a number that is prime to p. Since the order of X is coprime to p, it cannot be the case that all orbits have cardinality divisible by p; since p is prime, at least one of the orbits must have cardinality that is coprime to p. Fix an orbit $\mathcal{O}$ whose order is coprime to p and pick $x \in \mathcal{O}$.

The orbit-stabilizer formula tells us that $|H| = |O| \cdot |H_x|$. Since H_x is the intersection of H with a conjugate of a Sylow p-subgroup, it is itself a p-group. Since $|O|$ is coprime to p, and H_x is a p-group, we then conclude that H_x must be a p-Sylow subgroup. □

Theorem 4.1.3.4. *If G is a finite group, then G has a p-Sylow subgroup.*

Proof. Suppose G is a finite group, and p is a prime dividing $|G|$. By Proposition 4.1.2.1, we may embed G in $GL_n(\mathbb{F}_p)$ (take $n = |G|$). We observed in Example 4.1.3.2 that $GL_n(\mathbb{F}_p)$ has a p-Sylow subgroup. Appealing to Lemma 4.1.3.3 we conclude that G has a p-Sylow subgroup as well. □

Remark 4.1.3.5. There are a number of variants of this kind of proof. For example, Herstein constructs a Sylow p-subgroup of symmetric groups and then uses the "permanence" property above. The proof above, I learned from notes of Serre.

4.1.4 Counting formulas and the class equation

Suppose G is a group acting on a set X. We know that this action gives a partition of X into orbits for the G-action and, furthermore, each orbit is, after choice of a point in the orbit, isomorphic to a coset space for G. There are, however, various refinements of this partition. For example, those orbits consisting of only a single element, i.e., the fixed points of the group action, are distinguished (they are the points whose stabilizer is the whole group). Write X^G for the set of points in X that are fixed by G, i.e., whose stabilizer group is all of G. Any G-orbit in X that is not in $X^G \subset X$ is necessarily an orbit consisting of more than 1 element; equivalently, the stabilizer of any point in the orbit is a proper subgroup of G. Let I be a set indexing the distinct orbits of G whose stabilizers are proper subgroups of G, and for each $i \in I$, fix a representative x_i of the orbit parameterized by $i \in I$. The choice of x_i determines a bijection from G/G_{x_i} to the orbit through x_i, and the following result is an immediate consequence of the definitions.

Lemma 4.1.4.1. *If G is a finite group acting non-trivially on a set X, and I indexes the distinct orbits of X that have more than 1 element, and x_i is a chosen representative of each such orbit, then*

$$|X| = |X^G| + \sum_{i \in I} |G/G_{x_i}|.$$

In the special case where G is a p-group, the orders of orbits are necessarily powers of p. Therefore, $\sum_{i \in I} |G/G_{x_i}|$ will always be divisible by p.

Lemma 4.1.4.2. *If G is a p-group acting on a set X, then*

$$|X| \equiv |X^G| \mod p.$$

In particular, if G acts non-trivially, and X is coprime to p, then X^G is non-empty.

We can specialize the above to the case where $X = G$ under the conjugation action. Orbits of this action are, by definition, conjugacy classes, while stabilizers of points are, by definition, centralizers of elements. To say that a point $g \in G$ is a fixed point for the conjugation action is to say that, for every $h \in G, hgh^{-1} = g$, i.e., $hg = gh$. In other words, the fixed points of the conjugation action are precisely elements of the center of G. Thus, we can partition G into $Z(G)$ and those orbits of size ≥ 1. Now, if we fix a representative x_i from each conjugacy class consisting of more than 1 element, then this choice gives an identification of $\mathcal{O}_{x_i}$ with the coset space $G/C_G(x_i)$. Lemma 4.1.4.1 then specializes to the following result.

Lemma 4.1.4.3 (Class equation)**.** *If G is a finite group, I indexes the distinct conjugacy classes of G that have more than 1 element, and $\{x_i\}_{i \in I}$ is a chosen element of each conjugacy class that consists of more than 1 element, then*

$$|G| = |Z(G)| + \sum_{i \in I} |[G : C_G(x_i)]|.$$

4.2 Lecture 13: More on Sylow's theorems and applications

4.2.1 Applications of counting formulas:

Lemma 4.2.1.1. *If G is a p-group, then $Z(G)$ is non-trivial.*

Proof. Assume $|G| = p^r$. Let I be a set indexing distinct conjugacy classes with more than 1 element. If I is empty, there is nothing to check. Suppose I is non-empty. In that case, $C_G(x_i)$ is also a p-group, and has order p^j with $j < r$. It follows that $|G/C_G(x_i)|$ is divisible by p. Since the $|G|$ is divisible by p it follows that $p||Z(G)|$. Since $Z(G)$ is a subgroup, it is non-empty, so $|Z(G)| \geq 1$, which means $|Z(G)| \geq p$. □

Corollary 4.2.1.2. *Every group of order p^2 is isomorphic to $\mathbb{Z}/p \times \mathbb{Z}/p$ or $\mathbb{Z}/p^2$.*

Proof. Suppose G is a group of order p^2. We know that $Z(G)$ is non-trivial. If $Z(G) = p^2$, we're done. Assume that $|Z(G)| = p$. In that case, since $Z(G)$ is a normal subgroup, it follows that $G/Z(G)$ is a group of order p and therefore a cyclic group of order p. Pick a generator of the quotient and any lift σ of that element to G. The distinct cosets of $G/Z(G)$ are then of the form $\sigma^i Z(G)$. And any element of G can be written in the form $\sigma^i x^j$ for some element of the center. However, such elements commute by explicit computation. Thus, we conclude that G is abelian. The result then follows from the structure theorem depending on whether G has an element of order p^2 or not. □

The general "fixed point partition" lemma 4.1.4.1 has applications as well: all Sylow p-subgroups are conjugate (we know the set of Sylow p-subgroups is non-empty by appeal to Theorem 4.1.3.4).

Theorem 4.2.1.3 (Sylow II)**.** *If G is a finite group and $p||G|$, then all Sylow p-subgroups are conjugate.*

Proof. If S is a Sylow p-subgroup of G, then consider G/S. The stabilizers for the left G-action on G/S are precisely the conjugates of S in G. Now, if S' is another Sylow p-subgroup, then S' also acts on G/S via the inclusion $S' \subset G$. In terms of this action, showing S' is conjugate to S is equivalent to showing that this action of S' on G/S fixes a point. Indeed, if S' lies in the stabilizer in $Stab_G(x)$ for $x \in G/S$, then S' necessarily fixes x, but then since $|S'| = |Stab_G(x)|$ the inclusion $S' \subset Stab_G(x)$ must be an equality.

Having establish this equivalence, observe that G/S is a set having order coprime to p. The action of S' on G/S is non-trivial, so Lemma 4.1.4.2 implies that $|X^G|$ is necessarily non-empty. □

Remark 4.2.1.4. If $H \subset G$ is any p-group, and $S \subset G$ is a Sylow p-subgroup, then we may consider the induced action of H on G/S as well. In this case, as above, we conclude that the H-action on G/S contains a fixed point, i.e., H is contained in a conjugate of S. Since all Sylow p-subgroups are conjugate, this means that every p-group is contained in a Sylow p-subgroup.

Here is a convenient summary of the Sylow theorems so far. Let $Syl_p(G)$ be the set of Sylow p-subgroups of G; this is a subset of the set $Sub(G)$ of all subgroups of G. Since the conjugate of a Sylow p-subgroup is again a Sylow p-subgroup, the action induced by conjugation on $Sub(G)$ preserves $Syl_p(G)$.

Theorem 4.2.1.5. *Let G be a finite group and $p||G|$ a prime. If $Syl_p(G)$ is the set of Sylow p-subgroups of G, viewed as a G-set by means of conjugation, then*

1. *$Syl_p(G)$ is non-empty*
2. *$Syl_p(G)$ consists of a single G-orbit.*

Choose a point in $Syl_p(G)$: this corresponds to fixing a Sylow p-subgroup P of G. Consider the action of P on $Syl_p(G)$ induced by the inclusion $P \hookrightarrow G$. The action of P on $Syl_p(G)$ fixes at least 1 point of $Syl_p(G)$, namely P. Suppose $Q \subset G$ corresponds to some other point of $Syl_p(G)$ fixed by conjugation by P, i.e., Q is a Sylow p-subgroup of G, and Q is stable by conjugation by every $p \in P$. To say that Q is stable by conjugation by any element of P is equivalent to saying that $P \subset N_G(Q)$. Now, Q is normal in $N_G(Q)$ by construction, and $N_G(Q)$ is the largest subgroup of G in which Q is normal. Since $N_G(Q) \subset G$, it follows that P and Q are Sylow subgroups of $N_G(Q)$ as well. Thus, by another application of the second Sylow theorem, we conclude that P is conjugate to Q in $N_G(Q)$. Since Q is normal in $N_G(Q)$ and P is conjugate in $N_G(Q)$ to it, it follows that $P = Q$. In other words, the action of P on $Syl_p(G)$ has at most 1 fixed point, which is P itself, and we have established the following fact.

Proposition 4.2.1.6. *Suppose G is a finite group and $p||G|$. If $P \in Syl_p(G)$ is a Sylow p-subgroup, then the P-action on $Syl_p(G)$ induced by conjugation has precisely 1 fixed point.*

Remark 4.2.1.7. I think of Theorem 4.2.1.5 in conjunction with Proposition 4.2.1.6 as the "geometric" content of the Sylow theorems.

4.2.2 Sylow's theorems: refinements

We may now deduce the numerical content of the Sylow theorems by analyzing $Syl_p(G)$ in more detail. Let n_p be $|Syl_p(G)|$, i.e., the number of distinct Sylow p-subgroups of G. Upon choosing a point, since $Syl_p(G)$ consists of a single orbit, the orbit-stabilizer formula yields a relationship between the normalizer of a Sylow P-subgroup and the number of Sylow subgroups.

Corollary 4.2.2.1. *Suppose G is a finite group, p is a prime dividing $|G|$, and $P \subset G$ is a Sylow p-subgroup (i.e., a choice of point in $Syl_p(G)$). The equality $n_p = |G/N_G(P)|$ holds, i.e., the number of Sylow p-subgroups is precisely equal to the index of the normalizer of a fixed Sylow p-subgroup in G.*

Proof. By Theorem 4.2.1.3, the orbit of the conjugation action on $Sub(G)$ has precisely 1 orbit, namely the subset of Sylow p-subgroups $Syl_p(G)$. If P is a Sylow p-subgroup of G, then we may consider $N_G(P)$, the normalizer of P in G. The stabilizer of an element of $Sub(G)$ by the conjugation action is precisely its normalizer. Combining these facts, the stabilizer of an element P of $Syl_p(G)$ for the action induced by conjugation is precisely $N_G(P)$. Therefore, the orbit-stabilizer formula applied to the action induced by conjugation on $Sub(G)$ tells us that the number of Sylow p-subgroups times the order of $N_G(P)$ is the order of the group. In other words, $n_p = |G/N_G(P)|$. □

The above corollary allows us to provide one answer to the question: when is a Sylow p-subgroup normal? Indeed, the corollary tells us that P is normal if and only if $N_G(P) = G$, i.e., $n_p = 1$.

Corollary 4.2.2.2. *If G is a finite group, $p||G|$, then a Sylow p-subgroup is normal if and only if $n_p = 1$.*

By replacing our appeal to the orbit stabilizer formula by appeal to Lemma 4.1.4.1, we may deduce additional properties of n_p. Since P is a finite p-group, it follows that

$$n_p = |Syl_p(G)| \cong |Syl_p(G)^P| \mod p,$$

i.e., the number of Sylow p-subgroups is congruent to the number of fixed points for the P-action on $Syl_p(G)$ by conjugation. In conjunction with Proposition 4.2.1.6, we conclude that $n_p \equiv 1 \mod p$. Finally, using this fact, we may refine our observation above that $n_p = |G/N_G(P)|$ above. Since $|G| = p^r m$ with $gcd(p,m) = 1$, it follows that n_p divides p^r or $n_p|m$. However, since $n_p \equiv 1 \mod p$, it follows that n_p cannot divide p^r, so it must divide m. Putting all of this together, we have established the following result.

Theorem 4.2.2.3 (Sylow III)**.** *Suppose G is a finite group and $|G| = p^n m$ with m coprime to p. If n_p is the number of Sylow p-subgroups of G, then*

i) $n_p \equiv 1 \mod p$.

ii) $n_p|m$, *and*

4.2.3 Non-existence of simple groups of various orders

We now present some applications of the Sylow theorems.

Lemma 4.2.3.1. *There is no simple group of order* 30.

Proof. Suppose G is a simple group of order 30. From the congruences in the Sylow theorem, see that $n_2 \equiv 1 \mod 2$ and $n_2|30$, i.e., n_2 is either $1, 3, 5$ or 15. Similarly, $n_2 \equiv 1 \mod 3$ and $n_2|10$; therefore $n_3 = 1$ or $n_3 = 10$. Finally, $n_5 \equiv 1 \mod 5$ and $n_5|6$; therefore $n_5 = 1$ or $n_5 = 6$.

If G is simple, then n_2, n_3 and n_5 cannot be equal to 1, since otherwise G would have a non-trivial proper normal subgroup. Therefore, either $n_2 = 3, 5$ or 15, and $n_3 = 10$ and $n_5 = 6$.

A Sylow p-subgroup in each of the above cases is cyclic of order p. Therefore, such a subgroup is generated by any non-zero element. Thus, for example, the condition $n_2 = 15$, gives 15 distinct subgroups of order 2; this accounts for 15 distinct elements of G of order 2 and 16 elements in total since we include the identity. Likewise, $n_3 = 10$ gives 20 non-identity elements (2 for each distinct Sylow 3-subgroup), and $n_5 = 6$ gives 24 non-identity elements (4 for each distinct Sylow 5-subgroup). Since the order of an element is well-defined, it follows that all of these elements are distinct. Therefore, if G was simple, it must have at least $1+15+20+24$ elements, which contradicts our assumption that it had 30 elements. □

Lemma 4.2.3.2. *There is no simple group of order* 36.

Proof. Suppose G is a group of order $36 = 2^2 3^2$. Appealing to the Sylow theorems, one sees that a Sylow 2-subgroup of G has either 1, 3 or 9 distict conjugates while a Sylow 3-subgroup has either 1 or 4 distinct conjugates conjugates. We eliminate the possibility that $n_2 = n_3 = 1$ because of simplicity of G. Thus, there must be 3 or 9 Sylow 2-subgroups and 4 Sylow 3-subgroups.

The conjugation action of G on itself induces an action on $Syl_p(G)$. In the former case, this corresponds to a homomorphism $G \to S_3$ or a homomorphism $G \to S_9$, while in the latter, we obtain a homomorphism $G \to S_4$. In each case, the kernel of such a group homomorphism is a normal subgroup of G. By assumption, there is more than 1 Sylow p-subgroup for either $p = 2$ or 3, and thus in each case G must act non-trivially on the set $Syl_p(G)$. Since G is simple, it follows that the kernel of such a homomorphism is necessarily the trivial subgroup of G, i.e., each homomorphism considered above is injective. In particular, we conclude that there is an injective homomorphism $G \to S_4$, which is a contradiction, since $|G| = 36 > 24 = |S_4|$. □

4.3 Lecture 14: Group extensions

4.3.1 Groups of order pq

Above, we saw that groups of order p^2 were always abelian. We can analyze groups G of order pq in a similar fashion using the Sylow theorems. Let us assume for simplicity that $p > q$. Now, $n_p \cong 1 \mod p$ and $n_p|q$. The second condition gives $n_p = 1$ or q. Since $p > q$, the first condition guarantees that $n_p = 1$. Thus, G has $\mathbb{Z}/p$ as a normal subgroup. Similarly, $n_q \cong 1 \mod q$ and $n_q|p$. Thus, the second condition yields $n_q = 1$ or p. If $p-1|q$, then then there are two possibilities for n_q, but if not, we know $n_q = 1$. In that case, we have the following result.

Proposition 4.3.1.1. *If G is a finite group of order pq and $p-1$ does not divide q, then G is isomorphic to $\mathbb{Z}/pq$.*

Proof. In this case, we know that $n_p = 1$ and $n_q = 1$. In particular, this means that every element of order p in G is contained in the Sylow p-subgroup, and every element of order q is contained in the Sylow q-subgroup. Thus, the elements of order p, q and the identity give a total of $1+(p-1)+(q-1) = p+q-1$ elements. However, $pq > p+q-1$, so G must have a non-identity element whose order is different from p or q. Such an element must have order pq and generates a cyclic subgroup of G isomorphic to $\mathbb{Z}/pq$; this subgroup is necessarily isomorphic to G. □

4.3.2 Extensions I: "split" extensions

We now analyze the case $p-1|q$. Recall that $p > q$ implied that $n_p = 1$, so there is always a normal cyclic subgroup of order p. In other words, we are in the following situation: there is an exact sequence of the form

$$1 \longrightarrow \mathbb{Z}/p \longrightarrow G \longrightarrow \mathbb{Z}/q \longrightarrow 1.$$

Thus, we would like to understand extensions of $\mathbb{Z}/q$ by $\mathbb{Z}/p$.

Let us understand the situation in slightly greater generality: suppose N is a normal subgroup of a group G with quotient Q, i.e., we have a short exact sequence of the form

$$1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1.$$

To understand the group structure on G is tantamount to understanding the multiplication table in G. Since the function $\varphi : G \to Q$ is surjective, we can always pick a function (just of sets!) $\theta : Q \to G$ such that $Q \to G \to Q$ is the identity on Q (i.e., we pick a single representative in the pre-image of each $q \in Q$ under the surjective map $G \to Q$); we will refer to the choice of θ as a *section* of φ. The simplest case is where we can pick θ to be a group homomorphism; in this case, we will say that the exact sequence above is *split*.

In analyzing groups of order pq, we can always choose a splitting. When $Q = \mathbb{Z}/q$, a choice of section that is actually a homomorphism corresponds to an element of order q in G (the choice of a generator of $\mathbb{Z}/q \subset G$). Thus, we need to know that G has an element or order q; however, if $|G| = pq$, then since G has a Sylow q-subgroup, it contains a subgroup of order q and thus an element of order q as well. Thus, we will, for the time being, focus on the case where θ may be chosen to be a group homomorphism. Note: examples we already know show that we may not always be able to choose θ to be a homomorphism (see Example 4.3.2.4).

By the universal property of the Cartesian product, the inclusion map $N \to G$ and the function $\theta : Q \to G$ give a function

$$N \times Q \xrightarrow{i,\theta} G;$$

this map is a bijection by construction. The multiplication on G can be viewed as a product operation on the set $N \times Q$, which we would like to describe in more detail.

Since N is normal, N is stable by conjugation in G. Since conjugation is a homomorphism, the conjugation action of G on H defines a homomorphism $G \to Aut(N)$. Pre-composing with the homomorphism $\theta : Q \to G$ then gives a homomorphism $Q \to Aut(N)$ that sends an element $q \in Q$ to conjugation of N by $\theta(q)$. (In general, if θ may not be chosen to be a group homomorphism, then the composite is simply a function). Given $q \in Q$, we write $\omega_{\theta(q)}$ for the automorphism of N determined by $\theta(q)$, and the fact that θ is a homomorphism implies that the formula

$$\omega_{\theta(qq')} = \omega_{\theta(q)\theta(q')} = \omega_{\theta(q)}\omega_{\theta(q')}$$

holds. Equivalently, $\omega_{\theta(q)}\omega_{\theta(q')}\omega^{-1}_{\theta(qq')}$ would be the identity in $Aut(N)$.

Now, we would like to write down a formula for multiplication in G, and the idea is to try to use θ as a way to modify the multiplication in the Cartesian product $N \times Q$. Since $N \times Q \to G$ is a bijection, every $g \in G$ may be written as $g = n\theta(q)$. We can be really explicit about this here: if $f : G \to Q$ is the homomorphism in the extension, then given an element $g \in G$, we can look at $\theta(f(g))$, which is an element of G. Since θ is a section, the two elements g and $\theta(f(g))$ differ by an element in the kernel of f, i.e., there is a unique element $n \in N$ such that $g = n\theta(f(g))$.

To write down the multiplication in G, we now take pairs $g = (n, \theta(q))$ and $g' = (n', \theta(q'))$ and multiply them in G. By means of the discussion above, multiplication is given by juxtaposition in G, and then

$$(n\theta(q))(n'\theta(q')) = n\theta(q)n'\theta(q)^{-1}\theta(q)\theta(q') = (n\omega_{\theta(q)}(n'), \theta(q)\theta(q')).$$

Since θ is a homomorphism, one may show that this yields a new group structure on the set $N \times Q$ with identity (e_N, e_Q).

Definition 4.3.2.1. If N and Q are groups, and $\omega : Q \to Aut(H)$ is a group homomorphism, then the semi-direct product $N \rtimes_\omega Q$ is the group with underlying set the Cartesian product $(N \times Q)$, the identity element is (e_H, e_Q), multiplication is given by the formula $(n, q) \cdot (n', q') = (n\omega(q)(n'), qq')$, and inversion is given by $(n, q)^{-1} = (\omega(q^{-1}(n^{-1}))q^{-1})$.

Remark 4.3.2.2. If ω is the trivial homomorphism, then $N \rtimes Q$ is simply $N \times Q$. Different homomorphisms $\varphi : Q \to Aut(N)$ may yield non-isomorphic groups!

Proposition 4.3.2.3. *Given an extension of the form* $1 \to N \to G \to Q \to 1$*, a choice of splitting* $\theta : Q \to G$ *determines an isomorphism of G with a semidirect product of the form* $N \rtimes_\varphi Q$*, where* $\varphi : Q \to Aut(N)$ *is the composite of* θ *and the action of G on N by conjugation.*

In order to analyze semi-direct products, we need to understand the group $Aut(N)$. In our motivating examples $N = \mathbb{Z}/p$ and so we want to know $Aut(\mathbb{Z}/p)$. The n-th power map $\mathbb{Z}/p \to \mathbb{Z}/p$ is an isomorphism if $(n, p) = 1$. Since any automorphism is determined by where it sends a cyclic generator, we conclude that $|Aut(\mathbb{Z}/p)| = p - 1$, and combining these two facts we conclude that $Aut(\mathbb{Z}/p)$ is cyclic of order $p - 1$.

Example 4.3.2.4. Even when Q is cyclic, we may not always be able to choose θ to be a homomorphism. Indeed, for a prime p consider the group $\mathbb{Z}/p^2$ which can be written as an extension

$$1 \longrightarrow \mathbb{Z}/p \longrightarrow \mathbb{Z}/p^2 \longrightarrow \mathbb{Z}/p \longrightarrow 1.$$

Since $Aut(\mathbb{Z}/p) = \mathbb{Z}/(p-1)$, there are no non-trivial homomorphism $\mathbb{Z}/p \to \mathbb{Z}/(p-1)$ and thus $\mathbb{Z}/p^2$ is not a semi-direct product. Equivalently, we cannot find a section of the surjection that is a group homomorphism.

Example 4.3.2.5. Consider the symmetric group S_n and the sign homomorphism $S_n \to \mathbb{Z}/2$. There is a short exact sequence

$$1 \longrightarrow A_n \longrightarrow S_n \longrightarrow \mathbb{Z}/2 \longrightarrow 1.$$

The choice of a transposition in S_n determines a subgroup of S_n of order 2 that determines a splitting of the sign homomorphism. In S_n, all transpositions are conjugate, so one concludes that S_n is the semi-direct product of A_n and $\mathbb{Z}/2$ with the homomorphism $\omega : \mathbb{Z}/2 \to Aut(A_n)$ defined by conjugation by a transposition.

Groups of order pq, $p > q$ prime

We now observe that for groups of order pq, the extension we considered above may always be assumed split.

Lemma 4.3.2.6. *If G has order pq, then a choice of Sylow q-subgroup of G determines a splitting of the exact sequence $1 \to \mathbb{Z}/p \to G \to \mathbb{Z}/q \to 1$. In particular, every group of order pq is a semi-direct product.*

Proof. Let P be the (normal) p-Sylow subgroup of G, and let Q by a (non-normal) q-sylow subgroup. The quotient G/P is a group of order q. Since any non-identity element of Q has order q, it follows that $Q \cap P = e$. Therefore, the composite map $Q \to G \to G/P$ is necessarily an isomorphism. In other words, any choice of a Sylow q-subgroup of G (equivalently, any choice of an element of order q) determines a section of $G \to G/P$ that is a homomorphism, and G is necessarily a non-trivial semi-direct product. □

Since $Aut(\mathbb{Z}/p) = \mathbb{Z}/p - 1$, there is a non-trivial homomorphism $\mathbb{Z}/q \to Aut(\mathbb{Z}/p)$ if and only if $q|p-1$. In that case, if G is a group of order pq, then since all Sylow q-subgroups are conjugate, it follows that up to conjugation, there two possible choices of homomorphism $\mathbb{Z}/q \to Aut(\mathbb{Z}/p)$: the trivial homomorphism and a non-trivial homomorphism. I leave it to you to turn this observation into a careful proof of the following fact.

Lemma 4.3.2.7. *If $q|p-1$, then there is a unique, up to isomorphism, non-trivial semi-direct product of the form $\mathbb{Z}/p \rtimes \mathbb{Z}/q$.*

Thus, putting everything together, we have proven the following result.

Proposition 4.3.2.8. *Suppose $p > q$ are primes. If $p-1$ does not divide q, $\mathbb{Z}/pq$ is the unique up to isomorphism group of order pq. If $p-1|q$, then there are two isomorphism classes of groups of order pq: the cyclic group $\mathbb{Z}/pq$ and the semi-direct product of the previous lemma.*

4.3.3 Groups of order p^3 I

We saw that groups of order p^2 were always abelian. We now analyze groups of order p^3 using the Sylow theorems. Using the semi-direct product construction we can obtain a new group of order p^3 that is not abelian.

Example 4.3.3.1. The dihedral group of order 8 is a semi-direct product of $\mathbb{Z}/4$ and $\mathbb{Z}/2$.

Recall that we proved that any p-group has a non-trivial center. Thus, if G has order p^3, there are three possibilities for the order of the center: $\mathbb{Z}(G)$ could have order p^3, p^2 or p. In the first case, $Z(G) = G$ by comparing orders and we conclude that G is abelian, in which case it must be isomorphic to $\mathbb{Z}/p^{\times 3}$, $\mathbb{Z}/p \times \mathbb{Z}/p^2$ or $\mathbb{Z}/p^3$. Thus, the first possibly interesting case is that when $\mathbb{Z}(G)$ has order p^2. In this case, the quotient of G by its center is a cyclic group of order p and a slight abstraction of our proof that groups of order p^2 is abelian yields the following result.

Lemma 4.3.3.2. *If G is a finite group and $G/Z(G)$ is cyclic, then G is abelian.*

Thus, the only interesting case is when $Z(G)$ is $\mathbb{Z}/p$. In that case, the quotient $G/Z(G)$ has order p^2 and is thus abelian, i.e., it is isomorphic to $\mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$. Thus, if we want to try to build groups of order p^3 as semi-direct products, we either need a non-trivial homomorphism $\mathbb{Z}/p^2 \to Aut(\mathbb{Z}/p)$ or a homomorphism $\mathbb{Z}/p \times \mathbb{Z}/p \to Aut(\mathbb{Z}/p)$. Note that there are no such non-trivial homomorphisms! Indeed, any such group has to have order dividing $p - 1$, and must have order either $1, p$ or p^2, which is a contradiction. Nevertheless, we will see that it is possible to build non-trivial non-split extensions in these cases!

Chapter 5

Extensions and cohomology

5.1 Lecture 15: Extensions continued

Semi-direct product groups of order p^3

While the center of a non-abelian group of order p^3 necessarily has order p, a non-abelian group of order p^3 could have $\mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$ as a normal subgroup that is *not* equal to the center. In either case, we would have

$$1 \longrightarrow N \longrightarrow G \longrightarrow \mathbb{Z}/p \longrightarrow 1.$$

In this situation it *is* possible to build non-trivial split extensions. To see this, we need to analyze homomorphisms $\mathbb{Z}/p \to Aut(\mathbb{Z}/p^2)$ or homomorphisms $\mathbb{Z}/p \to Aut(\mathbb{Z}/p \times \mathbb{Z}/p)$. The first case is easy, generalizing what we said about the cyclic group above.

Lemma 5.1.0.3. *The automorphism group of $\mathbb{Z}/p^2$ is cyclic of order $p(p-1)$.*

There is a non-trivial homomorphism $\mathbb{Z}/p \to Aut(\mathbb{Z}/p^2\mathbb{Z})$; indeed, up to conjugation in the target, there is a unique such non-trivial homomorphism. Now, consider the semi-direct product

$$(\mathbb{Z}/p^2\mathbb{Z}) \rtimes_{\varphi} \mathbb{Z}/p,$$

where φ sends a generator of $\mathbb{Z}/p\mathbb{Z}$ to a non-trivial automorphism of order p in $\mathbb{Z}/p^2\mathbb{Z}$.

Lemma 5.1.0.4. *The group $M_3(p) := \mathbb{Z}/p^2 \rtimes \mathbb{Z}/p$ is a non-abelian group of order p^3.*

Proof. To see this, it suffices to show that $\mathbb{Z}/p^2$ is not equal to the center of $M_3(p)$ since if it was in the center (indeed, if it were in the center, then the quotient would be a cyclic group of order p and thus the whole group would be abelian; so this condition is equivalent to the semi-direct product being non-abelian in this case).

The multiplication in $M_3(p)$ is defined on a pair (a, b) with $a \in \mathbb{Z}/p^2$, $b \in \mathbb{Z}/p$ by the formula

$$(a, b) * (a', b') = (a + \varphi(b')a', b + b').$$

Now, simply take $b = b' = 1$, and $a = 0$. In that case, $(0, b) * (a', b) = (\varphi(1)a', 2)$, while $(a', b) * (0, b) = (a', 2)$. As long as $\varphi(1)$ is not the identity automorphism, we are guaranteed that we can find at least 1 a' such that $\varphi(1)a' \neq a'$. □

5.1.1 Groups of order p^3 continued

We can also consider the other possibility: i.e., form a semi-direct product $(\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_{\varphi} \mathbb{Z}/p$ by means of a homomorphism $\mathbb{Z}/p \to Aut(\mathbb{Z}/p \times \mathbb{Z}/p)$.

Lemma 5.1.1.1. *For any prime p, $Aut(\mathbb{Z}/p \times \mathbb{Z}/p) \cong GL_2(\mathbb{Z}/p)$.*

Recall that $|GL_2(\mathbb{Z}/p)| = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$. Any subgroup of order p is a Sylow p-subgroup, and therefore conjugate to $U(\mathbb{F}_p) \cong \mathbb{Z}/p$. Thus, there are, up to conjugation in the target, two homomorphisms $\mathbb{Z}/p \to Aut(\mathbb{Z}/p \times \mathbb{Z}/p)$: the trivial homomorphism and a non-trivial homomorphism. The non-trivial homomorphism is generated by an element of order p in $GL_2(\mathbb{F}_p)$, which we may take to be

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

for example. A non-trivial homomorphism φ gives rise to a semi-direct product of $(\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_{\varphi} \mathbb{Z}/p$.

Lemma 5.1.1.2. *The semi-direct product $(\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_{\varphi} \mathbb{Z}/p$ for a non-trivial homomorphism $\mathbb{Z}/p \to GL_2(\mathbb{F}_p)$ is a non-abelian group of order p^3.*

Proof. Here, the multiplication is given by

$$((a, b), c) * ((a', b'), c') = ((a, b) + \varphi(c)((a', b')), c + c')$$

Now, $\varphi(c)(a', b') = (a' + cb', b')$. Thus, the group we obtain is

$$((a, b), c) * ((a', b'), c') = ((a + a' + cb', b + b'), c + c').$$

Taking $a = a' = c' = b = 0$, we get the formula

$$((0, 0), c) * ((0, b'), 0) = ((cb', b'), c)$$

while

$$((0, b'), 0) * ((0, 0), c) = ((0, b'), c).$$

□

The natural question is about the relationship between the Heisenberg group just defined and the group $M_3(p)$ constructed in the previous lecture.

5.1.2 Extensions II: extensions by abelian groups

Example 5.1.2.1. The quaternion group of order 8, often denoted Q_8, is the group presented by $\langle i, j, k | i^2 = j^2 = k^2 = ijk \rangle$. The common element $i^2 = j^2 = k^2 = ijk$ lies in the center of Q_8 and is often denoted -1. Thus, $i^3 = -i$, $j^3 = -j$ and $k^3 = -k$. You can check that this group has 8 elements: $\pm 1, \pm i, \pm j, \pm k$. Observe also that it is non-abelian: $ijk = -1$ and therefore $ij = -k^{-1}$. Since $k^4 = 1$, it follows that $k^{-1} = -k$. Thus, $ij = k$. Similarly, one shows that $ji = -k$ so $ij \neq ji$. You may show that the quaternion group of order 8 is not the semi-direct product of any two non-trivial subgroups.

As before, consider a sequence of groups of the form

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} Q \longrightarrow 1.$$

We would like to approach the problem of classifying group structures on extensions by refining our analysis of group structures in the semi-direct product case. A choice of set-theoretic section $\theta : Q \to G$ determines a bijection between $N \times Q$ and G, and we will attempt to write down "twists" of the group structure on $N \times Q$ to obtain all possible group structures on extensions. The data we attach to a given extension will *a priori* depend on the choice of section θ, but to make sure the outcome is intrinsic to the extension itself, we will need to analyze the dependence on θ of whatever data we attach to the extension.

Each $g \in G$ acts on N by conjugation and thus we always have a function $G \to Aut(N)$; this function is a homomorphism. Let θ be a section of π. Composing θ and the homomorphism $G \to Aut(N)$, we obtain a function $\omega : Q \to Aut(N)$ defined by

$$\omega_q(n) = \theta(q) n \theta(q)^{-1}$$

Since θ fails to be a homomorphism, we cannot expect this function to be a homomorphism in general either.

If θ' is another such section, then there is an associated function $\omega' : Q \to Aut(N)$ defined in an analogous fashion. To analyze the relationship between ω and ω', we need to quantify the relationship between θ and θ', we define a new function ψ that measures the difference, i.e.,

$$\theta(q) = \psi(q)\theta'(q),$$

so $\psi(q)\theta(q)\theta'(q)^{-1}$. Since π is a group homomorphism and θ is a section of π, we see that

$$\pi(\psi(q)) = \pi(\theta(q)\theta'(q)^{-1}) = \pi(\theta(q))\pi(\theta(q))^{-1} = qq^{-1} = 1,$$

i.e., that $\psi(q) \in N$. In that case,

$$\omega_q(n) = \theta(q)n\theta(q)^{-1} = \psi(q)\theta'(q)n\theta'(q)^{-1}\psi(q)^{-1} = \psi(q)\omega'_q(n)\psi(q)^{-1}.$$

In other words, ω_q and ω'_q differ by conjugation by an element of N.

Now, if H is any group, the image of the homomorphism $H \to Aut(H)$ sending $h \to c_h(-)$ is called the subgroup of inner automorphisms and denoted $Inn(H)$. The subgroup $Inn(H) \subset Aut(H)$ is a normal subgroup, and we define $Out(H) := Aut(H)/Inn(H)$. The discussion of the previous paragraph shows that the composite of $\omega : Q \to Aut(N)$ with the quotient map $Aut(N) \to Out(N)$ defines a function $\omega : Q \to Out(N)$ that does not depend on choice of section θ, i.e., is intrinsic to the extension.

If H is an abelian group, then conjugation is trivial, so $Inn(H)$ is the trivial subgroup of $Aut(H)$. We now consider extensions

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

where A is an abelian group. In that case, we obtain an intrinsically defined function $\omega : Q \to Aut(A)$. There is one case where further simplifications appear: if $A \subset Z(G)$. In that case, the conjugation action of G on A is trivial, which means that $\omega : Q \to Aut(A)$ is the trivial homomorphism. We will refer to extensions with $A \subset Z(G)$ as *central* extensions of Q by A.

As in the split case, we would like to write a formula for multiplication in G in terms of multiplication in Q and A. Since the function $G \to Q$ is surjective, we can, as above, choose a section $\theta : Q \to G$, i.e., we pick a coset representative of each $q \in Q$ under the identification $Q \cong G/A$. As in the split case, the choice of θ allows us to represent every element of G uniquely in the form $(a, \theta(q))$. Again, we would like to describe a multiplication in G in terms of the data in hand. We have already treated the case where θ was a group homomorphism, so let us assume that is no longer the case.

As before, we can write

$$gg' = a\theta(q)a'\theta(q') = a\theta(q)a'\theta(q)^{-1}\theta(q)\theta(q') = a\omega_{\theta(q)}(a')\theta(q)\theta(q').$$

Since θ is no longer assumed to be a group homomorphism, the product $\theta(q)\theta(q')$ will differ from the $\theta(qq')$. Our goal is simple: let us try to compare the multiplication on G (via the above formula) with the multiplication in the semi-direct product. To do this, we need to first quantify the extent to which θ fails to be a group homomorphism as this will allow us to measure how $\theta(q)\theta(q')$ deviates from the usual product in Q.

The failure of θ to be a group homomorphism can be quantified by defining a function that measures this failure. Namely, set

$$f(q_1, q_2) = \theta(q_1)\theta(q_2)\theta(q_1q_2)^{-1}$$

so that $\theta(q_1)\theta(q_2) = f(q_1, q_2)\theta(q_1q_2)$. By construction $f(q_1, q_2) = e$ precisely if $\theta(q_1q_2) = \theta(q_1)\theta(q_2)$.

Note that $\pi(f(q_1, q_2)) = \pi(\theta(q_1)\theta(q_2)\theta(q_1q_2)^{-1})$ and the latter expression is equal to $1_Q \in Q$ since π is a homomorphism and θ is a section of π. Thus, $f(q_1, q_2)$ may be viewed as a function $Q \times Q \to A$. The group structure on G imposes restrictions on f that we now explore. This function f is usually called a *factor set*. Furthermore, our definition of f depends on the choice of θ and we need to explore this dependence.

Restrictions on factor sets arising from the group structure

Given an extension

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

where A is an abelian group associativity of multiplication in G imposes conditions on f. Indeed, grouping one way we see that:

$$\theta(q_1)\theta(q_2)\theta(q_3) = f(q_1,q_2)\theta(q_1q_2)\theta(q_3) = f(q_1,q_2)f(q_1q_2,q_3)\theta(q_1q_2q_3),$$

while grouping the other way, we similarly conclude

$$\begin{aligned}\theta(q_1)\theta(q_2)\theta(q_3) &= \theta(q_1)f(q_2,q_3)\theta(q_2q_3) = \theta(q_1)f(q_2,q_3)\theta(q_1)^{-1}\theta(q_1)\theta(q_2q_3)\\ &= \theta(q_1)f(q_2,q_3)\theta(q_1)^{-1}f(q_1,q_2q_3)\theta(q_1q_2q_3).\end{aligned}$$

Conjugation by $\theta(q_1)$ corresponds to applying ω_{q_1} to $f(q_2,q_3)$, thus we obtain the identity

$$f(q_1,q_2)f(q_1q_2,q_3) = \omega_{q_1}(f(q_2,q_3))f(q_1,q_2q_3),$$

which we refer to as the *generalized cocycle identity*. Likewise, the identity proper for multiplication implies that $\theta(1_Q)\theta(q) = f(1_Q,q)\theta(q)$, i.e., $\theta(1_Q) = f(1_Q,q)$. Similarly, $\theta(1_Q) = f(q,1_Q)$. For simplicity, we will assume that $\theta(1_Q) = 1_G$, so $f(1_Q,q) = f(q,1_Q) = 1_G$. Notice that when $A \subset Z(G)$, ω_{q_1} acts trivially, and therefore the cocycle identity simplifies.

Putting everything together, we have extracted from an extension of a group Q by an abelian group A the following data:

- a homomorphism $\omega : Q \to Aut(A)$ (i.e., an action of Q on A),
- a *normalized factor set*, i.e., a function $f : Q \times Q \to A$ satisfying the following conditions:
  1. $f(q_1,q_2)f(q_1q_2,q_3) = \omega_{q_1}(f(q_2,q_3))f(q_1,q_2q_3)$ for every $q_1,q_2,q_3 \in Q$; and
  2. $1_A = f(1_Q,q) = f(q,1_Q)$.

In fact, this data determines the group G uniquely up to isomorphism since given an action of Q on A and a factor set f satisfying these above two conditions, we may define a multiplication on the product $A \times Q$ by the formula

$$(a,q)(a',q') = (a\omega_{\theta(q)}(a'), f(q,q')qq')$$

and the formulas above show that this multiplication equips $A \times Q$ with a group structure with identity $(1_A, 1_Q)$ (and appropriate formula for inversion).

We now analyze the dependence of the factor set on the choice θ of section. If θ' is another section, we now analyze how ω and f change. As before, write $\theta(q) = \psi(q)\theta'(q)$. We observed above that if A is abelian, then ω and ω' coincide because $Inn(A)$ is trivial. Thus, it remains to analyze the dependence of f on θ.

$$f(q_1,q_2)\theta(q_1q_2) = f(q_1,q_2)\psi(q_1q_2)\theta'(q_1q_2),$$

while

$$\begin{aligned}\theta(q_1)\theta(q_2) &= \psi(q_1)\theta'(q_1)\psi(q_2)\theta'(q_2) = \psi(q_1)\theta'(q_1)\psi(q_2)\theta'(q_1)^{-1}\theta'(q_1)\theta'(q_2)\\ &= \psi(q_1)\omega'_{q_1}(\psi(q_2))f'(q_1,q_2)\theta'(q_1q_2).\end{aligned}$$

In other words, the identity

$$f(q_1,q_2)\psi(q_1q_2) = \psi(q_1)\omega_{q_1}(\psi(q_2))f'(q_1,q_2)$$

holds. Since A is abelian, this can be rewritten as

$$f(q_1,q_2) = \psi(q_1)\omega_{q_1}(\psi(q_2))\psi(q_1q_2)^{-1}f'(q_1,q_2)$$

i.e., if θ and θ' are different sections, $f(q_1,q_2)$ and $f'(q_1,q_2)$ differ by $\psi(q_1)\omega'_{q_1}(\psi(q_2))\psi(q_1q_2)^{-1}$ for some function $\psi : Q \to A$. Note that our simplifying assumption that $\theta(1_Q) = 1_G$ implies that $\psi(1_Q) = 1_A$.

The condition in the previous paragraph provides an equivalence relation $\sim$ on the set of normalized factor sets: we say that $f \sim f'$ if there exists a function $\psi : Q \to A$ such that $\psi(1_Q) = 1_A$ such that $f(q_1,q_2) = \psi(q_1)\omega'_{q_1}(\psi(q_2))\psi(q_1q_2)^{-1}f'(q_1,q_2)$. I leave it as an exercise to check that this relation is actually an equivalence relation (straightforward computation).

Theorem 5.1.2.2. *Suppose Q is a group, A is an abelian group, and $\omega : Q \to Aut(A)$ is an action of Q on A. There is a bijection between the set of extensions G of Q by A with the specified action of Q on A and the set of equivalence classes of normalized factor sets, i.e., functions $f : Q \times Q \to A$ satisfying the following conditions:*

1. *$f(q_1,q_2)f(q_1q_2,q_3) = \omega_{q_1}(f(q_2,q_3))f(q_1,q_2q_3)$ for every $q_1,q_2,q_3 \in Q$; and*
2. *$1_A = f(1_Q,q) = f(q,1_Q)$;*

and $f \sim f'$ if there exists a function $\psi : Q \to A$ such that $\psi(1_Q) = 1_A$ such that $f(q_1,q_2) = \psi(q_1)\omega_{q_1}(\psi(q_2))\psi(q_1q_2)^{-1}f'(q_1,q_2)$.

Proof. In brief, to go from an extension with fixed ω to a normalized factor set satisfying the cocycle condition, we simply choose a section. Conversely, given an action ω and a normalized factor set f, we define a multiplication on $A \times Q$ by means of the formula

$$(a_1,q_1)(a_2,q_2) = (a_1\omega_{q_1}(a_2)f(q_1,q_2), q_1q_2).$$

One checks as before this defines a group structure on $A \times Q$ and that the functions $a \mapsto (a,1)$ and $(a,q) \mapsto q$ identify A as a normal subgroup of $A \times Q$ with this multiplication with quotient Q. The explicit formulas written above show that the two constructions are mutually inverse bijections. □

Remark 5.1.2.3. After Theorem 5.1.2.2, the problem of classifying extensions of the form $1 \to A \to G \to Q \to 1$ thus depends on the problem of classifying homomorphisms $Q \to Aut(A)$ (since we have described extensions with a fixed such action). Next time, we will reformulate the classification above more explicitly.

5.2 Lecture 16: Extensions and group cohomology

At the end of last class, we established some relationship between extensions and factor sets satisfying a generalized cocycle condition. We now give an alternative description of this set that will identify additional structure and (eventually) be more amenable to computations.

5.2.1 The (generalized) cocycle condition revisited

Pointwise addition in A gives a way to add functions $Q \times Q \to A$. We write $Fun(Q \times Q, A)$ for the set of all functions (just as sets, not necessarily homomorphism). The set $Fun(Q \times Q, A)$ itself forms an abelian group under pointwise addition in A, and for this reason we use the additive notation for sums of functions. The function that is identically 0 necessarily satisfies $f(1_Q, q') = 0_A = f(q, 1_Q)$ and moreover, this function evidently satisfies the cocycle condition. If f and f' are *normalized*, in the sense that $f(1_Q, q') = 0_A = f(q, 1_Q)$, then their sum $f + f'$ has this property as well.

Lemma 5.2.1.1. *If $\omega : Q \to Aut(A)$ is an action, then the set of normalized cocycles satisfying the generalized cocycle identity forms a subgroup of $Fun(Q \times Q, A)$ under pointwise addition.*

Proof. We want to check that the sum of normalized cocycles is again a normalized cocyle. Since A is abelian, let us write the generalized cocycle condition additively as:

$$f(q_1, q_2) + f(q_1q_2, q_3) = \omega_{q_1}(f(q_2, q_3)) + f(q_1, q_2q_3)$$

Since ω is an automorphism of A, it follows that $\omega_q(f + f') = \omega_q(f) + \omega_q(f')$. It follows immediately that if f and f' satisfy the cocycle condition, then so does $f + f'$. □

Granted this result, we make the following definition.

Definition 5.2.1.2. We write $Z^2(Q, A, \omega)$ for the subgroup of $Fun(Q \times Q, A)$ consisting of normalized factor sets satisfying the generalized cocycle condition; elements of this group will be called 2-cocycles.

There is an alternative definition of $Z^2(Q, A, \omega)$ that makes it immediately apparent it is a subgroup. Define a function

$$d^2 : Fun(Q \times Q, A) \longrightarrow Fun(Q \times Q \times Q, A)$$

as follows: if $f \in Fun(Q \times Q, A)$, then set

$$d^2(f)(q_1, q_2, q_3) = \omega_{q_1} f(q_2, q_3) - f(q_1q_2, q_3) + f(q_1, q_2q_3) - f(q_1, q_2). \tag{5.2.1}$$

Observe that $d^2(f) = 0$ if and only if f satisfies the cocycle condition. Moreover, Lemma 5.2.1.1 shows that d^2 is a homomorphism of abelian groups and thus $Z^2(Q, A, \omega)$ is identified as the kernel of d^2.

Now, we want to analyze the equivalence relation on normalized factor sets we considered in our theorem. To begin, recall that if we obtained the factor set f from a section θ and f' from a section θ' then, f and f' were related. Indeed, if $\psi : Q \to A$ was defined by $\theta(q)\theta'(q)^{-1}$, the identity

$$f(q_1, q_2) + \psi(q_1q_2) = \psi(q_1) + \omega_{q_1}(\psi(q_2)) + f'(q_1, q_2)$$

holds (we write it additively now since A is abelian). Equivalently,

$$f(q_1, q_2) - f'(q_1, q_2) = \omega_{q_1}\psi(q_2) - \psi(q_1q_2) + \psi(q_1).$$

Since the set of 2-cocycles is a group, it follows that $\omega_{q_1}\psi(q_2) - \psi(q_1q_2) + \psi(q_1)$ is automatically a 2-cocyle as well.

Define

$$d^1 : Fun(Q, A) \longrightarrow Fun(Q \times Q, A) \tag{5.2.2}$$

by the formula

$$d^1(\psi)(q_1, q_2) = \omega_{q_1}\psi(q_2) - \psi(q_1 q_2) + \psi(q_1)$$

Once again, Lemma 5.2.1.1 implies that d^1 is a homomorphism. Thus, the image of d^1 is a subgroup of $Fun(Q \times Q, A)$. A straightforward direct computation shows that $im(d^1)$ is always contained in $Z^2(Q, A, \omega)$, i.e., $d^2 \circ d^1 = 0$. It follows that if $f \in Z^2(Q, A, \omega)$ is any 2-cocycle, and $\psi : Q \to A$ is a function, then $f + d^1(\psi)$ is also automatically a 2-cocycle. Since $Im(d^1)$ defines a (normal) subgroup of $Z^2(Q, A, \omega)$, there is an associated partition of the latter into cosets for this subgroup. Unwinding the definitions, it is immediate that the equivalence relation in Theorem 5.1.2.2 coincides with the equivalence relation arising from the partition into orbits.

Remark 5.2.1.3. In our formulation of Theorem 5.1.2.2, we considered normalized extensions. It is straightforward to show that any cocycle is equivalent to a normalized cocycle.

Definition 5.2.1.4. We write $B^2(Q, A, \omega)$ for the image of the homomorphism $Fun(Q, A) \to Z^2(Q, A, \omega)$ described above; elements of this group are called 2-coboundaries. We write $H^2(Q, A, \omega)$ for the quotient group $Z^2(Q, A, \omega)/B^2(Q, A, \omega)$, this group is called the *second cohomology group of* Q *with coefficients in* (A, ω).

Combining everything we have done so far, Theorem 5.1.2.2 may then be rephrased as follows.

Theorem 5.2.1.5. *Suppose* Q *is a group,* A *is an abelian group, and* $\omega : Q \to Aut(A)$ *is an action of* Q *on* A*. There is a bijection between the set of extensions* G *of* Q *by* A *with the specified action of* Q *on* A *and elements of the abelian group* $H^2(Q, A, \omega)$*.*

Remark 5.2.1.6. This theorem yields more than just a reformulation of our solution to the extension problem because $H^2(Q, A, \omega)$ is a group. In particular, we see that there is a well-defined procedure to *add* extension classes so that new extensions may be generated from old ones. In fact, if Q is finite and A is a finitely generated abelian group (e.g., finite abelian), then $Fun(Q^n, A)$ is again a finitely generated abelian group. It follows that, in that case, $H^2(Q, A, \omega)$ is automatically a finitely generated abelian group as well. Therefore, we may analyze this group by appealing to the structure theorem for finitely generated abelian groups.

Remark 5.2.1.7. Appendix A.2 contains various generalizations of Theorem 5.2.1.5 when one considers extensions of arbitrary groups.

Remark 5.2.1.8 (Classifying spaces and group cohomology). One may show that the group $H^2(Q, A, \omega)$ admits a topological interpretation. The description is simplest when Q is a finite group, so we impose that assumption. Define a topological space BQ as follows. Let EQ be a contractible space with free Q-action. To build such a space, take a faithful representation of Q over the complex numbers, i.e., pick an injective homomorphism $Q \to GL(V)$ where V is a complex vector space of some dimension n. Observe that Q acts diagonally on the direct sum $V^{\oplus N}$ for any $N > 0$. While Q fixes, for example, the origin, there is a maximal open subset U_N of $V^{\oplus N}$ on which Q acts freely (namely, take the complement of the locus of points $w \in V^{\oplus N}$ where w has a non-trivial stabilizer in Q. In the limit as $N \to \infty$, one obtains a space U_∞ that has a free action of Q. One can show that U_∞ is also contractible as a topological space because it is an increasing union of spaces U_N that have high codimension in a Euclidean space. The quotient U_∞/Q is a model for BQ.

In the special case where Q acts trivially on A, one may show that $H^2(BQ, A)$ (i.e., ordinary singular cohomology of the topological space BQ with coefficients in the abelian group A) coincides with $H^2(Q, A)$ defined above (ω has been suppressed because Q acts trivially on A). More generally, BQ as defined above is a topological space with fundamental group Q by construction. The action of Q on A determines a local coefficient system A_ω on BQ, and the group $H^2(Q, A, \omega)$ may be identified with the singular cohomology group $H^2(BQ, A_\omega)$.

If $Q = \mathbb{Z}/2$, then Q has a faithful representation on the 1-dimensional $\mathbb{C}$-vector space given by the sign action. Then, U_N is the complement of the origin in $\mathbb{C}^n$ and the diagonal action corresponds to the action sending a vector $(w_1, \ldots, w_n)$ to $(-w_1, \ldots, -w_n)$. The quotients $U_N/\mathbb{Z}/2$ are homotopy equivalent to $\mathbf{RP}^n$, and $B\mathbb{Z}/2 = \mathbf{RP}^\infty$.

5.2.2 Isomorphism of extensions and abstract isomorphism

Our initial interest in classification of extensions came from the problem of classifying groups up to isomorphism. There is some subtlety in using Theorem 5.2.1.5 to deduce results about isomorphism of groups. To understand this, let us start with a simple example.

Example 5.2.2.1. Let us consider central extensions of $\mathbb{Z}/p$ by $\mathbb{Z}/p$; here $\omega : \mathbb{Z}/p \to Aut(\mathbb{Z}/p)$ is the trivial homomorphism, and we want to compute $H^2(\mathbb{Z}/p, \mathbb{Z}/p, 1)$. Note that $Fun(\mathbb{Z}/p, \mathbb{Z}/p)$ is an abelian group of order p^p (we have p-choices for the value of a function f at each point of the source). Likewise, $Fun(\mathbb{Z}/p \times \mathbb{Z}/p, \mathbb{Z}/p)$ is again an abelian p-group of order p^{2p}. Therefore, $H^2(\mathbb{Z}/p, \mathbb{Z}/p, 1)$ is necessarily also a p-group. It follows that if $H^2(\mathbb{Z}/p, \mathbb{Z}/p, 1)$ is non-trivial, it must have order at least p. Since we know that there are at least 2 non-isomorphic extensions of $\mathbb{Z}/p$ by $\mathbb{Z}/p$ (i.e., $\mathbb{Z}/p^2$ and $\mathbb{Z}/p \times \mathbb{Z}/p$), it follows that $H^2(\mathbb{Z}/p, \mathbb{Z}/p, 1)$ must have order at least p. Thus, we conclude that different extensions may give rise to groups that are abstractly isomorphic.

Definition 5.2.2.2. If Q is a group, and A is a group, define a category $ext(Q, A)$ as follows:

- objects are short exact sequences of the form $1 \to A \to G \to Q \to 1$,
- morphisms are homomorphisms $\varphi : G \to G'$ that induce the identity on A and Q.

Lemma 5.2.2.3. *Any morphism in $ext(Q, A)$ is an isomorphism.*

Proof. We want to show that φ is a bijection. Let us first show that φ is surjective. If $x \in G$ goes to 1 under φ, then x goes to 1 in Q by commutativity. In other words, x lies in A. However, commutativity again implies x must be equal to 1 in A since the restriction of φ to A is the identity.

Next, let us show that it is surjective. If $x \in G'$, then we may consider the image $\bar{x}$ of x in Q. In that case, $\bar{x}$ may be lifted to an element $\tilde{\bar{x}}$ in G. By construction, $\varphi(\tilde{\bar{x}})$ and x both map to $\bar{x}$ in Q. Thus, $\varphi(\tilde{\bar{x}})x^{-1}$ lies in A, i.e., $\varphi(\tilde{\bar{x}})a = x$. However, since φ is a homomorphism and the identity on A, we conclude that

$$\varphi(\tilde{\bar{x}})a = \varphi(\tilde{\bar{x}})\varphi(a) = \varphi(\tilde{\bar{x}}a),$$

and $\tilde{\bar{x}}a$ provides the required lift. □

Note that any morphism in this category is an isomorphism. We will say that two extensions are *equivalent* if they are isomorphic as objects in this category. By construction, Theorem 5.2.1.5 provides a description of the set of equivalence classes of extensions of Q by A, essentially by construction.

On the other hand, suppose G is a group and $\varphi : G \to G$ is a group homomorphism. If $N \subset G$ is a normal subgroup, then N is stable by conjugation (i.e., under inner automorphisms) but need not be stable by arbitrary automorphisms. For example, in $\mathbb{Z}/2 \times \mathbb{Z}/2$, we may consider the automorphism switching the two factors. The subgroup $N = \langle(1, 0)\rangle$ is sent to $N' = \langle(0, 1)\rangle$ by this automorphism. In other words, the automorphism φ does not even restrict to an automorphism of N. Moreover, even if the given automorphism restricts to an automorphism of N, there is no need for the induced map to be the identity on N. In other words, there is a further equivalence relation on extensions induced by "abstract isomorphism" of groups.

There is another notion of "equivalence" of extensions we may consider based on the above observation. We will say that two extensions of Q by A are *weakly equivalent* if there is an isomorphism $\varphi : G \to G'$ that restricts to an automorphism of A (and then necessarily induces an automorphism $Q \to Q$). This notion of equivalence stems from a natural group action of $Aut(A) \times Aut(Q)$ on the set of all extensions $ext(Q, A)$.

5.2.3 An example

Example 5.2.3.1 (Extra-special p-groups). Consider the group $Q = \mathbb{Z}/p \times \mathbb{Z}/p$ and $A = \mathbb{Z}/p$. We would like to construct an extension of Q by A. Take the action of Q on A to be trivial. And define a function $Q \times Q \to A$ by the formula: $f((a,b),(a',b')) = ab'$ (notice: here we are using the multiplication in $\mathbb{Z}/p$, rather than addition). We have to check that this f satisfies the cocycle condition. Let $q = (a,b)$, $q' = (a',b')$ and $q'' = (a'',b'')$. In that case the cocyle condition should be written additively in A as well:

$$f(q,q')+f(qq',q'') = f((a,b),(a',b'))+f((a+a',b+b'),(a'',b'')) = ab'+(a+a')b'' = ab'+ab''+a'b''.$$

Now, since the conjugation action is trivial, the right hand side of the cocycle condition becomes:

$$f(q',q'')f(q,q'q'') = f((a',b'),(a'',b''))+f((a,b),(a'+a'',b'+b'')) = a'b''+a(b'+b'') = a'b''+ab'+ab'',$$

and the two results agree. The result is a group of order p^3 and it can be identified explicitly as $U(\mathbb{F}_p) \subset GL_3(\mathbb{F}_p)$. Indeed, we identify the center $\mathbb{Z}(U(\mathbb{F}_p))$ with matrices of the form

$$\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

the quotient of $U(\mathbb{F}_p)$ by its center is given a group of order p^2 which can be identified with $\mathbb{Z}/p \times \mathbb{Z}/p$. The section map $\mathbb{Z}/p \to \mathbb{Z}/p \to U(\mathbb{F}_p)$ can be taken to be

$$(a,c) \mapsto \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

and you can compute that the factor set is given precisely by the formula above. The group $U(\mathbb{F}_p)$ is called a Heisenberg group, and it is an example of what is called an *extra-special p-group*. One can show that this group of order p^3 is isomorphic to the semi-direct product $(\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes \mathbb{Z}/p$ described in Lemma 5.1.1.2.

Similarly, the functions $f(q,q') = \alpha ab'$ also define extensions for $0 \leq \alpha \leq p-1$. The extension with $\alpha = 0$ is the trivial extension. Moreover, the subgroup of $H^2(\mathbb{Z}/p \times \mathbb{Z}/p, \mathbb{Z}/p)$ generated by $[f]$ consists precisely of extensions of this form. Indeed, f is a representative of $[f]$ in $Z^2(\mathbb{Z}/p \times \mathbb{Z}/p, \mathbb{Z}/p)$ and multiples of f in $Z^2(\mathbb{Z}/p \times \mathbb{Z}/p, \mathbb{Z}/p)$ precisely correspond to multiples of $[f]$ in $H^2(\mathbb{Z}/p \times \mathbb{Z}/p, \mathbb{Z}/p)$.

Remark 5.2.3.2. More generally, an extra special p-group is a group G of prime power order with center isomorphic to $\mathbb{Z}/p$ and with $G/Z(G) \cong \mathbb{Z}/p^{\times n}$. As above, to classify such extensions, we begin by observing that an action of $\mathbb{Z}/p^{\times n}$ on $\mathbb{Z}/p$ is a homomorphism $\mathbb{Z}/p^{\times n} \to \mathbb{Z}/(p-1)$, and all such homomorphisms are trivial. Thus, we want to build central extensions of $Z/p^{\times n}$ by $\mathbb{Z}/p$ and such groups are classified by elements of $H^2(\mathbb{Z}/p^{\times n}, \mathbb{Z}/p)$.

5.3 Lecture 17: Solvability and nilpotence

5.3.1 Solvable groups

If we begin with the class of abelian groups, then we may build more complicated groups by studying iterated extensions. Based on the two types of extensions we analyzed previously, we distinguish two classes of groups we want to study: we may study iterated *central* extensions of abelian groups, or simply iterated extensions of abelian groups. Loosely, a group G is *nilpotent* if it is an iterated central extension of abelian groups and *solvable* if it is an iterated extension of abelian groups. There are a number of ways to make these notions precise, but introduce a bit of terminology to organize the various versions. We begin by making an "inductive" definition, which amounts to a precise version of what we just said.

Definition 5.3.1.1. A group G is *solvable* (resp. nilpotent) if it lies in the *smallest* class of groups Solv (resp. Nilp) satisfying the following two properties

i) every abelian group is a member of Solv (resp. Nilp);

ii) if G lies in Solv (resp. Nilp) and A is any abelian group, then any (central) extension of G by A lies in Solv (resp. Nilp).

One positive property of this definition is that it is a quick formulation of the intuitive notion. However, it does not give any idea how to tell if a given group is solvable. Let us try to implement the algorithm implicit in the definition. If A and A' are abelian groups, then any extension of the form:

$$1 \longrightarrow A' \longrightarrow H \longrightarrow A \longrightarrow 1$$

is also a solvable group. Note that the trivial extension lies among such extensions so it is possible that G remains abelian (and, of course, H might be abelian even if the extension is non-trivial). This observation suggests a measure of complexity: loosely, how far is H from being abelian?

Note also that A' provides a normal subgroup of H such that the quotient H/A' is abelian. Now, suppose we have a further extension G of H by A'', i.e., we have an exact sequence of the form

$$1 \longrightarrow A'' \longrightarrow G \longrightarrow H \longrightarrow 1.$$

The composite map $G \to H \to A$ is a surjective group homomorphism. The kernel of this surjective homomorphism is a normal subgroup G_1 of G that contains A'' and has abelian quotient. Since G_1 contains A'' by construction, and $G_1 \cap A''$ is normal in G_1, it follows that A'' is itself a normal subgroup of G_1. Because G_1 is defined to be the kernel of the composite $G \to H \to A$, it follows that there is a short exact sequence of the form

$$\begin{tikzcd}
1 \arrow[r] & \ker(G \to H) \arrow[r] \arrow[d, "="] & \ker(G \to A) \arrow[r] \arrow[d, "="] & \ker(H \to A) \arrow[r] \arrow[d, "="] & 1 \\
& A'' \arrow[r] & G_1 \arrow[r] & A'. &
\end{tikzcd}$$

If we define $G_2 = A''$ and $G_3 = 1$, then we have obtained an increasing sequence of subgroups $1 = G_3 \subset G_2 \subset G_1 \subset G_0 = G$ such that each G_i is normal in G_{i-1} and the quotients G_{i-1}/G_i are all abelian groups. Note that this procedure may also be reversed, so the original pair of short exact sequences may be extracted from the sequence of subgroups. We can turn this observation into an equivalent definition of solvability, but let us first introduce some terminology.

Definition 5.3.1.2. If G is a group, then a *subnormal series* for G is a sequence of subgroups

$$1 = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G$$

such that G_i is normal in G_{i-1} for all i. If each of the inclusions is a proper inclusion, then we will refer to n as the length of the subnormal series, and we refer to the quotient groups G_{i-1}/G_i as the *successive subquotients*. A *normal series* for G is a subnormal series in which each G_i is normal in G itself.

Remark 5.3.1.3. Remember that normality is not transitive: if G_1 is normal in G_2 and G_2 is normal in G_3, then G_1 need not be normal in G_3. For example take $G = S_4$ and $H \subset G$ the subgroup generated by products of disjoint transpositions (which is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$). The cyclic subgroup generated by any product of disjoint transpositions gives a subgroup $\mathbb{Z}/2 \subset H$, which is normal since H is abelian. One may check that H is normal in G as well. However, you may check that the cyclic subgroup generated by a product of disjoint transpositions is not normal in S_4. It is because normality is not transitive that we distinguish between subnormal and normal series.

Proposition 5.3.1.4. *A group G is* solvable *if and only if there exists a subnormal series with successive subquotients G_{i+1}/G_i abelian.*

Proof. If G is solvable in the sense defined above, then it is a straightforward induction generalizing our discussion above to show that it admits a subnormal series with abelian subquotients. The converse is similar and obtained by induction on the length of a subnormal series. The result is evidently true for group with a subnormal series of length 1, and one proves the result inductively by reversing the procedure described above. □

Remark 5.3.1.5. A solvable group may have normal series of different lengths witnessing solvability. For example, suppose $A = A' \times A''$ is a product of abelian groups. Then $1 \subset A$ is a subnormal series of length 1, while $1 \subset A' \subset A$ is a subnormal series of length 2.

Definition 5.3.1.6. If G is a solvable group, then its *solvable length* is the minimal length of a normal series for G.

Example 5.3.1.7. Abelian groups have solvable length 1, and thus solvable length can be viewed as a measure of complexity of a solvable group (roughly, how far is it from being abelian).

Example 5.3.1.8. Non-abelian simple groups are *not* solvable. Indeed, such a group contains no non-trivial normal subgroups and therefore cannot support subnormal series of length > 1. As a consequence, any group that contains a normal subgroup that is a non-abelian simple group is *not* solvable. Thus, for example, the symmetric group S_5 is not solvable. Later, we will see that S_n for $n \geq 6$ is also not solvable. In contrast, S_n for $n \neq 4$ *is* solvable.

Remark 5.3.1.9. Note that all iterated extensions of cyclic groups are solvable. If G is a finite group, then we will establish a converse to this statement.

5.3.2 Permanence properties of solvable groups

Lemma 5.3.2.1. *If $\varphi : G \to G'$ is a group homomorphism, and $N \subset G'$ is a normal subgroup, then $H = \varphi^{-1}(N)$ is a normal subgroup of G.*

Lemma 5.3.2.2. *The following statements hold.*

1. *Any subgroup of a solvable group is solvable.*
2. *Any quotient of a solvable group is solvable.*

3. Any extension of solvable groups is solvable.

Proof. Fix $G_i \subset G$ as in the definition of a solvable group. The intersections $G_i \cap H$ define normal subgroups $H_i \subset H$ which necessarily exhaust H. In that case, the quotients H_{i+1}/H_i are subgroups of G_{i+1}/G_i and are thus abelian groups themselves.

A similar argument works for quotient groups: if $\pi : G \to Q$ is a surjective group homomorphism, then the image of G_i in Q is a normal subgroup $Q_i \subset Q$ (check this!). In that case, Q_{i+1}/Q_i is a quotient of an abelian group and thus also abelian.

Suppose we are given an extension of the form

$$1 \longrightarrow S \longrightarrow G \longrightarrow S' \longrightarrow 1$$

where both S and S' are solvable. If S is itself abelian, then G is solvable by definition. To generalize this, we proceed by induction on the length of the filtration $1 = S_0 \subset S_1 \subset \cdots \subset S_n = S$. Assume we know the result for solvable groups where length of the defining filtration has no more than $n-1$ steps. Then, by assumption, S has a normal subgroup S_{n-1} such that S_n/S_{n-1} is abelian. □

Example 5.3.2.3 (A non-central extension). Suppose V is a finite dimensional F-vector space. An element of $GL(V)$ acts on V by automorphisms. Any element of V acts on V by translations. Of course, V is an abelian group under addition. Consider the semi-direct product $Aff(V) := V \rtimes GL(V)$ where the action of $GL(V)$ on V is the one just specified. Here, V is a non-central abelian normal subgroup of $Aff(V)$. If V is 1-dimensional, then $GL(V)$ is abelian, and thus we obtain an example of a solvable group.

Proposition 5.3.2.4. *Any finite solvable group admits a subnormal series where the successive subquotients are cyclic.*

Proof. Suppose G is a finite solvable group and fix a subnormal series for G. In that case, G_i/G_{i-1} is a finite abelian group for each i. As a finite abelian group, G_i/G_{i-1} is a direct product of cyclic groups. Fix a total ordering of the (finite) index set A_i of this product. And define $G_{i,\alpha} \subset G_i$ to be the kernel of the projection

$$G_{i,\alpha} \to \prod_{\beta \geq \alpha} C_{i,\beta}.$$

Note that $G_{i,\alpha} \subset G_{i,\alpha'}$ if $\alpha \leq \alpha'$, and the successive subquotients are identified with $C_{i,\alpha}$. Thus, we have refined the given subnormal series for G into one with successive subquotients that are cyclic. □

Lemma 5.3.2.5. *Any finite p-group is solvable.*

Proof. Groups of order p^2 are abelian. Any group of order p^n has a non-trivial center and therefore may be written as an extension of a group of order p^{n-r} for $r > 0$ by a group of order p^r. The result follows immediately by induction on n and the fact that extensions of solvable groups are solvable. □

Example 5.3.2.6. More generally, a result of Burnside shows that groups of order $p^a q^b$ are solvable. The latter result may be proven using ideas of group theory, but many proofs (including the original) use representation theory of finite gorups.

Example 5.3.2.7 (Feit-Thompson). A very difficult and famous result of W. Feit and J. Thompson guarantees that any group of odd order is solvable!

5.4 Lecture 18: Nilpotence and solvability continued

5.4.1 Nilpotent groups

A group G is called nilpotent if it can be built by iterated *central* extensions. For example, begin with a central extension

$$1 \to A' \to G' \to A \to 1,$$

i.e., $A' \subset Z(G)$. And suppose we are also given

$$1 \to A'' \to G \to G' \to 1,$$

again with $A'' \subset Z(G)$. Repeating our initial analysis of iterated extensions by abelian groups, begin by observing that the preimage of A' under the homomorphism $G \to G'$ is a subgroup $G_1 \subset G$ with $G/G_1 \cong A$. Set $G_0 = G$, $G_2 = A''$ and $G_3 = 1$. As before, $A'' \subset G_1$, but $A'' \subset Z(G)$, and $G_1 \subset G$, we conclude $A'' \subset Z(G_1)$ as well. In terms of the new notation, we write this as: $G_2/G_3 \subset Z(G_0/G_3)$. Similarly, $G_1/A'' \cong A' \subset Z(G')$, and we can rewrite this as $G_1/G_2 \subset Z(G_0/G_2)$. Note here that A'' is a normal subgroup of G (since it lies in the center) and likewise G_1 is a normal subgroup of G by construction. Iterating this procedure with longer strings of central extensions yields the following definition.

Definition 5.4.1.1. If G is a group, then say G is *nilpotent* if there exists a normal series $1 = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$ with $G_{i+1}/G_i \subset Z(G/G_i)$. We say that G has nilpotence class c if the minimal length of a normal series for G is c.

Remark 5.4.1.2. A series as in Definition 5.4.1.1 is sometimes called a *central series* for G. In particular, in order that the quotient G/G_i makes sense, we have implicitly assumed that G_i is a normal subgroup of G. We will revisit this below.

Proposition 5.4.1.3. *The following statements hold.*

1. *Any subgroup of a nilpotent group is nilpotent.*
2. *Any quotient of a nilpotent group is nilpotent.*
3. *Any finite product of nilpotent groups is nilpotent.*

Proof. Given a central series for G, then for the first point, one checks that $H_i := H \cap G_i$ is a central series for H. For the second point, one checks that if $\pi : G \to H$ is a surjective group homomorphism, then $\pi(G_i)$ is a central series for H_i. We leave the third point as an exercise. □

Example 5.4.1.4. Any extension of abelian groups that is not central yields an example of a solvable group that is not nilpotent. For example, the symmetric group on 3 elements is an extension of $\mathbb{Z}/2$ by $\mathbb{Z}/3$, but the center of S_3 is trivial. Similarly, S_4 is a solvable group that is not nilpotent. Thus, extensions of nilpotent groups need not be nilpotent, in contrast to the situation for solvable groups!

Lemma 5.4.1.5. *Any central extension of a nilpotent group is again nilpotent.*

Proof. Suppose we are given a central extension of the form $1 \to A \to G \to N \to 1$ where N is nilpotent. By assumption, there exists an increasing sequence of subgroups $1 = N_0 \subset \cdots \subset N_n = N$ such that each N_i is normal in N and $N_{i+1}/N_i \subset Z(N/N_i)$. If $\pi : G \to N$ is the quotient homomorphism, define $G_1 = A$ and $G_{i+1} = \pi^{-1}(N_i)$. One may check that this produces the required central series. □

Remark 5.4.1.6. Lemma 5.4.1.5 essentially completes the proof that the two definitions of nilpotent we have given are equivalent. In particular, it shows that groups that are nilpotent in the sense described last time are nilpotent in terms of the definition we gave this time. Conversely, reverse engineering the procedure described at the beginning of the lecture, we can observe that any group that possesses a finite central series is an iterated central extension; we leave the details as an exercise.

Proposition 5.4.1.7. *Any p-group is nilpotent. Any finite direct product of p-groups is also nilpotent.*

Proof. The result is clearly true for groups of order exactly p since all such groups are themselves abelian. Assume inductively the result is true for groups of order p^{n-i} for $i \geq 1$. Assume G is a group of order p^n. Since $Z(G)$ is non-trivial, it follows that $G/Z(G)$ is again a p-group of lower order. Since central extensions of nilpotent groups are again nilpotent, the result follows. An analogous argument works for direct products. □

We want to prove the following result, which includes a converse to the above statement.

Theorem 5.4.1.8. *A finite group G is nilpotent if and only if it is isomorphic to the direct product of its Sylow p-subgroups (in particular, it is a finite direct product of p-groups).*

Nilpotent finite groups

We would like to analyze nilpotent finite groups in general. To this end, we want to study proper subgroups of nilpotent groups. The basic idea is to analyze the interaction of a proper subgroup with a central series.

Proposition 5.4.1.9. *If G is a finite nilpotent group and H is a proper subgroup of G, then H is a proper subgroup of $N_G(H)$.*

Proof. Suppose we take a central series for G. Since $G_n = 1$ and $G_0 = G$, there exists an integer j such that G_j is not a subgroup of H while G_{j+1} is a subgroup of H. Since G_i is normal (for any i) in G by assumption, we see that set HG_i is a subgroup of G. H is a proper subgroup of HG_j by assumption, and $HG_j \subset N_G(H)$

Since G_{j+1} is normal in G it is automatically normal in H as well and thus H/G_{j+1} is a group. Moreover, H/G_{j+1} is a subgroup of $G_j/G_{j+1} \subset Z(G_0/G_{j+1})$, which is abelian, thus H/G_{j+1} is automatically a normal subgroup of G_j/G_{j+1}. We may then conclude that H is normal in HG_j. , we conclude that $H \neq N_G(H)$ as claimed. □

To prove Theorem 5.4.1.8, we will begin by proving that if G is a finite nilpotent group, then all p-Sylow subgroups are normal. We will return to this next time.

5.4.2 Series

If G is a group that is a group that is solvable, the we can produce a filtration of G by subgroups to witness solubility. First, we observe that we can characterize abelian groups as those whose commutator subgroups are trivial, i.e., $[G, G] = e$. If G is a group, then $[G, G]$ is a naturally defined normal subgroup of G. If G is a group and N is a normal subgroup, observe that G/N is abelian if and only if $N \subset [G, G]$.

Derived series

Definition 5.4.2.1. If G is a group, the *derived series* of G is the sequence of subgroups $G^{(i)}$ defined inductively by the formula $G^{(0)} = G$, and $G^{(i)} := [G^{(i-1)}, G^{(i-1)}]$.

Remark 5.4.2.2. Note that the derived series is a *decreasing* sequence of subgroups, i.e.,

$$G = G^{(0)} \supset G^{(1)} \supset \cdots .$$

It is a standard convention to write decreasing sequences with superscripts and increasing filtrations with subscripts.

Lemma 5.4.2.3. *A group G is solvable if and only if the derived series terminates after finitely many steps, i.e., there exists some finite integer n such that $G^{(n)} = e$.*

Proof. Since the quotient $G^{(i)}/G^{(i+1)}$ is always abelian, one direction follows from the definition of solvability. In the other direction, assume that G is solvable, i.e., we have a filtration $G_i \subset G$ such that G_i is normal in G_{i+1} and G_{i+1}/G_i is abelian. In this case, it follows from the universal property of the commutator subgroup that $[G_i, G_i] \subset G_i$. Now, we simply reindex the filtration. □

Upper central series

As regards nilpotence, there are several central series we may write down to witness nilpotence. Observe that the primordial central extension is

$$1 \longrightarrow Z(G) \longrightarrow G \longrightarrow G/Z(G) \longrightarrow 1.$$

We may define *higher centers* of a group G inductively as follows: set $Z_0(G) = 1$, and if $\pi_i : G \to G/Z_i(G)$, then set

$$Z_{i+1}(G) := \pi^{-1}(Z(G/Z_i(G))).$$

Thus, $Z_1(G) = Z(G)$ and by construction by construction $Z_i(G) \subset Z_{i+1}(G)$. Unwinding the definitions, we observe that we obtain a a central series for G.

Definition 5.4.2.4. The upper central series for a group G is the series of groups defined by

$$1 = Z_0(G) \subset Z_1(G) \subset \cdots \subset Z_i(G) \subset \cdots .$$

Lemma 5.4.2.5. *A group G is nilpotent if and only if the upper central series terminates, i.e., there exists an integer n such that $Z_n(G) = G$.*

Proof. If the upper central series terminates, then G has a central series and is thus nilpotent. Conversely, suppose G has a central series. In that case, by induction one shows that $G_{i+1}/G_i \subset Z_i(G)$ and from this one may deduce that $Z_i(G)$ terminates. □

Lower central series

There is another reformulation of the definition of nilpotence.

Definition 5.4.2.6. If H and H' are subgroups of a group G, then $[H, H']$ is the subgroup of G generated by all commutators of the form $[x, y]$ with $x \in X$, $y \in H'$.

Definition 5.4.2.7. If G is a group, the *lower central series* is the decreasing sequence of subgroups of G defined inductively by $G^0 = G$, and $G^i := [G, G^{i-1}]$.

Lemma 5.4.2.8. *A group G is nilpotent if and only if the lower central series terminates.*

Proof. Exercise. □

5.5 Lecture 19: the Jordan–Hölder theorem

5.5.1 Finite nilpotent groups continued

Last time, we started trying to prove that finite nilpotent groups were isomorphic to the direct product of their Sylow p-subgroups. If this statement is true, then each Sylow p-subgroup of a finite nilpotent group is normal. Thus, the normalizer of a Sylow p-subgroup is equal to the whole group. We began by analyzing the relation between a subgroup of a finite nilpotent group and its normalizer and we established the following fact.

Proposition 5.5.1.1. *Assume G is a finite nilpotent group. If H is a proper subgroup of G, then $H \neq N_G(H)$.*

If G is a finite nilpotent group, and H is a subgroup, then we may build a chain of subgroups of G by iteratively taking normalizers. The above proposition applied iteratively shows that eventually the iterated normalizer must be all of G. Therefore, we want to analyze iterated normalizers of Sylow subgroups. We establish the following result first.

Proposition 5.5.1.2 (Frattini Argument)**.** *Let G be a finite group and $K \subset G$ a normal subgroup. If P is a Sylow p-subgroup of K, then $G = KN_G(P)$.*

Proof. Let $g \in G$. Since K is normal in G and $P \subset K$, it follows that ${}^gP$ is again a Sylow p-subgroup of K. Since any two Sylow p-subgroups of K are conjugate, it follows that ${}^gP = {}^kP$ for some $k \in K$. In that case, ${}^{k^{-1}g}P = P$, i.e., $k^{-1}g \in N_G(P)$. Since g was arbitrary, and since $g = k(k^{-1}g) \in KN_G(P)$ the conclusion follows. □

Proposition 5.5.1.3. *If G is a finite group, and P is a Sylow p-subgroup of G, then $N_G(N_G(P)) = N_G(P)$.*

Proof. Since $N_G(P)$ is a normal subgroup of $N_G(N_G(P))$ by defn, and since $P \in Syl_p(N_G(P))$, the Frattini argument shows that $N_G(N_G(P)) = N_G(P)N_{N_G(N_G(P))}(P)$. But $N_{N_G(N_G(P))}(P) \subset N_G(P)$ and we conclude. □

Theorem 5.5.1.4. *If G is a finite nilpotent group, then*

1. *each Sylow subgroup is normal, and*
2. *G is isomorphic to the product of its Sylow p-subgroups.*

Proof. If P is a Sylow p-subgroup of G, then P is a Sylow p-subgroup of $N_G(P) \subset G$. Moreover, P is normal in $N_G(P)$ by definition, so it suffices to prove that $N_G(P) = G$. We know $N_G(N_G(P)) = N_G(P)$ by appeal to Proposition 5.5.1.3. On the other hand, if $N_G(P)$ was a proper subgroup of G, then since G is assumed nilpotent, $N_G(P) \neq N_G(N_G(P)$ by appeal to Proposition 5.5.1.1, which contradicts the previous assertion. Thus, $N_G(P) = G$.

To conclude that G is a product of its p-Sylow subgroups, we proceed by induction. Suppose $P_1, \ldots, P_n$ are the different Sylow subgroups (corresponding to different primes $p_1, \ldots, p_n$). We will inductively show that the product map $P_1 \times \cdots P_n \to G$ is an injective homomorphism. This is evidently true if there is a single factor. Assume inductively that the product map is a homomorphism for $i < n$ factors. In that case, the intersection of P_{i+1} with $P_1 \cdots P_i$ consists of the identity element 1 since orders are coprime. Moreover, since P_i is normal in G and $P_1 \cdots P_{i-1}$ is normal in G (as an internal direct product of normal subgroups). Then, $(g,p) \cdot (g',p') = gpg'p' = gg'(g')^{-1}pg'p^{-1}pp'$. However, $(g')^{-1}pg'p^{-1} = [g'^{-1},p]$ lies in $[N, P_i]$ where $N = P_1 \cdots P_{i-1}$. Note NP_i is normal in G since both N and P_i are normal in G, and the orders of N and P_i are coprime. Thus, $[N, P_i] \subset N \cap P_i = e$. Thus, the product map $N \times P_i \to NP_i$

is an isomorphism. Since G and $P_1 \times \cdots \times P_n$ have the same orders, we conclude that the product map is an isomorphism. □

5.5.2 Composition series and the Jordan-Hölder theorem

In the above, we isolated a class of groups that were built up by iterated extensions. The definition of solvability or nilpotence simply required the existence of a filtration that witnessed the corresponding property, but via the derived series or central series, we saw there was a special filtration that had the same property. However, unless the abelian groups by which we were extending at each stage were simple, this was not a successive extension by simple groups.

Definition 5.5.2.1. Given a group G, and a subnormal series $\{G_i\}_{i=0,\ldots,n}$ for G is called *a Jordan-Hölder filtration of G of length* n if the successive subquotients G_i/G_{i+1} are non-trivial simple groups for each $0 \leq i \leq n-1$.

Remark 5.5.2.2. For the purposes of induction arguments later, it will be convenient to index our Jordan–Holder filtrations by a totally ordered finite set I of cardinality $n+1$ instead of $\{0,\ldots,n\}$. Typically, we will take $I = \{0,\ldots,n\}$, but when we pass to subgroups and quotients, we will sometimes want to pick out subsets of I (which are again totally ordered). The trivial group has the Jordan-Hölder filtration $1 = G_0$ of length 0. A simple group has a Jordan-Hölder-filtration of length 1. The definition has been made in this fashion to eliminate silly possibilities like the following:

$$1 \subset 1 \subset G \subset G.$$

Indeed, in the definition we have given, the inclusion map $G_i \hookrightarrow G_{i+1}$ is never an isomorphism.

Proposition 5.5.2.3. *If G is a finite group, then G has a Jordan-Hölder filtration.*

Proof. We establish this by induction on the order of G. The result is clearly true for groups of order 1. If G is simple, then G has a Jordan-Holder filtration of length 1. If G is not simple, it has a non-trivial proper normal subgroup. Since G is finite, it has a non-trivial proper normal subgroup N of maximal order. I claim that G/N is then simple. Indeed, a normal subgroup of G/N, via the correspondence theorem, corresponds with a normal subgroup of G that contains N, which by maximality of N is either equal to G itself or N. The subgroup N has order strictly smaller than G since it is proper, so by the induction hypothesis guarantees that we have a Jordan-Hölder filtration for N, say $(N_0,\ldots,N_{n-1},N)$. The sequence $(N_0,\ldots,N_{n-1},N,G)$ is then a Jordan-Hölder filtration of G. □

Remark 5.5.2.4. If G is infinite, then it need not have a Jordan-Hölder filtration. Indeed, we know that simple abelian groups are finite and that any finite abelian group is a direct product of cyclic groups of prime power order. In particular, using these facts one can show that $\mathbb{Z}$ cannot have a Jordan-Hölder filtration.

Theorem 5.5.2.5 (Jordan-Hölder)**.** *If G is a finite group, and* $\{G_i\}_{i=0,\ldots,n}$ *is a Jordan-Hölder filtration of G, then the set of successive quotients* $gr_iG := \{G_{i+1}/G_i\}$ *is independent of the filtration (i.e., two filtrations have the same set of quotients).*

Proof. It suffices to show that if S is a fixed, finite simple group, then the number of times S appears as a quotient in a Jordan-Hölder filtration for G, call this number $n(G,G_i,S)$, is independent of the filtration. The idea of the proof is again to proceed by induction. The result is true for the trivial group or for a simple group since in that case the Jordan-Hölder filtration itself is unique. To proceed, we need to understand a bit how Jordan-Hölder filtrations interact with passage to normal subgroups and the corresponding quotients.

If H is a subgroup of G, and $\{G_i\}_{i=0,\ldots,n}$ is a filtration of G, then we can consider the induced filtration on H by setting $H_i := G_i \cap H$. Consider the inclusion $H_i \subset H_{i+1} = G \cap H_{i+1}$. If $h \in H_{i+1}$, then $hH_ih^{-1} = h(G_i \cap H)h^{-1}$; for any $x \in G_i \cap H$, $hxh^{-1} \in G_i$ since G_i is normal in G_i and in H since $x \in H$. Therefore, $hH_ih^{-1} \subset G_i \cap H$, i.e., each H_i is normal in H_{i+1}. Note also that we have maps $H_{i+1}/H_i \to G_{i+1}/G_i$ induced by the inclusions, though there is no reason for H_{i+1}/H_i to be simple because we cannot guarantee that H_{i+1}/H_i is a *normal* subgroup of G_{i+1}/G_i without further hypotheses. In other words, the induced filtration need not be a Jordan-Hölder filtration on H.

Assume further that N is normal in G. In that case, it follows from the isomorphism theorems that N_i is normal in G_i and furthermore that N_{i+1}/N_i is a normal subgroup of G_{i+1}/G_i. As a consequence, there is a filtration on G/N defined by $(G/N)_i := G_i/(G_i \cap N)$. The exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

induces the exact sequences

$$1 \longrightarrow N_i/N_{i-1} \longrightarrow G_i/G_{i-1} \longrightarrow (G/N)_i/(G/N)_{i-1} \longrightarrow 1$$

for the successive quotients. Now, notice that if we start with a Jordan-Hölder filtration for G, then the induced filtration on N has gr_iN either trivial or isomorphic to $gr_i(G)$. Therefore, by reindexing if necessary, we can obtain a Jordan-Hölder filtration for N and also for G/N given one for G.

Given these observations, we can now establish the theorem. Start with a Jordan-Hölder filtration for G and suppose N is a normal subgroup. Either $gr_iN = 1$ and $gr_iG/N = G$ or $gr_iN = gr_i(G)$ and $gr_iG/N = 1$. If $I = \{0, \ldots, n\}$, then we obtain a partition of I into two sets: $I_1 := \{i | gr_i(N) = 1\}$, and $I_2 := \{i | gr_i(N) = gr_i(G)\}$.

Now, we proceed by induction on the order of G. Assume inductively that the number of occurrences of a simple group S in Jordan-Hölder-filtrations of groups of smaller order than G is independent of the filtration. We can assume that G is non-trivial and not simple. In that case, there exists a proper normal subgroup N of G. Observe that $|G/N| < |G|$ as well. The induction hypothesis applies to N and G/N and we conclude that $n(N, \{N_i\}_{i\in I_2}, S)$ and $n(G/N, \{(G/N)_i\}_{i\in I_1}, S)$ are independent of the chosen Jordan-Hölder filtrations. However,

$$n(G, \{G_i\}_{i\in I}) = n(N, \{N_i\}_{i\in I_2}, S) + n(G/N, \{(G/N)_i\}_{i\in I_1}, S),$$

which did not depend on the precise choice of the filtration. □

Example 5.5.2.6. A Jordan-Hölder filtration for S_3 is given by $1 \subset A_3 \subset S_3$. A Jordan-Holder filtration of S_4 can be given by

$$1 \subset \mathbb{Z}/2 \subset V \subset A_4 \subset S_4.$$

For $n \geq 5$, the sequence

$$1 \subset A_n \subset S_n$$

is a Jordan-Hölder filtration of S_n.

Chapter 6

More on simple groups

6.1 Lecture 20: Group actions and simplicity

Having analyzed the problem of building finite groups as extensions of finite simple groups, we now turn to the problem of producing more examples of simple groups. When we studied the symmetric group, we carefully analyzed its action on the set $\{1,\ldots,n\}$. Note that, given any element $x \in \{1,\ldots,n\}$, the stabilizer of this element is the symmetric group S_{n-1}. On the other hand, the orbit of this element is the whole set $\{1,\ldots,n\}$, i.e., any element $x \in \{1,\ldots,n\}$ can be moved to any other element by an element of S_n. Thus, the action of S_n on $\{1,\ldots,n\}$ transitive. We also showed that A_5 was simple by an analysis of conjugacy classes. After developing a bit more theory (motivated from the study of actions of groups of matrices), we will prove simplicity of all the alternating groups.

6.1.1 Transitive actions on the projective line

Definition 6.1.1.1. Given an action of a group G on a set X, we will say the action is *transitive* if for every $x, x' \in X$, there is a $g \in g$ such that $g \cdot x = x'$.

Let F be a field. Consider the vector space $V := F^{\oplus 2}$ (thought of as column vectors with entries in F). Write $\mathbb{P}^1(F)$ for the set of 1-dimensional subspaces of V. The groups $GL_2(F)$ and $SL_2(F)$ both act on V by left multiplication. We claim that $GL_2(F)$ and $SL_2(F)$ both act on $\mathbb{P}^1(F)$. Indeed, if $L = \lambda(\alpha_1,\alpha_2)^t$ is a line, then note that the scaling action of λ may be viewed as induced by left multiplication by λId_2 and scalar multiples of the identity lie in the center of $GL_2(F)$ (you even proved on your HW that this is precisely the center). Therefore, if $X \in GL_2(F)$ or $SL_2(F)$, the equalities

$$X \cdot \lambda(\alpha_1,\alpha_2)^t = X(\lambda Id_2)(\alpha_1,\alpha_2)^t = (\lambda Id_2)X \cdot (\alpha_1,\alpha_2)^t = \lambda(X \cdot (\alpha_1,\alpha_2)^t)$$

show that X sends lines to lines.

We now introduce a device to keep track of the fact that elements of $\mathbb{P}^1(F)$ may be thought of as scalar multiples of pairs $(\alpha_1,\alpha_2)^t$: homogeneous coordinates. Define an action of $F^\times$ on V by $\lambda \cdot (x_1,x_2)^t = (\lambda x_1, \lambda x_2)^t$. Define an equivalence relation on pairs $(x_1,x_2)^t$ by saying $(x_1,x_2)^t \sim (x_1,x_2')$ if there is a $\lambda \in F^\times$ such that $\lambda(x_1,x_2)^t = (x_1',x_2')^t$. Write $[x_1 : x_2]$ for the corresponding equivalence class; we will refer to such an equivalence class as the homogeneous coordinates of the line defined by $\lambda(x_1,x_2)^t$. Thus, points of $\mathbb{P}^1(F)$ may be thought of in terms of homogeneous coordinates.

Remark 6.1.1.2. There is another more elementary way to think about homogeneous coordinates: if $x_0 \neq 0$, then $\frac{x_1}{x_0}$ corresponds to the slope of the line through the vector $[x_0 : x_1]$, and lines are uniquely determined by their slope. If $x_0 = 0$, then up to rescaling $[0 : x_1] \sim [0 : 1]$. In other words, the set $\mathbb{P}^1(F)$ can be thought of as $F \sqcup \{\infty\}$ via interpreting lines in terms of their slop. We set $0 = [1 : 0]$, $\infty = [0 : 1]$, and $1 = [1 : 1]$; in terms of slopes, these correspond to $0 \in F \sqcup \{\infty\}$, $\infty \in F \sqcup \{\infty\}$ and $1 \in \sqcup\{\infty\}$.

It is a classical fact that the action of $GL_2(F)$ or $SL_2(F)$ on $\mathbb{P}^1(F)$ is transitive, but the action also classically has much stronger properties. We now want to analyze the action of $GL_2(F)$ on $\mathbb{P}^1(F)$ in more detail: what can we say about transitivity, stabilizers, etc.?

6.1.2 Multiple transitivity and stabilizers

Suppose we take two non-zero vectors in $F^{\oplus 2}$. If these vectors $v_1 = (x_{11},x_{21})^t$ and $v_2 = (x_{12},x_{22})^t$ do not lie on the same line, then they are linearly independent. In that case, the matrix M whose columns are given by the two vectors is invertible and M applied to the vector $(1,0)^t$ gives v_1, while M applied to $(0,1)^t = v_2$. The inverse matrix thus moves v_1 to $(1,0)^t$ and v_2 to $(0,1)^t$. Thus, we deduce that any pair of (non-zero) non-collinear vectors in $F^{\oplus 2}$ may be moved to any other pair of (non-zero) non-collinear vectors. Equivalently, any pair of distinct points in $\mathbb{P}^1(F)$ may be moved to any other pair of distinct points by the action of a single element of $GL_2(F)$. This is an example of a "multiply transitive" action, which we now define.

Definition 6.1.2.1. Suppose X is a set equipped with an action a of a group G. The action a is called n-*transitive* if X has at least n distinct elements, and for any sequences $(x_1, \ldots, x_n) \in X^n$ and $(x'_1, \ldots, x'_n) \in X^n$ in which the entries of $\mathbf{x}$ and $\mathbf{x}'$ are pairwise distinct, there exists an element $g \in G$ such that $(g \cdot x_1, \ldots, g \cdot x_n) = (x'_1, \ldots, x'_n)$.

Example 6.1.2.2. The discussion before the definition shows that $GL_2(F)$ acts 2-transitively on $\mathbb{P}^1(F)$.

Suppose the group G acts 2-transitively on the set X. Fix an element $x \in X$. The set $X \setminus x$ has an induced action of $G_x := Stab_G(x)$. Roughly speaking, to say that G acts 2-transitively is to say that G_x acts transitively on $X \setminus x$. For this to be interesting, we need to assume that X is sufficiently large.

Lemma 6.1.2.3. *If X is a set equipped with an action of G, and $|X| \geq 3$, then G acts 2-transitively if and only if, for any $x \in X$, the group $G_x := Stab_G(x)$ acts transitively on $X \setminus x$.*

Proof. The condition that $|X| \geq 3$ is in place to eliminate silly examples. If $|X| = 2$, then we can consider G acting trivially on X, and then $X \setminus x$ has a transitive action of G, but the action on X is not 2-transitive.

Suppose a subgroup $H \subset G$ acts on X. Define the twisted product $G \times^H X$ to be the quotient of $G \times X$ by the action of H defined by

$$h \cdot (g, x) = (gh, h^{-1} \cdot x).$$

The H-equivariant map $X \to pt$ induces a map $G \times^H X \to G \times^H pt = G/H$. Since G acts on X, there is also the product map $(g, x) \to g \cdot x$; this map factors through a map $G \times^H X \to X$. Together, there is an induced map $G \times^H X \to G/H \times X$, and this map is a G-equivariant bijection. The inclusion map $X \to G \times X$ gives rise to a map $X \to G \times^H X$, and this map determines a bijection between the G-orbits in $G/H \times X$ and the H-orbits in X.

If G acts transitively on $X \times X$, then consider the map $X \times X \to X$ induced by projection onto the first factor; this map is G-equivariant. Fix a point $(x_1, x_2) \in X \times X$. The G-orbit through (x_1, x_2) projects onto the G-orbit through x_1. The G-orbit through x_1 (in X) is in bijection with the set G/G_{x_1}. Thus, we can identify $X \times X$ with $G/G_{x_1} \times X$ and apply the observations of the previous paragraph. □

Remark 6.1.2.4. Analogous statements can be made for multiply transitive actions (though similar cardinality restrictions arise). For example, replacing $X \times X$ with $X^{\times n}$ and X with $X^{\times n-1}$ in the above argument, one deduces that for $|X| > n$, G acts n-transitively on X if and only if G_x acts $(n-1)$-transitively on $X \setminus x$.

The action of $GL_2(F)$ or $SL_2(F)$ on $\mathbb{P}^1(F)$ actually is even better than just transitive: it is a fact of classical geometry that the action of $GL_2(F)$ acts 3-transitively: this is the statement that any 3 points on the projective line can be moved to any other 3-points by a single element of $GL_2(F)$. The proof of this fact comes from an explicit computation: given 3 (distinct) lines L_1, L_2 and L_3, say with homogeneous coordinates $[x_1 : y_1]$, $[x_2 : y_2]$ and $[x_3 : y_3]$, it suffices to show that these three lines can be moved to a fixed set of 3 lines. The standard choices are $[1 : 0]$, $[1 : 1]$ and $[0 : 1]$, and these points are often denoted $0, 1$ and ∞.

Lemma 6.1.2.5. *There exists a matrix $M \in GL_2(F)$, unique up to multiplication by λId_2, that takes (L_1, L_2, L_3) to $(0, 1, \infty)$.*

Proof. We assume some familiarity with linear algebra. The (distinct) lines L_1 and L_2 are linearly independent subspaces of V. Therefore, the vector $(x_3, y_3)^t$ can be written as $\alpha(x_1, y_1)^t + \beta(x_2, y_2)^t$ for some unique $\alpha, \beta \in F$; since the line L_3 is distinct from L_1 and L_2, it follows that $\alpha, \beta \neq 0$. Now, consider the 2 × 2-matrix M whose columns are $\alpha(x_1, y_1)^t$ and $\beta(x_1, y_1)^t$. Note that, by construction, $M \cdot (1, 0)^t = \alpha(x_1, y_1)^t$, $M \cdot (0, 1)^t = (x_2, y_2)^t$, and $M \cdot (1, 1)^t = (x_3, y_3)^t$, which is what we wanted to prove. The matrix M is not unique, since we can multiply it by λId_2, but it is unique up to this choice. □

Remark 6.1.2.6. Note that if $F = \mathbb{F}_2$, then $\mathbb{P}^1(F)$ consists of just the 3 elements $0, 1$ and ∞, which are all distinct; $GL_2(F)$ still acts 3-transitively here.

Recall that

$$PGL_n(F) := GL_n(F)/Z(GL_n(F))$$
$$PSL_n(F) := SL_n(F)/Z(SL_n(F)).$$

On the homework, we saw that $Z(GL_2(F))$ consists of precisely the scalar multiples of the identity. On the other hand, one can similarly show that $Z(SL_2(F))$ consists of matrices of the form $diag(\alpha, \alpha)$ with $\alpha^2 = 1$, i.e., square roots of unity in F. Note that the center of either $GL_2(F)$ or $SL_2(F)$ acts trivially on $\mathbb{P}^1(F)$, essentially by construction. Therefore, there is an induced action of $PGL_2(F)$ (or $PSL_2(F)$). The lemma above shows that $PGL_2(F)$ acts 3-transitively on $\mathbb{P}^1(F)$.

Remark 6.1.2.7. Roughly speaking there are 4 parameters in $GL_2(F)$ the entries of the matrix, and 3 parameters in an element of $PGL_2(F)$.

6.1.3 Stabilizers of points

If we fix the point $[1 : 0]$ in $\mathbb{P}^1(F)$, the stabilizer of this line consists of the subgroup $B(F)$ of upper triangular matrices. Likewise, the stabilizer of $[1 : 0]$ consists of lower triangular matrices; we write $B^-(F)$ for this subgroup. Since $GL_2(F)$ or $SL_2(F)$ act transitively on $\mathbb{P}^1(F)$, we conclude that the stabilizer of any point is a conjugate of $B(F)$. We write $T(F)$ for the intersection $B(F) \cap B^-(F)$; $T(F)$ consists of diagonal matrices.

Lemma 6.1.3.1. *The group $U(F)$ is a normal subgroup of $B(F)$.*

Proof. Any element of $B(F)$ can be written as

$$\begin{pmatrix} \alpha_1 & \gamma \\ 0 & \alpha_2 \end{pmatrix},$$

and the inverse of such a matrix is

$$\begin{pmatrix} \alpha_1^{-1} & \frac{\gamma}{\alpha_1\alpha_2} \\ 0 & \alpha_2^{-1} \end{pmatrix},$$

so the result follows by explicit matrix multiplication. □

6.1.4 Multiple transitivity of $SL_2(F)$

We now study multiple transitivity of the action of $SL_2(F)$ where some subtleties arise.

Corollary 6.1.4.1. *The group $SL_2(F)$ acts 2-transitively on $\mathbb{P}^1(F)$. This action is 3-transitive if and only if every element of $F^\times$ is a square.*

Proof. For the first statement, we can fix any element of $\mathbb{P}^1(F)$, say the element ∞. In that case, it suffices to prove that the induced action of $B(F)$ on $\mathbb{P}^1(F) \setminus \infty$ is transitive. If we think of elements of $\mathbb{P}^1(F)$ in terms of homogeneous coordinates, then we have removed $[1 : 0]$. Given any element $[x_1 : y_1]$ with $y_1 \neq 0$, this element is uniquely specified by $[\frac{x_1}{y_1} : 1]$. Now, take the vector $[0 : 1]$. An upper-triangular matrix in $SL_2(F) \cap B(F)$ is of the form

$$\begin{pmatrix} \alpha^{-1} & \beta \\ 0 & \alpha \end{pmatrix},$$

and this acts on $(0,1)^t$ by sending it to $(\beta, \alpha)^t$, which corresponds to the point $\frac{\beta}{\alpha}$. This provides the required matrix.

For the last statement, we can observe that $SL_2(F)$ acts 3-transitively on $\mathbb{P}^1(F)$ if and only if for any two points $x_1, x_2 \in \mathbb{P}^1(F)$, $G_{x_1} \cap G_{x_2}$ acts transitively on $\mathbb{P}^1(F) \setminus \{x_1, x_2\}$. Since $SL_2(F)$ acts 2-transitively, we can pick x_1 and x_2 however we wish, so take $x_1 = 0$ and $x_2 = \infty$. In that case $G_{x_1} = B(F)$, while G_{x_2} is the subgroup of lower triangular matrices intersected with $SL_2(F)$. Therefore, $G_{x_1} \cap G_{x_2} = T(F) := diag(\alpha, \alpha^{-1})$. Therefore, we want to show that $x \in \mathbb{P}^1(F) \setminus \{0, \infty\}$, then $T(F)$ acts transitively. Consider the points $[x : 1]$ with $x \neq 0$. We want to know that $diag(\alpha, \alpha^{-1})(1,1)^t = \lambda(x,1)^t$, but the former is equivalent to $[\alpha^2 : 1] = [x : 1]$, so the condition $x = \alpha^2$ is necessary and sufficient. □

6.1.5 Multiple transitivity and normality

Proposition 6.1.5.1. *If a group G acts 2-transitively on a set X, then any normal subgroup $N \subset G$ acts on X either trivially or transitively.*

Proof. Suppose N acts non-trivially on X. Then, there exists $x \in X$ such that $n \cdot x = x' \neq x$. Now, pick y and y' with $y \neq y'$. Since G acts 2-transitively, we can pick $g \in G$ such that $y = gx$ and $y' = gx' = g \cdot nx$. In that case, $g \cdot nx = gng^{-1} \cdot gx$, i.e., $y' = n'y$, with $n' = gng^{-1}$. □

Neither of the groups $SL_2(F)$ or $GL_2(F)$ are simple *in general* as in either case there is an evident normal subgroup: the center of $SL_2(F)$ or $GL_2(F)$. If F has characteristic 2, then $\alpha^2 - 1 = (\alpha - 1)^2$ and thus the subgroup $Z(SL_2(F))$ is trivial. Since the centers act trivially on $\mathbb{P}^1(F)$, it follows that both $PGL_2(F)$ and $PSL_2(F)$ act on $\mathbb{P}^1(F)$. We will analyze simplicity of $PSL_2(F)$ next time by studying the action on $\mathbb{P}^1(F)$: we will analyze the action of normal subgroups of $SL_2(F)$ and show they must be non-trivial, and then conclude that normal subgroups must therefore be "big".

6.2 Lecture 21: Simplicity of some group actions

6.2.1 Simplicity of $PSL_2(F)$

Last time we studied the actions of $PGL_2(F)$ and $PSL_2(F)$ on $\mathbb{P}^1(F)$. In particular, we showed the former action was 3-transitive while the latter action was always at least 2-transitive. We wanted to investigate simplicity of $PSL_2(F)$. To this end, we want to analyze normal subgroups of $PSL_2(F)$. Since the action of $PSL_2(F)$ on $\mathbb{P}^1(F)$ is 2-transitive, it follows from Proposition 6.1.5.1 that the induced action of a normal subgroup of $PSL_2(F)$ on $\mathbb{P}^1(F)$ is either trivial or transitive.

Lemma 6.2.1.1. *A normal subgroup of $PSL_2(F)$ acts transitively on $\mathbb{P}^1(F)$.*

Proof. By the correspondence theorem, there is a bijection between normal subgroups of $PSL_2(F)$ and normal subgroups of $SL_2(F)$ that contain the center, so it suffices to show that any normal subgroup of $SL_2(F)$ that acts trivially on $\mathbb{P}^1(F)$ necessarily is contained in the center.

Suppose N is a normal subgroup of $SL_2(F)$ and assume N acts trivially on $\mathbb{P}^1(F)$. Since the stabilizers of the $SL_2(F)$-action on $\mathbb{P}^1(F)$ are the conjugates of $B(F)$, we conclude that N is contained in the intersection of the conjugates of $B(F)$. In particular, N is contained in the intersection of $B(F)$ (the stabilizer of 0) and $B^-(F)$ (the stabilizer of ∞). These correspond to upper and lower triangular matrices, and their intersection consists of diagonal matrices, so in particular we know that $N \subset T(F)$. Any element of $T(F)$ is of the form $diag(\alpha, \alpha^{-1})$ since it is a diagonal matrix with determinant 1. On the other hand, there is a bijection $F^\times \to \mathbb{P}^1(F) \setminus \{0, \infty\}$ given by $x \mapsto [x : 1]$. An element $diag(\alpha, \alpha^{-1})$ of $T(F)$ acts trivially on $[x : 1]$ if and only if $\alpha^2 = 1$, but this means that the element is in the center. Thus, a normal subgroup of $SL_2(F)$ acting trivially on $\mathbb{P}^1(F)$ is contained in the center of $SL_2(F)$, and we conclude. □

Since normal subgroups of $SL_2(F)$ that contain the center must act transitively on $\mathbb{P}^1(F)$, we want to show that such subgroups are large. First, we will observe that the subgroups $B(F)$ themselves have a maximality property. Then, we remember some facts about generation of $SL_2(F)$ by shearing matries (from the HW). Combining these facts will allow us to conclude.

Lemma 6.2.1.2. *Subgroups conjugate to $B(F)$ are maximal subgroups, i.e., proper subgroups of $SL_2(F)$ that are contained in no other proper subgroup.*

Proof. We actually prove a more general statement: if a group G acts 2-transitively on a set X, then the stabilizer of any point is a maximal subgroup. To see this, fix a point $x \in X$, and let $H = G_x$. Suppose H is not maximal, i.e., there exist proper inclusions of the form $H \subset K \subset G$. Pick $g \in G$ with $g \notin K$ and $k \in K$ with $k \notin H$. Since g and k are not in H, they do not stabilize H_x and thus gx and kx are not equal to x. Now since G acts 2-transitively on X, there exists $h \in G$ such that $hx = x$ and $h(gx) = kx$, i.e., $h \in H$ and $k^{-1}hgx = x$, i.e., $k^{-1}hg \in H$. Since $H \subset K$ by assumption, it follows that $kH \subset K$ and thus that $k(k^{-1}hg) = hg \in K$. Again, multiplying on the left by h^{-1}, which is an element of H, we conclude that $g \in K$, which is a contradiction. □

Theorem 6.2.1.3. *If $|F| \geq 4$, then $PSL_2(F)$ is simple.*

Proof. Suppose N is a normal subgroup of $SL_2(F)$. Without loss of generality, we may assume that N is strictly larger than the center. In that case, by appeal to Lemma 6.2.1.1, we may assume that N acts transitively on $\mathbb{P}^1(F)$. The subset $NB(F)$ is a subgroup of $SL_2(F)$ (since N is normal) which contains $B(F)$ by construction. Since $B(F)$ is a maximal subgroup by Lemma 6.2.1.2, $NB(F)$ is either equal to $B(F)$ or all of $SL_2(F)$. If $NB(F) = B(F)$, then that means $N \subset B(F)$ and thus N fixes a point, which contradicts the fact that it acts transitively. Therefore, we conclude that $NB(F) = SL_2(F)$.

We also saw that $B(F)$ has the normal subgroup $U(F)$, which happens to be an abelian group (isomorphic to the additive group of F). Since N is normal in $SL_2(F)$, we conclude that $NU(F)$ is necessarily normal in $NB(F) = SL_2(F)$ as well. For an arbitrary element $g \in SL_2(F)$, since $U(F) \subset NU(F)$, note that $gU(F)g^{-1} \subset gNU(F)g^{-1}$ and the latter is simply $NU(F)$ since it is normal. Since g was arbitrary, we conclude that $NU(F)$ contains all the conjugates of $U(F)$. However, $SL_2(F)$ is generated by the subgroup $U(F)$ and its conjugates (in fact, just $U(F)$ and $U^{-}F$), so we conclude that $NU(F) = SL_2(F)$ itself.

By the isomorphism theorems, $SL_2(F)/N = NU(F)/N = U(F)/(N \cap U(F))$. Since $U(F)$ is abelian, so is $U(F)/(N \cap U(F))$. By the universal property of the commutator subgroup, we conclude that $[SL_2(F), SL_2(F)] \subset N$. However, if $|F| \geq 4$, then $[SL_2(F), SL_2(F)] = SL_2(F)$ (again, established on HW1), so we conclude that $N = SL_2(F)$. □

Remark 6.2.1.4. The only place $|F| \geq 4$ is used in the proof is in the assertion about the commutator subgroup. Note that the statements above are actually false if $|F| = 2$ or $|F| = 3$. The last step also explains why we did not bother working with $GL_2(F)$ from the start: upon passing to the commutator subgroup we would have ended up in the same place.

6.2.2 Simplicity of $PSL_n(F)$

The arguments we have given here can be significantly generalized. The method of proof we used to establish simplicity of $PSL_2(F)$ can be axiomatized in the following form.

Theorem 6.2.2.1 (Iwasawa)**.** *Let G be a group that acts doubly transitively on a set X via $\varphi : G \to Isom(X)$, and set $K = \ker(\varphi)$. If*

i) for some $x \in X$, $Stab_G(x)$ has an abelian normal subgroup whose conjugates generate G, and

ii) $[G, G] = G$,

then G/K is a simple group.

Theorem 6.2.2.2. *If $n \geq 3$ is an integer, and F is a field, then $PSL_n(F)$ is simple.*

Sketch of proof. In this generality, Iwasawa's lemma can be used to prove simplicity of $PSL_n(F)$. Indeed, define $\mathbb{P}^{n-1}(F)$, to be the set of 1-dimensional subspaces of $F^{\oplus n}$. The standard left multiplication action of $SL_n(F)$ on $F^{\oplus n}$ (column vectors of length n) induces an action of $PSL_n(F)$ on $\mathbb{P}^{n-1}(F)$.

Consider the action of $GL_n(F)$ on $\mathbb{P}^{n-1}(F)$. We can show this action is 2-transitive, and the 2-transitivity of the $SL_n(F)$ action can be deduced from this. Next, we already know that the commutator subgroup of $SL_n(F)$ is equal to $SL_n(F)$: if $n \geq 3$ this is true without restriction on F!

Finally, we have to show that stabilizers of points have abelian normal subgroups whose conjugates generate the whole group. Any stabilizer is conjugate to the stabilizer of $[1 : 0 : \cdots : 0]$ (this is a natural generalization of what we wrote before for $\mathbb{P}^1(F)$. Indeed, the stabilizer of the subspace $(\lambda, 0, \ldots, 0)^t$ in GL_n consists of block matrices of the form

$$P(F) := \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ 0 & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & x_{2n} & \cdots & x_{nn} \end{pmatrix}.$$

The normal subgroup consisting of matrices of the form

$$U(F) := Id_n + \sum_{j=2}^{n} x_{1j} e_{1j}$$

is an abelian normal subgroup. It remains to check that its conjugates generate all of $SL_n(F)$, but I leave this is an exercise using elementary matrix factorizations. □

6.2.3 Simplicity of A_n

The ideas used above can, in some sense, also be used to prove simplicity of A_n. We have a natural action of A_n on a set with n elements. When $n = 3$, this action is transitive since A_3 is the cyclic group of order 3, and this group acts transitively on a 3 element set.

If we consider A_n acting $\{1, \ldots, n\}$, then the stabilizer of any point is isomorphic to A_{n-1}. Using an induction argument and the characterization of multiple transitivity, we gave above, it is straightforward to demonstrate the following fact.

Lemma 6.2.3.1. *For any integer $n \geq 3$, the standard action of the group A_n on the set $\{1, \ldots, n\}$ as permutations is $(n-2)$-transitive.*

Remark 6.2.3.2. Consider the group A_5. One can show that A_5 is abstractly isomorphic to $PSL_2(\mathbb{F}_5)$, and therefore its simplicity is assured by our results above. Hopefully, we will come back to this later. Nevertheless, Iwasawa's lemma isn't so useful in proving that the alternating groups are simple for $n \geq 6$ since point stabilizers will be simple and therefore will not contain non-trivial abelian normal subgroups.

Lemma 6.2.3.3. *The group A_n is generated by 3-cycles for $n \geq 3$.*

Proof. Since every element of S_n may be written as a product of transpositions, and sign the kernel of the sign homomorphism consists of even permutations, it follows that every element of A_n may be written as a product of disjoint transpositions. Therefore, to establish the result it suffices to show that any product of transpositions can be written as a product of 3-cycles. Now, we treat a few cases. If the 2-cycles in a product of disjoint transpositions agree, then the element is the identity. If the disjoint transpositions have 1 element in common, then the formula $(ij)(jl) = (ijl)$ shows they already yield a 3-cycle. Finally, if they have no element in common, then they commute. In that case, the formula $(ij)(kl) = (ijk)(jkl)$, which is obtained by direct computation, shows that they may be written as a product of 3-cycles. □

Since we already showed that all 3-cycles are conjugate in A_n, the next result is an immediate consequence.

Corollary 6.2.3.4. *If a normal subgroup of A_n, $n \geq 3$, contains a 3-cycle, then it must be all of A_n.*

Theorem 6.2.3.5. *The group A_n, $n \geq 5$ is simple.*

Proof. Assume $n \geq 5$, and we proceed by induction. We already know A_5 is simple. Consider the action of A_n on the set $\{1, \ldots, n\}$. The stabilizer of any point is isomorphic to A_{n-1}, which by the induction hypothesis is assumed simple. Suppose N is a non-trivial normal subgroup of A_n; our goal is to show that $N = A_n$.

Pick a non-trivial element σ of N. Since N is normal, all conjugates of σ are contained in N. To use the induction hypothesis, we want to produce a subgroup that intersects the stabilizer of a point non-trivially.

To do this, it suffices to show that given our element σ, and some integer i, we can produce a conjugate σ' (not equal to σ!) that fixes i. The product $\sigma'\sigma^{-1}$ then lies in the stabilizer H_i of i and produces a non-trivial element of the intersection of $N \cap H_i$. However, $N \cap H_i = H_i$ since H_i is simple by induction. Note that each H_i contains a 3-cycle, so assuming the claim, we are done. □

Lemma 6.2.3.6. *For any integer $n \geq 5$, given any any $\sigma \neq 1$ in A_n, there exists a conjugate σ' of σ with $\sigma' \neq \sigma$ such that $\sigma(i) = \sigma'(i)$ for some i.*

Example 6.2.3.7. If $\sigma = (12345)$ in A_5, then $\sigma(1) = 2$. We thus want to find a conjugate σ' of σ that still has $\sigma'(1) = 2$. If we conjugate by a cycle disjoint from 1 and 2 then this will do the job. For example, if $\pi = (45)$, then $\pi\sigma\pi^{-1} = (12534)$, which is not equal to (12345) since the values at $\sigma(2)$ differ. Likewise, conjugation by $\pi = (34)$ or (35) or (345) will do the job. The proof in the general case can be reduced to treating cycles.

Remark 6.2.3.8. If $n = 4$, the statement is simply false in general. For example, take two products of disjoint transpositions (there are 3): $(12)(34)$, $(13)(24)$ and $(14)(23)$; none of these transpositions fix an element. However, this problem (at least with disjoint transpositions) disappears if $n \geq 5$: all of these disjoint transpositions will fix, e.g., 5.

Proof. Let σ be a non-identity element of A_n. Let r be the length of longest disjoint cycle appearing in a decomposition of σ. By conjugating, we may assume that $\sigma = (12 \cdots r)\pi$, where $(12 \cdots r)$ and π are disjoint. Now, we do a case by case analysis. Since σ is not the identity, $r \geq 2$.

If $r = 2$, then σ is a product of disjoint transpositions. If there 2 disjoint transpositions involved, then after further conjugation if necessary, we can assume that $\sigma = (12)(34)$. As we saw in the above example, if we take $\sigma' = (13)(24)$, then σ and σ' are conjugate in A_n and they both fix 5. If σ has at least 3 disjoint transpositions, then $n \geq 6$ and we can write $\sigma = (12)(34)(56) \cdots$ by conjugating if necessary. If $\tau = (12)(35)$, then a straightforward computation shows that $\sigma' = \tau\sigma\tau^{-1} = (12)(36)(45)$. Here $\sigma(1) = \sigma'(1) = 2$, while $\sigma(3) \neq \sigma'(3)$ (of course, there are other possible choices).

If $r \geq 3$, then $\sigma(1) = 2$. Take, e.g., $\tau = (345)$. In that case set $\sigma' = \tau\sigma\tau^{-1}$ and observe that $\sigma(1) = \sigma'(1) = 2$, while $\sigma(2) = 3$, while $\sigma'(2) = 4$, i.e., $\sigma' \neq \sigma$. □

Part II

Fields and Galois theory

Chapter 7

Basic theory of field extensions

7.1 Lecture 22: Preliminaries on Rings and Fields

While we have already been using some basic facts from the theory of rings and fields, let us fix the definitions now for completeness.

7.1.1 Ring theoretic terminology

Recall that a (unital) ring is a collection $(R, +, \cdot, 0, 1)$ where R is a set, $+, \cdot$ are functions $R \times R \to R$ such that $(R, +, 0)$ forms an abelian group, $(R, \cdot, 1)$ is a monoid (i.e., multiplication is associative and 1 is a multiplicative unit), and multiplication distributes over addition. There is a unique ring structure on the 1 element set 0; we call this the trivial ring and note that in this ring $0 = 1$. In fact, if $0 = 1$ in a ring, then the ring is trivial ($r = 1r = 0r = 0$ for every $r \in R$). A ring is called commutative if $\cdot$ is a commutative multiplication.

A ring homomorphism is a function $f : R \to S$ that preserves addition and multiplication and sends 1_R to 1_S. There is a unique ring homomorphism $R \to 0$. Likewise, there is a unique ring homomorphism $\mathbb{Z} \to R$ sending 1.

If R is a ring, then each element $r \in R$ defines a function $R \to R$ via left (resp. right) multiplication (this function is not a ring homomorphism as it does not respect multiplication; because of distributivity it is a homomorphism of the underlying additive groups). We will say that r is a left (resp. right) unit if left multiplication by r (resp. right multiplication by r) is an isomorphism of rings. We will say that r is a two-sided unit if both left and right multiplication by R are isomorphisms. If both left and right multiplication by r are isomorphisms, there exists a uniquely defined element $s \in R$ such that $rs = sr = 1$; we write r^{-1} for s.

We will say that $r \in R$ is a (left, right, two-sided) *zerodivisor* if the relevant multiplication map has a non-zero kernel. We will say that r is (left, right, two-sided) *regular* if the relevant multiplication map is injective. For commutative rings there is no need to distinguish cases. Note that the zero ring has no non-zero divisors by this definition.

Definition 7.1.1.1. A ring R is called an *integral domain* if it is non-zero and contains no non-zero zero-divisors (sometimes these are called non-trivial zero divisors).

The set of non-zero divisors in a R is a multiplicatively closed set in that it contains 1 and for any two elements in this set, the product is also in this set.

If S_1 and S_2 are two subsets of a ring R, then we write S_1S_2 for the subset of R consisting of all finite sums $r_1s_1 + \cdots + r_ns_n$ with $r_i \in S_1$ and $s_i \in S_2$. A subset $I \subset R$ is a *(left, right, two-sided) ideal* if I is an additive subgroup of R and $RI \subset I$ (resp. $IR \subset I$, $RI \subset I$ and $IR \subset I$). Intersections of ideals are ideals, and one checks that RS (resp. SR, resp. RSR) is the smallest left (resp. right, two-sided) ideal containing S; we write $\langle S \rangle \subset R$ for this ideal if there is no possibility of confusion. If R is a ring, and I is a two-sided ideal, then there is a unique up to isomorphism ring R/I and a ring homomorphism $\varphi : R \to R/I$ with kernel equal to I. We define R/I as a set to be the cosets of I in R and the ideal property implies that multiplication makes sense.

Example 7.1.1.2. The ring $\mathbb{Z}$ is an integral domain. We know that every subgroup of the additive group $\mathbb{Z}$ is isomorphic to $n\mathbb{Z}$ for some integer n. In fact, each of these subgroups has the structure of an ideal (the product of numbers divisible by n is divisible by n), so it follows that the quotient ring $\mathbb{Z}/n\mathbb{Z}$ makes sense and comes equipped with a ring homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ (the underlying abelian group of the latter is $\mathbb{Z}/n\mathbb{Z}$). If m and n are coprime integers, then our isomorphism of abelian groups $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is actually a ring isomorphism (the ring structure on the product is componenentwise addition and multiplication with zero element $(0, 0)$ and unit $(1, 1)$). In particular, $(1, 0)$ is a zero-divisor if m and n are both not 1. Thus, $\mathbb{Z}/n\mathbb{Z}$ contains zero divisors if n has more than 1 prime factor. If $n = p^r$ for $r > 1$, then $p \cdot p^{r-1} = 0$ so we have non-trivial zero divisors as well. Therefore, $\mathbb{Z}/\langle n \rangle$ is an integral domain if and only if n is either a prime number or 0.

7.1.2 Definitions and examples

Definition 7.1.2.1. A quintuple $(F, +, \cdot, 0, 1)$ with $0 \neq 1$ is called a field if it is a commutative ring and the unit group $F^{\times}$ coincides as a set with $F \setminus 0$. A morphism of fields is a morphism of the underlying rings.

Remark 7.1.2.2. Note that in the definition we require that the commutative ring underlying a field cannot be the zero ring!

Example 7.1.2.3. For any prime number p, the ring $\mathbb{Z}/p\mathbb{Z}$ has the structure of a field; we will usually write $\mathbb{F}_p$ for this field. We write $\mathbb{Q}$ for the field of rational numbers.

Example 7.1.2.4. Suppose F is any field. Write $F[t]$ for the polynomial ring in 1 variable over F, i.e., elements of $F[t]$ are finite sums of the form $\sum_i a_i t^i$, where t is an indeterminate and $a_i \in F$. A rational function is a fraction $\frac{p(t)}{q(t)}$ where $q(t) \neq 0$. With the usual notions of addition and multiplication of fractions, the set $F(t)$ of rational functions in a single variable is a field, which is an extension of F. Analogously, we can define $F(t_1, \ldots, t_n)$ as the set of rational functions in several variables: these are quotients of polynomials in the indeterminates $t_1, \ldots, t_n$, again with non-zero denominator.

Example 7.1.2.5. If F is a field, and t is a variable, a formal power series with coefficients in F is an expression of the form $\sum_{i \geq 0} a_i t^i$ with $a_i \in F$. Write $F[[t]]$ for the set of formal powers series in 1 variable over F. Such expressions form a ring under componentwise addition, and multiplication defined by

$$f(t)g(t) = (\sum_{i \geq 0} a_i t^i)(\sum_{j \geq 0} b_i t^j) = \sum_{k \geq 0} \sum_{i+j=k} a_i b_j t^k.$$

A *formal Laurent series* over F is an expression of the form

$$\sum_{i \geq -n} a_i t^i,$$

i.e., a sum $\sum_{i \in \mathbb{Z}} a_i t^i$ where all but finitely many a_i with $i < 0$ are zero. Write $F((t))$ for the set of formal Laurent series with coefficients in F. The set $F((t))$ is a field with addition and multiplication defined as for formal power series.

Example 7.1.2.6. Recall that a function $f : \mathbb{C} \to \mathbb{C}$ is said to be analytic at $a \in \mathbb{C}$ if there exists an open disc around a such that $f(z)$ is equal to a convergent power series $\sum_{n=0}^{\infty} c_n (z-a)^n$ in that open disc. Write $Hol(z)$ for the set of functions analytic at every point $a \in \mathbb{C}$; we refer to functions in this set as holomorphic (or entire). The set of holomorphic functions forms a ring (we can think of this as a sub-ring of the ring of formal power series over $\mathbb{C}$). A *meromorphic function* is an expression of the form $\frac{f(z)}{g(z)}$ where $f(z)$ is holomorphic and $g(z)$ is a non-zero holomorphic function. The set $Mer(z)$ is a field for the usual notions of addition and multiplication of fractions.

Example 7.1.2.7. Consider the integers $\mathbb{Q}$ and fix a prime number p. Given any non-zero rational number q, there is a unique way to write $q = p^n \frac{a}{b}$ where neither a nor b is divisible by p. Define a function $\mathbb{Q} \setminus 0 \to \mathbb{Q}^{>0}$ by the formula

$$q = p^n \frac{a}{b} \mapsto p^{-n} =: |q|_p.$$

Extend this function to $\mathbb{Q}$ by setting $|0|_p = 0$. Observe that, with this definition, $|q|_p = 0$ if and only if $q = 0$. Given a pair of rational numbers q and q', consider the function $|q - q'|_p$. This function is non-negative and symmetric by construction. Also $|q - q'|_p = 0$ only if $q = q'$. A very strong form of the triangle inequality holds:

$$|q - q''|_p \leq max(|q - q'|_p, |q' - q''|_p);$$

this formula is called the ultrametric inequality. We define $\mathbb{Q}_p$ to be the Cauchy completion of the metric space $(\mathbb{Q}, | - |_p)$. You can check that $\mathbb{Q}_p$ is a field.

7.1.3 The characteristic of a field

If F is a field, then we consider the ring homomorphism $\mathbb{Z} \to F$ sending 1 to 1_R. The image of this ring homomorphism is isomorphic to a quotient ring of $\mathbb{Z}$, and we analyzed all such quotients in Example 7.1.1.2. As the image of this ring homomorphism is a non-zero subring of F, it necessarily contains no zerodivisors and is thus an integral domain. Thus, again by appeal to Example 7.1.1.2 we conclude that it must be isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for n either 0 or a prime number.

Definition 7.1.3.1. If F is a field, the characteristic of F is a natural number n that is defined to be 0 if the canonical homomorphism $\mathbb{Z} \to F$ is injective, and p if the image of the canonical homomorphism $\mathbb{Z} \to F$ is $\mathbb{Z}/p\mathbb{Z}$.

7.1.4 Field extensions

Lemma 7.1.4.1. *Any morphism of fields is injective.*

Proof. Suppose $\varphi : F \to E$ is a homomorphism of fields. If $I = \ker(\varphi)$, then I is an ideal. If $x \in I$ is a non-zero element, then observe that x has a multiplicative inverse, and $1 = x^{-1}x \in I$. As a consequence we see that I contains all of F. Thus, $\varphi : F \to E$ must be the trivial map, but the trivial map is not a ring homomorphism since it does not send the identity to the identity. □

Definition 7.1.4.2. If $F \to E$ is a morphism of fields, then we will say that E is an extension of F.

Lemma 7.1.4.3. *If E is an extension of F, then E has the structure of an F-vector space.*

Proof. We already know that F is a group under addition. Scalar multiplication by elements of F arises from the inclusion $F \hookrightarrow E$ and the usual multiplication in F. The field axioms then imply the vector space axioms hold. □

Definition 7.1.4.4. An extension E/F is said to be *finite* if E is a finite-dimensional F-vector space and *infinite* otherwise. If E/F is a finite extension, then the natural number $[E : F] := dim_F E$ is called the degree of the extension.

7.2 Lecture 23: Extensions, automorphisms and algebraicity

Today, we will continue developing terminology related to extensions of rings. Last time, we observed that every homomorphism of fields is injective. In particular, if $i : F \to E$ is an extension, then E is an F-vector space.

7.2.1 Extensions and automorphisms

Lemma 7.2.1.1. *If F is a field having characteristic 0, then F is an extension of the rational numbers. If F is a field having characteristic $p > 0$, then F is an extension of $\mathbb{F}_p$. Moreover, any finite field necessarily has p^n elements for p some prime number.*

Proof. For the first case, since $\mathbb{Z} \hookrightarrow F$ is an injection, and F is a field, we conclude that $\frac{1}{n}$ lies in F for each $n \in \mathbb{Z} \setminus 0$ and thus $\frac{p}{q}$ lies in F for each $q \neq 0$. For the second point, if $E/\mathbb{F}_p$ is a finite extension, then E is a finite-dimensional $\mathbb{F}_p$-vector space and is thus isomorphic to $\mathbb{F}_p \oplus \cdots \mathbb{F}_p$ after choice of a basis. In particular, if n is the dimension of $E/\mathbb{F}_p$, then E has p^n elements. □

If we fix a field F, then we may consider the category Fld_F of extensions of F: objects are extensions $i : F \to E$ and morphisms are commutative diagrams of field homomorphisms. Morphisms are suitable commutative diagrams. Typically, we will write E/F, viewing F as a subfield of E via i, which is suppressed from notation.

Example 7.2.1.2. While a morphism in Fld_F is always injective, morphisms need not be surjective in general. For exmaple, take $F = \mathbb{Q}$ and $E = \mathbb{Q}(t)$, the field of rational functions in 1 variable over $\mathbb{Q}$. The assignment $t \mapsto t^2$ defines a field homomorphism $\mathbb{Q}(t) \hookrightarrow \mathbb{Q}(t)$, but this homomorphism is evidently not surjective.

Definition 7.2.1.3. If E/F is a field extension, an F-isomorphism of E is an isomorphism $\varphi : E \to E$ in Fld_F, i.e., it is a ring isomorphism $\varphi : E \to E$ such that $\varphi(f) = f$.

Since Fld_F is a category, the set of F-isomorphisms of an extension E/F form a group $Aut_F(E)$. Given a tower of extensions $L/E/F$, i.e., given any morphism $E \to L$ in Fld_F, we may consider the groups $Aut_F(L)$, and $Aut_E(L)$. Since $F \subset E$, every E-isomorphism of L may be viewed as an F-isomorphism of L, i.e., there is an injective homomorphism $Aut_E(L) \to Aut_F(L)$. Our primary goal will be to analyze properties of fields in terms of these automorphism groups.

7.2.2 Generating new extensions

Lemma 7.2.2.1. *If E/F is a finite extension of fields of degree $[E : F]$ and L/E is another finite extension of fields of degree $[L : E]$, then L/F is also a finite extension of degree $[L : F] = [L : E][E : F]$.*

Proof. Exercise. □

Lemma 7.2.2.2. *If E/F is a field extension, and $A \subset E$ is a collection of elements, then there is a unique smallest sub-field $F(A) \subset E$ with $F \subset F(A)$ containing the elements of A.*

Proof. The collection of all fields containing $F \cup A$ is non-empty (it contains E). Since the intersection of two fields is a field, we simply take the intersection of all fields containing F and A. □

Definition 7.2.2.3. If E/F is a field extension, and $A \subset E$ is a subset of E, we refer to $F(A)$ as the subfield of E generated by A. An extension E/F is called *finitely generated over F* if there exists a finite set $A \subset E$ such that $E = F(A)$. An extension E/F is called *simple* if it can be generated by a single element.

Example 7.2.2.4. If E/F is a finite extension, then E is finitely generated over F. Indeed, E is a finite-dimensional F-vector space, so we may choose an F-basis of E/F. The elements of this F-basis yield the required generating set.

7.2.3 Recollections on principal ideal domains

If E/F is a finite extension, then left multiplication by $e \in E$ defines an endomorphism of E viewed as an F-vector space. We want to use "techniques of linear algebra" to study this endomorphism. Note that "left multiplication by a" gives rise to a ring homomorphism

$$\begin{aligned} F[t] &\longrightarrow End_F(E) \\ t &\longmapsto a \cdot . \end{aligned}$$

Note that αt^n gets sent to multiplication by αa^n under this homomorphism. The kernel of this ring homomorphism is an ideal I in $F[t]$. If the ideal I is non-zero, then it contains a non-zero polynomial $g(t)$ with coefficients in F. The fact that I is sent to zero under the homomorphism amounts to saying that $g(a) = 0$, i.e., that a satisfies a polynomial with coefficients in F. We can refine this observation significantly with more information about the ideal structure of $F[t]$.

Recall that an ideal is called principal if it can be generated by a single element. A commutative ring R is called a principal ideal ring if every ideal is principal and a *principal ideal domain* (PID) if it a principal ideal ring and also an integral domain.

Lemma 7.2.3.1. *If F is a field, then $F[t]$ is a principal ideal domain.*

Proof. If I is trivial, then $I = (0)$, so we may assume that I is non-trivial. Now, every element of I is a polynomial, and so we may choose any (non-zero) element f of I that has minimal degree. We claim that $I = (f)$. Now, in $F[t]$, we have division with remainder, i.e., if g is any polynomial, then we can uniquely write $g = qf + r$, where q and r are also polynomials and r has degree strictly smaller than f. Take any $g \in I$ and write $g = qf + r$. It follows that $r = g - qf$ is also in I. If r was non-zero, then we would contradict the minimality of f, so we conclude that $g = qf$, which is precisely what we wanted to show. □

Definition 7.2.3.2. If R is a commutative ring, an ideal $\mathfrak{p} \subset R$ is *prime* if given any two elements $a, b \in R$ with $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. An ideal $\mathfrak{m}$ is *maximal* if for any ideal $I \subset R$, the inclusion $\mathfrak{m} \subset I$ implies either $\mathfrak{m} = I$ or $I = R$.

Lemma 7.2.3.3. *If R is a principal ideal domain, then every non-zero prime ideal is maximal.*

Proof. Suppose $\mathfrak{p}$ is a non-zero prime ideal. We can write $\mathfrak{p} = (f)$ for some element $f \in R$. If I is an ideal with $\mathfrak{p} \subset I$, then we may write $I = (g)$ for some element $g \in R$. Since $f \in I$, it follows that $f = rg$ for some element $r \in R$. □

Definition 7.2.3.4. If F is a field, and $f \in F[t]$ is a non-constant polynomial, then f is called *irreducible* (over F) if (f) is prime.

Remark 7.2.3.5. Of course, this definition is equivalent to the classical definition of irreducibility in terms of writing f as a product of factors of strictly lower degree.

7.2.4 Algebraic extensions

Definition 7.2.4.1. If E/F is a field extension, an element $a \in E$ is called *algebraic over* F if there is a non-zero polynomial with coefficients in f, say $f(t)$, such that $f(a)$ = 0. Any element that is not algebraic over F is called *transcendental over* F. The extension E/F is called *algebraic* if every $a \in E$ is algebraic over F.

Example 7.2.4.2. Perhaps the basic example of an extension that is not algebraic is $F(t)/F$: by construction, the element t satisfies no polynomial with coefficients in F. Note that if $a \in E$ is algebraic over f, then since f satisfies some polynomial, by factoring the polynomial it satisfies, it necessarily satisfies some irreducible polynomial as well. We may analyze this polynomial in more detail now.

Lemma 7.2.4.3. *Suppose E/F is an extension, and $a \in E$ is algebraic over F. There is a unique monic irreducible polynomial $g \in F[t]$ such that $g(a) = 0$.*

Proof. Consider the ideal $ker(ev_a)$. Since a satisfies some polynomial with coefficients in F, say f, we know that $f \in ker(ev_a)$. Thus, $(f) \subset ker(ev_a)$. On the other hand, $F[t]$ is a principal ideal domain, and so $ker(ev_a)$ is principal, generated by an element g of minimal degree in $ker(ev_a)$. If $g = \sum_{i=0}^{d} a_i t^i$ with $a_d \neq 0$, then by multiplying by a_d^{-1}, we can assume that g is monic as well. By long division, this element is unique.

If $g(x)$ were reducible, we could write $g(x) = h(x)h'(x)$, which would mean that $g(a) = h(a)h'(a)$. Since $g(a) = 0$, this means $h(a) = 0$ or $h'(a) = 0$. However, this means that either $h(x)$ or $h'(x)$ is a polynomial of degree $< g(x)$ having a as a root, which contradicts the minimality of $g(x)$. □

7.3 Lecture 24: Algebraic extensions and splitting

7.3.1 Algebraic extensions

Last time we proved that if E/F is an extension and $a \in E$ is algebraic over F, then there is a unique monic irreducible polynomial $g \in F[t]$ such that a satisfies g, i.e., $g(a) = 0$. We now give this polynomial a name.

Definition 7.3.1.1. If E/F is an extension and $a \in E$ is algebraic over F, then the unique monic irreducible polynomial $g \in F[t]$ of lowest degree such that $g(a) = 0$ will be called the *minimal polynomial* of a.

Example 7.3.1.2. The minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$. The minimal polynomial of $2^{\frac{1}{3}}$ is $x^3 - 2$. In general, we need some criteria for determining irreducibility of a polynomial, and we will come back to this later.

Lemma 7.3.1.3. *If E/F is an extension field, $a \in E$ is algebraic over F, f is the minimal polynomial of a, and f has degree d, then $F(a)$ is an extension of degree d of F with a basis given by $1, a, \ldots, a^{d-1}$. Moreover, $F(a)$ is the field obtained by adjoining a to F (i.e., the notation is unambiguous).*

Proof. Since $F(a)$ is the quotient $F[t]/\ker(ev_a)$ we think of elements of $F(a)$ as expressions of the form $g + (f)$. Any such expression can be rewritten uniquely in the form $g' + (f)$ with g' of degree $< f$. Moreover, any polynomial of degree smaller than d can appear as such a coset. It follows that any element of $F(a)$ can be written in the form $\sum_{i=0}^{d-1} c_i a^i$, i.e., $1, a, \ldots, a^{d-1}$ form a basis for $F(a)/F$. It remains to observe that any extension field of F containing a must contain $F(a)$ as well. □

Lemma 7.3.1.4. *If E/F is a finite extension, then E/F is algebraic and generated by finitely many elements that are algebraic over F.*

Proof. Suppose n is the degree of E/F. Pick an F-basis $\alpha_1, \ldots, \alpha_n$ of E/F. We then have $E = F(\alpha_1, \ldots, \alpha_n)$, so E is finitely generated over F.

Given any element $a \in E$, we can write $a = \sum_i a_i \alpha_i$. Because E has degree n over F, the powers of a, i.e., $1, a, \ldots, a^n$ cannot all be distinct. Therefore, there exists a relation between these powers of the form $\sum_{i=0}^{n} \beta_i a^i = 0$. In other words, a satisfies the polynomial $\sum_{i=0}^{n} \beta_i x^i$ is a non-zero polynomial satisfied by a and thus $ker(ev_a)$ is a non-trivial ideal. Since a was arbitrary, it follows that E/F is algebraic. In particular, it follows that α_i is algebraic over F. □

The next result provides a converse to the previous result; we leave the proof as an exercise.

Lemma 7.3.1.5. *If E/F is generated by finitely many elements algebraic over F, then E is a finite extension of F.*

Remark 7.3.1.6. The subfield of $\mathbb{C}$ consisting of numbers algebraic over $\mathbb{Q}$ is an infinite extension of $\mathbb{Q}$ called the field of algebraic numbers. This field, like the rational numbers, is countable.

7.3.2 Transitivity of algebraicity

Even without assuming finite generation, we can guarantee that an algebraic extension of an algebraic extension is again an algebraic extension.

Lemma 7.3.2.1. *If E/F is an algebraic extension and L/E is an algebraic extension, then L/F is an algebraic extension.*

Proof. Let $\alpha \in L$ be an element. Since α is algebraic over E, we know that

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

with $a_i \in E$. Consider the field $F(\alpha, a_0, \ldots, a_n)$. Since E/F is algebraic by assumption, the elements a_i are all algebraic over F. Thus, the extension $F(a_0, \ldots, a_n)/F$ is generated by finitely many elements algebraic over F and thus itself algebraic over F by Lemma 7.3.1.5. The element α generates an extension of $F(a_0, \ldots, a_n)$ of degree $\leq n$ and we conclude then that $F(\alpha, a_0, \ldots, a_n)$ is also algebraic over F by Lemma 7.3.1.4. Since α was chosen arbitrarily, we conclude that L is algebraic over F. □

7.3.3 Algebraic closures

Given a field extension E/F, the extension need not be algebraic. Nevertheless, we can ask whether there exists a smallest subfield of E consisting of elements algebraic over F. Alternatively, does there exist a largest subfield of E consisting of elements algebraic over F? Intuitively, we want to consider the set of all elements $a \in E$ that are algebraic over F, but it is not immediately clear that this is a field.

Lemma 7.3.3.1. *If E/F is a field extension, and $F' \subset E$ is the set of all elements $a \in E$ that are algebraic over F, then F' is and algebraic extension of E; moreover F' is the* largest *extension of F contained in E that is algebraic over F.*

Proof. By construction $F' \subset E$ is the largest subset of E consisting of elements algebraic over F. Thus, if F' is itself a field, then the second condition is immediate.

To see that F' is a field, suppose that $a, b \in F'$. Consider the sub-extension $F(a, b) \subset F'$. Since both a and b are algebraic over F, $F(a, b)$ is generated by finitely many elements algebraic over F and is therefore itself algebraic over F. In particular, $a \pm b$, ab and $\frac{a}{b} \in F(a, b)$. Since the pair a, b were arbitrary, we conclude that F' is a subfield of E. □

Definition 7.3.3.2. If E/F is a field extension, then the *algebraic closure of F in E* is the subfield F' of E consisting of all elements that are algebraic over F.

7.3.4 Roots and Splitting fields

Lemma 7.3.4.1. *Suppose F is a field, and $\alpha \in F$. Given a polynomial f, $f(\alpha) = 0$ if and only if $f = (x - \alpha)f'$.*

Proof. Exercise. □

Definition 7.3.4.2. If F is a field, and $f \in F[x]$ is a polynomial of degree n, we say that f *has a root in F* if there exist an element $\alpha \in F$ and a polynomial f' of degree $n - 1$ such that $f = (x - \alpha)f' \in F[x]$ (the element α will be called a *root of f*). We will say that f *splits completely in F* if there exist $\alpha_1, \ldots, \alpha_n, \beta \in F$ such that $f = \beta \prod_{i=1}^{n}(x - \alpha_i)$.

Definition 7.3.4.3. If F is a field, and $f \in F[x]$, an extension E/F will be called a *splitting field* of f, if (i) f splits completely in E and, if $\alpha_1, \ldots, \alpha_n$ are the roots of f in E, then $E = F(\alpha_1, \ldots, \alpha_n)$.

7.4 Lecture 25: Splitting fields

7.4.1 Existence of splitting fields

Theorem 7.4.1.1. *If F is a field, and $f \in F[x]$ is a polynomial of degree n, then there exists an algebraic extension E/F of degree $\leq n!$ such that, viewing $f \in E[x]$, E is a splitting field for f.*

Proof. We proceed by induction on the degree of f. The result is clearly true for polynomials of degree 1. Write f as a product of irreducible factors. If f is not itself irreducible, then the induction hypothesis shows that some irreducible factor of f has a root in some algebraic extension. Factoring out this root, we obtain a polynomial of lower degree in some algebraic extension of L and we conclude by induction.

If f is irreducible, then $(f) \in F[x]$ is prime and thus $L := F[x]/(f)$ is an extension field of F. Set α_1 to be the image of x in L. Since $f(x) = 0$ in $F[x]/(f)$, it follows that $f(\alpha_1) = 0$. In that case, $x - \alpha_1$ divides f in $L[x]$ by the lemma above, so we can write $f = (x - \alpha_1)f'$, where f' has degree smaller than that of f. Thus, viewing f' as an element of $L[x]$, we have obtained a polynomial of lower degree in $L[x]$ and we can repeat the procedure. Since an iterated algebraic extension is algebraic by Lemma 7.3.2.1, the result follows. □

7.4.2 Algebraically closed fields

Definition 7.4.2.1. An extension $\bar{F}/F$ is called *algebraically closed* if every non-constant polynomial in $F[x]$ splits completely in $\bar{F}$. An extension $\bar{F}/F$ is called an *algebraic closure* of F, if it is algebraic over F and algebraically closed.

Theorem 7.4.2.2. *Every field has an algebraic closure.*

Here is a "proof" ignoring set-theoretic issues. Consider the collection E of all extensions K of F such that K is algebraic over F; this collection is partially ordered with respect to inclusion. The argument we gave before for transitivity of algebraic extensions shows that a union of a chain of algebraic extensions is algebraic. Therefore, if E is a set, Zorn's lemma applies and we may take $\bar{F}$ to be a maximal element. This extension is algebraically closed by maximality and algebraic by construction. The set-theoretic issue that may arise is that there is no reason for E to be a set. To deal with that problem, we can simply replace the word "all" by an explicit count.

Proof. Let F be a field. Let S be a set such that 1) $F \subset S$, 2) $|S| > \max(\aleph_0, |F|) =: \mathcal{N}$. Let $\mathscr{R} = \{L \subset S | F \subset L \text{is algebraic}\}$. We introduce a partial order in $\mathscr{R}$ by setting $L_2 > L_1$ if $L_1 \subset L_2$ is an algebraic extension. Now, by transitivity of algebraicity, we conclude that any chain has a least upper bound and therefore Zorn's lemma implies $\mathscr{R}$ has a maximal element L_0; we will show L_0 is an algebraic closure of F. Indeed, assume to the contrary that there exists a non-constant polynomial $f \in L_0[x]$ that has no root in L_0. We know that there always exists an algebraic extension L' of L_0 in which f has a root (in fact, even one in which f splits completely). Since L' is an algebraic extension of F as well (again by transitivity of algebraicity), we see that $|L_0| \leq |L'| \leq \mathcal{N}$, hence $|S \setminus L_0| = |S| > |L' \setminus L_0|$. Thus, there exists an injection $i : L' \to S$ such that $i(x) = x$ for $x \in L_0$. Use i to equip $i(L')$ with the structure of a field. However, the existence of L' contradicts maximality of L_0 and so we are done. □

7.4.3 Uniqueness of splitting fields

Recall the definition of splitting fields from the last lecture.

Theorem 7.4.3.1 (Uniqueness of splitting fields)**.** *Let $\sigma : F \to F'$ be an isomorphism of fields. Suppose f is a polynomial (of positive degree) in $F[x]$, and $\sigma(f)$ is the corresponding polynomial in $F'[x]$. If E is a splitting field of f over F, and E' is a splitting field of $\sigma(f)$ over F', then σ extends to an isomorphism $\tilde{\sigma} : E \to E'$.*

Proof. We proceed by induction on the degree of f. If f has degree 1, then we can simply take $\tilde{\sigma} = \sigma$. Thus, assume that f has degree > 1. If f has irreducible factors that are all of degree 1, then we are again done. Thus, assume that f has an irreducible factor of degree > 1, call it g. Let α be a root of g in E. You can check that σg is again irreducible in F'. If β is a root of σg in E', then we can extend σ to an isomorphism $\tilde{\sigma} : F(\alpha) \overset{\sim}{\to} F'(\beta)$ by setting $\tilde{\sigma}(a + a'\alpha) = \sigma(a) + \sigma(a')\beta$. You can check that this formula defines an isomorphism of fields. The induction hypothesis now guarantees the required extension. □

7.4.4 More about roots

If F is a subfield of the complex numbers, then we know how to differentiate elements of $F[x]$. Of course, we can make this definition completely formal: the derivative is an F-linear map from $F[x] \to F[x]$. Since $F[x]$ has a basis consisting of the monomials x^i, it suffices to give a formula for these. The relationship between the product in the polynomial ring and derivative is summarized by the product rule. Therefore, we make the following definition.

Definition 7.4.4.1. If F is a field, and R is a commutative, unital F-algebra, a derivation $\delta : R \to R$ is an F-linear map such that $\delta(ab) = a\delta(b) + \delta(a)b$.

With this formal definition, we can establish a number of the "usual" properties.

Lemma 7.4.4.2. *If R is a commutative unital F-algebra, then the following properties hold.*

i) $\delta(1) = 0$,

ii) $\delta(r^i) = ir^{i-1}\delta(r)$.

Proof. For the first statement, observe that $1 = 1 \cdot 1$ and thus that $\delta(1) = \delta(1 \cdot 1) = 1 \cdot \delta(1) + \delta(1) \cdot 1 = \delta(1) + \delta(1)$. Therefore, $\delta(1) = 0$. The second statement is proven by induction. The statement is clearly true for $i = 1$. Assume inductively the statement holds for $i = n - 1$.

$$\begin{aligned}\delta(r^n) &= \delta(r \cdot r^{n-1}) = \delta(r) \cdot r^{n-1} + r \cdot \delta(r^{n-1}) \\ &= \delta(r) \cdot r^{n-1} + r \cdot (n-1)r^{n-2}\delta(r) \\ &= \delta(r) \cdot r^{n-1} + (n-1)r^{n-1}\delta(r) \\ &= nr^{n-1}\delta(r),\end{aligned}$$

which is precisely what we wanted to show. □

Lemma 7.4.4.3. *If F is a field, then setting $\delta(x) = 1$, there is a unique extension of δ to a derivation $\delta : F[x] \to F[x]$.*

Proof. Using F-linearity and the power rule, there is a unique extension of δ to an F-linear map $F[x] \to F[x]$. Given two polynomials $f(x)$ and $g(x)$, the fact that $\delta(fg) = f\delta(g) + \delta(f)g$ can then be proven by explicit computation. Indeed, write $f(x) = \sum_{i=0}^{m} a_i x^i$ and $g(x) = \sum_{j=0}^{n} b_j x^j$ and then just apply δ to both sides and compare. □

Remark 7.4.4.4. Observe that $\delta(f)$ always has degree $<$ the degree of f. In F has characteristic $p > 0$, then $\delta(x^p) = px^{p-1} = 0$. Thus, non-constant functions can have derivative zero, in contrast to the familiar results from elementary calculus. We can determine exactly when $\delta(x^i) = 0$. Indeed, this happens if and only if $i \equiv 0 \mod p$. Thus, if $\delta(f) = 0$, it follows that $f = \sum_i a_i x^{pi} = \sum_i a_i x^{pi}$, i.e., $f(x) = g(x^p)$.

7.5 Lecture 26: Finite fields

7.5.1 Derivations and splitting

Suppose $f \in F[x]$ is a product of linear factors $f = \prod_i (x-\alpha_i)^{a_i}$. Suppose some $a_i > 1$; by reindexing, we can assume that $a_1 > 1$. In that case, $f = (x-\alpha_1)^{a_1} g$ and it follows from the product rule that

$$\delta(f) = (x-\alpha_1)^{a_1}\delta(g) + a_1(x-\alpha_1)^{a_1-1} g = (x-\alpha_1)^{a_1-1}((x-\alpha_1)\delta(g) + a_1 g).$$

Therefore, if $a_1 > 1$, then f and $\delta(f)$ have a common factor, i.e., $(x-\alpha_1)^{a_1-1}$. In other words, if f has a repeated root, f and $\delta(f)$ have a common factor.

If f is not a product of linear factors, we can always pass to a splitting field E/F where f factors as a product of linear factors. Now, note that if f and g are two polynomials that are coprime in $E[x]$, then we can find polynomials $a(x)$ and $b(x)$ such that $af + bg = 1$. Since $F[x] \subset E[x]$, this relation holds in particular in $E[x]$ as well. In other words, if f and g are coprime in $E[x]$ they are coprime in $F[x]$. We can now formulate a converse to our observation.

Lemma 7.5.1.1. *If F is a field, the polynomial $f \in F[x]$ has a repeated root if and only if f and $\delta(f)$ have a non-trivial common factor.*

Proof. By the remark we just made, we can check whether f has a repeated root by passing to a splitting field of F, i.e., we can assume without loss of generality that f splits in F. In that case, we have already seen that if f has a repeated root, then f and $\delta(f)$ have a common factor. For the converse, by the remark we just made, we can assume that f splits over F. For the converse, assume that $f(x)$ has no repeated root. Since f splits in F, we can write $f = \prod_{i=1}^n (x-\alpha_i)$, and then

$$\delta(f) = \sum_{i=1}^n \frac{1}{x-\alpha_i} \prod (x-\alpha_i).$$

Now, it suffices to show that no root of $f(x)$ is a root of $\delta(f)$. To see this, simply evaluate $\delta(f)$ at α_j. In that case,

$$\delta(f)(\alpha_j) = \prod_{j \neq i} (\alpha_j - \alpha_i),$$

but since F is a field, the expression on the right is non-zero. Now, simply observe that if f and f' have a non-trivial common factor, they have a common root, i.e., any root of this common factor. □

7.5.2 Finite fields

We now begin to study finite fields. We know that any finite field contains a subfield isomorphic to $\mathbb{F}_p$ and by the discussion above, we are considering finite extensions of $\mathbb{F}_p$. We already know that such extensions have p^r elements for some r. We now show that, for any integer $r \geq 1$, there exists a finite field of order p^r. The basic idea is to build these fields as splitting fields. We will build extensions as quotients of $\mathbb{F}_p[t]$, and to this end we need to construct irreducible polynomials of various degrees.

Example 7.5.2.1. Consider the polynomial x^2+1 in $\mathbb{F}_p$. When $p = 2$, this polynomial is reducible. However, when $p = 3$, it is straightforward to show that $\mathbb{F}_p$ is reducible (indeed, simply plug in $x = 1$ and $x = -1$). When $p = 5$, note that $3^2 = 9$ is congruent to -1 mod 5. Therefore, x^2+1 is not always irreducible mod p. In fact, it is irreducible if and only if $p \equiv 3 \mod 4$.

Lemma 7.5.2.2. *If F is a finite field of order q, then $a^q = a$.*

Proof. Since F is a field, $F \setminus 0$ is an abelian group, which in our case necessarily has order $q-1$. It follows from Lagrange's theorem that $a^{q-1} = 1$ for every non-zero element. Thus, $a^q = a$. However, this equation is satisfied for $a = 0$ as well. □

Proposition 7.5.2.3. *For any integer $r \geq 1$, there exists a finite field of order p^r.*

Proof. Consider the splitting field K of $x^{p^r} - x$. In K, let $F = \{a \in K | a^{p^r} = a\}$. By construction, the elements of F are the roots of $x^{p^r} - x$. First, let us show that all these roots are distinct; equivalently, we want to show that $x^{p^r} - x$ has no repeated roots. To see this, we can compute the derivative of $x^{p^r} - x$ and see whether it has a common factor with $x^{p^r} - x$. Now, we compute:

$$\delta(x^{p^r} - x) = \delta(x^{p^r}) - \delta(x) = -1.$$

Now, simply observe that -1 and $x^{p^r} - x$ have no common factor. Since $x^{p^r} - x$ has degree p^r, it has at most p^r roots. We have just seen that it has exactly p^r roots.

It remains to check that the roots actually form a field. Indeed, suppose $a, b \in F$. Then $a^{p^r} = a$ and $b^{p^r} = b$. Thus, $(ab)^{p^r} = ab$, i.e., $ab \in F$. Also, $(a \pm b)^{p^r} = a^{p^r} \pm b^{p^r} = a \pm b$. Hence F is a subfield. □

Now, we analyze the question of how many finite fields with p^r elements there are.

Proposition 7.5.2.4. *If a finite field F has p^r elements, then the polynomial $x^{p^r} - x$ factors in $F[x]$ as a product of linear factors. Moreover, any finite field of p^r elements is the splitting field of $x^{p^r} - x$. Thus, if a finite field with p^r elements exists, it is unique up to isomorphism.*

Proof. In a finite field F with p^r elements, we know that $a^{p^r} = a$ for every $a \in F$ by the lemma above. Thus, the elements of F are all roots of the polynomial $x^{p^r} - x$. Again, since $x^{p^r} - x$ has degree p^r, it has at most p^r-roots in an extension field. Thus, $x^{p^r} - x$ has exactly p^r roots in F and therefore splits completely in F. This polynomial cannot split in a smaller field since any smaller field would have p^m elements with $m < r$. Thus, the field F consists of precisely the roots of F and it follows that F is a splitting field for $x^{p^r} - x$. □

7.5.3 The multiplicative group of a finite field

We already saw that the group of automorphisms of $\mathbb{Z}/p\mathbb{Z}$ is cyclic of order $p-1$. In fact, every such automorphism is a ring automorphism, and therefore the group of units of a finite field of order p is cyclic of order $p-1$. We can analyze some other examples.

Example 7.5.3.1. Consider $F = \mathbb{F}_3[x]/(x^2+1)$. As a set, this has 9 elements, and there are 8 non-zero elements. The powers of the element x are $x, x^2 = -1 = 2$, $x^3 = 2x$, $x^4 = 2x^2 = -2 = 1$. On the other hand, the powers of $x+1$, are $x+1$, $(x+1)^2 = x^2+2x+1 = 2x$, $(x+1)^3 = 2x(x+1) = 2x^2+2x = -2+2x = 2x+1$, $(x+1)^4 = (2x+1)(x+1) = 2x^2+3x+1 = 2x^2+1 = x^2 = 2$, $(x+1)^5 = 2x+2$, $(x+1)^6 = (2x+2)(x+1) = 2(x+1)^2 = 4x = x$, $(x+1)^7 = x(x+1) = x^2+x = x+2$, and finally $(x+1)^8 = (x+2)(x+1) = x^2+3x+2 = x^2+2 = 1$. Thus, $F \setminus 0$, which is an abelian group, is necessarily cyclic. You can do a few more examples like this to convince yourself of the following fact.

Theorem 7.5.3.2. *If F is a finite field, then $F \setminus 0$ is cyclic.*

Proof. Let N be the largest order of an element of $F \setminus 0$. Since $F \setminus 0$ is a finite *abelian* group, all orders of elements divide N. In other words, every $a \in F \setminus 0$ satisfies $a^N = 1$, i.e., all elements of $F^\times$ are roots of $x^N - 1$.

Let $q = |F|$. The number of roots of a polynomial over a field is at most the degree of the polynomial, and $x^N - 1$ has $q-1$ roots in F so $q - 1 \leq N$. Since N is the order of an element in $F^\times$, it follows from

Lagrange's theorem that $N|(q-1)$, i.e., $N \leq q-1$. Thus, $N = q-1$, so there are elements of $F^\times$ of order $q-1$, which means $F^\times$ is cyclic. □

Corollary 7.5.3.3. *Every finite field is generated as an extension over $\mathbb{F}_p$ by a single element.*

Proof. By Theorem 7.5.3.2, $F \setminus 0$ is cyclic and a choice of a cyclic generator x of $F \setminus 0$ gives an element has the required property. □

Chapter 8

Separable extensions

8.1 Lecture 27: The primitive element theorem and separability

8.1.1 Simple extensions and the primitive element theorem

Example 8.1.1.1. Consider the extensions $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. You can show that $x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})$ and likewise that $x^2 - 2$ is irreducible in $\mathbb{Q}(\sqrt{3})$. Consider the splitting field of $x^2 - 2$ in $\mathbb{Q}(\sqrt{3})$; this is an extension of $\mathbb{Q}(\sqrt{3})$ and can be described as $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. On the other hand, consider the element $\sqrt{2} + \sqrt{3}$, which lies in this extension.

We claim that this element generates the whole extension. Indeed, if $a = \sqrt{2}+\sqrt{3}$, then $(a-\sqrt{2})^2 = 3$. Multiplying out gives $a^2 - 2a\sqrt{2} + 2 = 3$ and rearranging, we see that $\sqrt{2} = \frac{1}{2a}(a^2 - 1)$. Likewise, $\sqrt{3} = \frac{1}{2a}(a^2 + 1)$. Said differently, we have just shown that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. In other words, the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is, in fact, simple.

In fact, we have considerable flexibility in choosing an element a that generates $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. For example, if γ is a rational number, then consider $a = \sqrt{2} + \gamma\sqrt{3}$. In that case, $(a - \sqrt{2})^2 = 3\gamma^2$, so $a^2 - 2a\sqrt{2} + 2 = 3\gamma^2$, i.e., $\sqrt{2} = \frac{1}{2a}(a^2 - 3\gamma^2 + 2)$. Similarly, $(a - \gamma\sqrt{3})^2 = 2$, so $a^2 - 2a\gamma\sqrt{3} + 3\gamma^2 = 2$. Thus, if $\gamma \neq 0$, then $\sqrt{3} = \frac{a^2+3\gamma^2-2}{2a\gamma}$. Loosely speaking *almost all* linear combinations of $\sqrt{2}$ and $\sqrt{3}$ will generate $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

Lemma 8.1.1.2. *If F is a field that has characteristic 0, then an irreducible polynomial has no repeated roots in any extension E/F.*

Proof. By Lemma 7.5.1.1, f has a repeated root in an extension E/F, if and only if f and $\delta(f)$ have a common factor. Since f is irreducible, $f|\delta(f)$. However, $\delta(f)$ has degree smaller than f, and therefore f has a repeated root if and only if $\delta(f) = 0$. Since F has characteristic 0, this means $f = 0$. □

Proposition 8.1.1.3. *If F is a field having characteristic 0, and if a and b are algebraic over F, then there exists an element $c \in F(a, b)$ such that $F(c) = F(a, b)$.*

This result is the key step in establishing the following more general result.

Theorem 8.1.1.4 (Primitive element theorem I)**.** *If F is a field having characteristic 0, and E/F is a finite extension, then E is a simple extension.*

Proof. Since E is finite, it is generated by finitely many elements algebraic over F. The result then follows from induction using Proposition 8.1.1.3. □

Proof of Proposition 8.1.1.3. Assume $f(x)$ and $g(x)$ are the minimal polynomials of a and b and assume they have degrees m and n respectively. In Example 8.1.1.1, the polynomials in question split in $F(a,b)$, but this need not happen in general. As in Example 8.1.1.1, we would like to show that a suitable F-linear combination of a and b provides a simple generator for $F(a,b)$. In that case, there were certain degenerate linear combinations that we needed to avoid ($\gamma = 0$ in that example). Let $c = a + \gamma b$. By definition $F(c) \subset F(a,b)$, and we will show that $F(a,b) \subset F(c)$ for most values of γ. To see this, it suffices to show that $b \in F(c)$, since then $a = c - \gamma b$ is also in $F(c)$. To show that $b \in F(c)$ is equivalent to showing that b satisfies a linear polynomial in $F(c)$. Thus, we want to show that the minimal polynomial of b over $F(c)$ cannot have degree ≥ 2.

Thus, let L be some extension of F in which both $f(x)$ and $g(x)$ split completely. Since F has characteristic 0, it follows from Lemma 8.1.1.2 that neither f nor g has multiple roots in an extension field. Write $\alpha_1, \ldots, \alpha_m$ for the distinct roots of $f(x)$ and $\beta_1, \ldots, \beta_n$ for the distinct roots of g in L. Set $a = \alpha_1$ and $b = \beta_1$.

We want to analyze the minimal polynomial of b over $F(c)$, let us first write down some polynomial over $F(c)$ that b satisfies: since $c = a + \gamma b$, and a satisfies f, then b satisfies $h(x) := f(c - \gamma x)$, which is an element of $F(c)[x]$. Since b satisfies g by definition, it follows that the minimal polynomial of b over $F(c)$ necessarily divides both h and g. Thus, we will be done if we show that the greatest common divisor of h and g cannot have degree ≥ 2.

Suppose that the greatest common divisor of h and g does have degree ≥ 2. In that case, since g has no repeated roots, it follows that h and g have a common root $b' \neq b$. Then, $h(b') = 0$ means $f(c - \gamma b') = 0$, i.e., $c - \gamma b' = \alpha_i$ for some root α_i of f. Since $c = a + \gamma b$, this is equivalent to $(a + \gamma b) - \gamma b' = \alpha_i$, or

$$\gamma = \frac{\alpha_i - a}{b - b'}.$$

Thus, as long as we can choose γ to lie outside of the finite set of values $\frac{\alpha_i - a}{b - \beta_j}$, $j \neq 1$, the greatest common divisor of h and g has degree 1. Since F was assume to have characteristic 0, it contains $\mathbb{Q}$ and is thus infinite. In other words, we may always pick γ outside of the finite set of values just listed, and we're done. □

8.1.2 Separability

Proposition 8.1.2.1. *If F is a field, and $f \in F[x]$ is an irreducible polynomial, then*

i) if F has characteristic 0, f has no multiple roots;

ii) if F has characteristic $p > 0$, $f(x)$ has a multiple root if and only if $f(x) = g(x^p)$.

Proof. Since f is irreducible, its only factors in $F[x]$ are 1 and $f(x)$. If f has a multiple root, then f and $\delta(f)$ have a non-trivial common factor by the lemma, hence, again since f is irreducible, $f(x)|f'(x)$. Since the degree of $\delta(f)$ is smaller than the degree of f, the only way this can happen is if $f'(x) = 0$. If F has characteristic zero, this implies $\delta(f)$ is a constant, which means it has no roots. Likewise, in positive characteristic, $\delta(f) = 0$ implies that $f(x) = g(x^p)$ (by the remark above. □

The following example shows that irreducible polynomials can have repeated roots over fields having positive characteristic.

Example 8.1.2.2. Suppose F is a field having characteristic 2 and consider the rational function field $F(t)$. Consider the polynomial $x^2 - t$ in $F(t)[x]$. We claim this polynomial is irreducible. The argument is essentially the standard argument showing that $\sqrt{2}$ is not a rational number. Suppose $x^2 - t$ has a solution in $F(t)$, i.e., there exists a rational function $\frac{p(t)}{q(t)}$ whose square is t. If $\deg p(t) \leq \deg q(t)$, then

$\deg p^2(t) \leq degq^2(t)$. Note that $degtq^2(t) = degq^2(t) + 1$, and therefore, $\deg p^2(t) < degtq^2(t)$, i.e., we cannot have an equality. Therefore without loss of generality, we can assume that $\deg p(t) > \deg q(t)$. In that case, by long division, we can write $p(t) = a(t)q(t) + r(t)$ with $\deg r(t) < \deg q(t)$. Then, $p^2(t) = a^2(t)q^2(t) + 2a(t)q(t)r(t) + r^2(t)$. Suppose we had an equality $p^2(t) = tq^2(t)$. Re-arranging terms, we see that

$$(-a^2(t) + t)q^2(t) = r(t)(a(t)q(t) + r(t)).$$

Since the left hand is divisible by $q^2(t)$, the right hand side must be also. However, the right hand side is not divisible by $q(t)$.

Anyway, since this polynomial is irreducible, we can compute its derivative: $\delta(x^2 - t) = 2x = 0$. Therefore, this polynomial has a multiple root. On the other hand, it is evident that this polynomial is of the form $g(x^2)$ with $g(x) = x - t$. You can check that $x^p - t$ behaves in a similar fashion for any $p > 0$.

Definition 8.1.2.3. If F is a field, a polynomial $f \in F[x]$ is called *separable* over F if f has no repeated roots in a splitting field. If E/F is an extension, an element $a \in E$ is called *separable* over F if it satisfies a separable polynomial over F. An extension E/F is called *separable* if every element $a \in E$ is separable over F and *inseparable* otherwise. A field F is called *perfect* if all finite extensions of F are separable.

Remark 8.1.2.4. Lemma 8.1.2.1 gives a criterion by which to check whether a given irreducible polynomial is separable. Example 8.1.2.2 gives an example of an inseparable extension of $\mathbb{F}_2(t)$.

8.2 Lecture 28: Separability

Last time we introduce the notion of a separable extension: this was one where every element satisfied a separable polynomial. Today, we analyze this notion in greater detail.

8.2.1 Examples

Proposition 8.2.1.1. *If F is a field having characteristic 0, then any finite extension E/F is separable, i.e., fields having characteristic 0 are perfect.*

Proof. Suppose E/F is an extension. In that case, E is generated by finitely many elements algebraic over F. Given any such element, since F has characteristic 0 its minimal polynomial is a polynomial with no multiple roots. □

In positive characteristic, recall that an irreducible polynomial has multiple roots if and only if it is of the form $g(x^p)$.

Theorem 8.2.1.2. *A field K having characteristic $p > 0$ is perfect if and only if $K^p = K$, i.e., the p-th power map is an isomorphism.*

Proposition 8.2.1.3. *Finite fields are perfect.*

Proof. We first check this for $\mathbb{F}_p$. In this case, every finite extension is a splitting field of $x^{p^r} - x$ for some $r > 1$. The polynomial $x^{p^r} - x$ is separable since its derivative is -1. Now, if we start with $\mathbb{F}_q$ for some $q = p^m$, let F be a finite extension of $\mathbb{F}_q$. Since F is a vector space over $\mathbb{F}_q$, it follows that F has order q^r for some integer r. Since $q^r = p^{mr} = p^{mr}$, every element of F satisifes $x^{q^r} - x$. Again, this polynomial is separable. □

8.2.2 Separability in general

In our proof of the primitive element theorem in characteristic 0, the inductive step in the argument used the fact that a finite extension E/F was necessarily generated by finitely many elements algebraic over the base field. In characteristic 0, any irreducible polynomial is separable, so we conclude that E/F is necessarily generated by finitely many elements that are *separable* over the base field. For fields having positive characteristic, this is no longer true: we already saw examples of finite extensions that are not separable. Nevertheless, finite separable extensions are still finite extensions, and are therefore generated by finitely many algebraic elements. It is natural to ask whether we can choose those elements to actually be separable. Before doing this, we need some tools to measure separability.

If E/F is a finite extension, then since E is an F-vector space, we could consider $\dim_F E$, which we called the degree of an extension. Assume we are in the special case where E/F is a simple extension, obtained by adjoining some element α. In that case, the degree of the extension coincided with the degree of the minimal polynomial of α. In general, the minimal polynomial of α will not be separable, and therefore, it is natural to measure how far this extension deviates from separability. Since α is separable if and only if its degree is equal to the number of distinct roots, we can simply count the number of distinct roots. Here is a more precise definition.

Definition 8.2.2.1. If E/F is an extension, and $\alpha \in E$ is algebraic over F, then we set $deg_F(\alpha) = deg\mu_{\alpha,F}(t)$ (the minimal polynomial of α over F). We define the *separable degree of* α, denoted $sdeg(\alpha)$ to be the number of distinct roots of $\mu_{\alpha,F}(t)$ in some algebraic closure.

Remark 8.2.2.2. The separable degree does not depend on the choice of an algebraic closure. By construction, we have $sdeg(\alpha) \leq deg(\alpha)$ with equality if and only if the minimal polynomial of α is separable.

Lemma 8.2.2.3. *If $f \in F[x]$ is separable, and $F \subset E$ then any factor of f in E is also separable. An element in an extension of E that is separable over F is also separable over E.*

Proof. We know that a polynomial is separable if and only if it has no common factor with its derivative. Since f is separable, we conclude that f and f' are coprime. Therefore, we can find $u, v \in F[x]$ such that $fu + f'v = 1$. Now, suppose $g(x)$ is a factor of $f(x)$ in E, i.e., $f = gh$ in $E[x]$. In that case, combining these two facts, we see that $f' = gh' + g'h$ by the product rule and therefore

$$\begin{aligned} 1 &= fu + f'v \\ &= ghu + (gh' + g'h)v \\ &= g(hu + h'v) + g'(hv). \end{aligned}$$

Thus, g and g' are coprime.

Now, suppose α lies in an extension of E and it is separable over F. Since its minimal polynomial in $E[x]$ divides the minimal polynomial in $F[x]$, separability over E implies separability over F by the fact we just established. □

Lemma 8.2.2.4. *Let E and F be fields. If $\sigma : F \to E$ is a field embedding, then a polynomial $f \in F[x]$ is separable if and only if $\sigma f \in E[x]$ is separable.*

Proof. If f is separable, we can find u and v such that $fu + f'v = 1$. Applying σ to the coefficients yields a ring embedding $F[x] \to E[x]$ and $\sigma(f') = \sigma(f)'$. Therefore,

$$(\sigma f)(\sigma u) + (\sigma f')(\sigma v) = 1,$$

which shows that σf and $\sigma f'$ are coprime.

Now, assume that f is inseparable. In that case, there is a non-constant polynomial d such that $d|f$ and $d|f'$. Then σd is non-constant as well and divides σf and $\sigma f'$, so σf and $\sigma f'$ are not coprime, i.e., σf is inseparable. □

We would like to better understand the separable degree and to do this, we will establish a relationship between separable degree and embeddings into an algebraic closure. Here is an example of what we mean.

Example 8.2.2.5. Consider the field $E = \mathbb{Q}(\sqrt{2})$. There are 2 embeddings of E in in $\mathbb{R}$. Indeed, we fix the embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$, and we would like to extend this map to a homomorphism $\mathbb{Q}(\sqrt{2}) \to \mathbb{R}$. Such a homomorphism is uniquely determined by where it sends $\sqrt{2}$. The obvious choice is to send $\sqrt{2}$ to $\sqrt{2}$ in $\mathbb{R}$. However, sending $\sqrt{2}$ to $-\sqrt{2}$ is also a homomorphism. Indeed, this sends $a + b\sqrt{2}$ to $a - b\sqrt{2}$, and the map $a + b\sqrt{2} \to a - b\sqrt{2}$ is invertible over $\mathbb{Q}$.

Example 8.2.2.6. The field $E = \mathbb{Q}(2^{\frac{1}{3}})$. Since $x^3 - 2$ has 1 real root, there is a single embedding of E in $\mathbb{R}$. However there are 3 distinct embeddings of E in $\mathbb{C}$ corresponding to sending $2^{\frac{1}{3}}$ to any of the 3 cube roots of 2 in $\mathbb{C}$.

8.3 Lecture 29: Separability, embeddings and the primitive element theorem

8.3.1 Separability and embeddings

We can abstract the ideas involved in the previous example.

Claim 8.3.1.1. *Suppose E/F is an extension and $\alpha \in E$ is an element algebraic over F. If $\sigma : F \to L$ is a fixed embedding, then the number of homomorphisms $\tau : F(\alpha) \to L$ extending σ is the number of roots in L of the image of the minimal polynomial $\sigma(\mu_\alpha)$.*

Proof. By induction on the number of generators, it suffices to establish the result for $E = F(\alpha)$. In that case, observe that any element of $F(\alpha)$ may be represented (non-uniquely) as $p(\alpha)$ for some polynomial p with coefficients in F. Thus, such an embedding is uniquely determined by where it sends α. We claim that sending α to a root of $\sigma(\mu_\alpha)$ actually defines a field embedding. More precisely, given any element of $F(\alpha)$, represent it by $p(\alpha)$ for a suitable polynomial p (with coefficients in F). Let β be a root of $\sigma(\mu_\alpha)$ in L. Consider the formula

$$\tau(p(\alpha)) = \sigma(p)(\beta).$$

As long as this construction is well-defined it yields a field homomorphism. If $\tilde{p}$ is another representing polynomial of the given element, then since $\tilde{p}(\alpha) = p(\alpha)$, we conclude that α is a root of $\tilde{p} - p$. However, in that case, μ_α also divides $\tilde{p} - p$. Therefore, $\sigma(\mu_\alpha)|\sigma(\tilde{p} - \sigma(p))$ and thus $\sigma(\tilde{p})$ and $\sigma(p)$ take the same value on β. Of course, the two extensions have the same restriction to F by construction. □

Proposition 8.3.1.2. *Assume E/F is a degree n extension of fields, and suppose $\sigma : F \to L$ is a field embedding.*

i) The number of extensions of σ to an embedding $E \to L$ is at most n.
ii) If E/F is inseparable, then the number of extensions of σ to an embedding $E \to L$ is strictly smaller than n.
iii) If E/F is separable, then there is an extension L'/L such that number of extensions of σ to an embedding $E \to L'$ is exactly n.

Proof. We will argue by induction on the degree of the extension E/F. If $n = 1$, then $E = F$ and there is nothing to check. Therefore, suppose $n > 1$. In that case, we can pick $\alpha \in E$ with $\alpha \notin F$. We then have the tower of extensions $F \subset F(\alpha) \subset E$. Now, we want to bound the number of extensions of $\sigma : F \to L$ to an embedding $E \to L$. To do this, we first bound the number of extensions of σ to an embedding $\tau : F(\alpha) \to L$ and then bound the number of extensions of τ to an embedding $E \to L$.

The number of roots of the minimal polynomial is at most the degree of the extension $[F(\alpha) : F]$, but this inequality can be strict for two reasons: (i) the polynomial $\sigma(\mu_\alpha)$ might not split in $L[x]$, or (ii) it might split and be inseparable. Once we have extended σ to some τ on $F(\alpha)$, we can then try to count how many ways τ extends to an embedding of E in L. To do this, we can consider $F(\alpha)$ as the new base field. Since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, we see that $[E : F(\alpha)] < [E : F]$ and therefore the induction hypothesis guarantees that the number of extensions of $\tau : F(\alpha) \to L$ to an embedding of E in F is at most $[E : F(\alpha)]$. Combining these observations establishes part (i). For part (ii), we go back through the proof above a little more carefully. When E/F is inseparable, some $\alpha \in L$ is inseparable over F. Now if α is inseparable that means that every polynomial it satisfies has repeated roots. In particular, the minimal polynomial of α has repeated roots. Repeating the proof of (i) with this α, we see that the minimal polynomial of α has strictly fewer than $[F(\alpha) : F]$ distinct roots. The equality $[E : F(\alpha)][F(\alpha) : F] = [E : F]$ again yields the required inequality.

Finally, we treat (iii), i.e., assume that E/F is a finite separable extension. In that case, we can write $E = F(\alpha_1, \ldots, \alpha_r)$ for suitable elements $\alpha_1, \ldots, \alpha_r \in E$, each of which is separable over F. We want to construct a field L'/L such that $\sigma : F \to L$ has exactly $[E : F]$ extensions to an embedding $E \to L'$. The argument is, again, similar to that in part (i).

Let μ_{α_i} be the minimal polynomial of α_i in $F[x]$, so each μ_{α_i} is a separable polynomial. Take L'/L to be an extension in which each $\sigma(\mu_{\alpha_i}) \in L[x]$ splits. We will show that there are $[E : F]$ extensions of σ to an embedding of E into L'. If $[E : F] = 1$, then there is nothing to show, so we assume that $E \neq F$.

Since α_i is not in F for some i, by reordering if necessary, we may assume that $\alpha_1 \notin F$. The number of extensions of σ to an embedding $F(\alpha_1) \to L'$ is the number of roots of $\sigma\mu_{\alpha_1}$ in L'. Since the polynomial $\sigma\mu_{\alpha_1}$ is separable and splits, there are precisely $[F(\alpha_1) : F]$ extensions of σ to an embedding by the claim above. If $E = F(\alpha_1)$, we are done, so suppose that $E \neq F(\alpha_1)$.

Write $E = F(\alpha_1)(\alpha_2, \ldots, \alpha_r)$ and fix an embedding $\tau : F(\alpha_1) \to L'$ extending σ (there are precisely $deg(\alpha_1)$ such extensions). For $i = 2, \ldots, r$, let μ_i be the minimal polynomial of α_i in $F(\alpha_1)[x]$. Observe that $\mu_i | \mu_{\alpha_i}$ and therefore $\tau(\mu_i)$ divides $\tau(\mu_{\alpha_i}) = \sigma(\mu_{\alpha_i})$ (this uses the fact that μ_{α_i} has coefficients in F). Since $\sigma(\mu_{\alpha_i})$ is separable and splits in L', the same is true for the factor $\tau(\mu_i)$.

Thus, $E/F(\alpha_1)$ and the embedding $\tau : F(\alpha_1) \to L'$ have similar properties to E/F and the embedding σ: the extension has field generators α_i that are separable over $F(\alpha_1)$ and each $\tau(\mu_i)$ splits in $L'[x]$. However, since $[E : F(\alpha_1)] < [E : F]$, we can apply the induction hypothesis to conclude that there are precisely $[E : F(\alpha_1)]$ ways to extend τ to an embedding $E \to L'$. Thus, by the product formula, we can complete the proof. □

8.3.2 The primitive element theorem in general

Theorem 8.3.2.1. *An finite extension E/F is separable if and only if we can find finitely many elements $\alpha_1, \ldots, \alpha_n \in E$ that are* separable over F *such that $E = F(\alpha_1, \ldots, \alpha_n)$.*

Proof. One direction here is immediate: if E/F is separable, then any generating set will consist of separable elements. For the converse, we essentially appeal to the proof of the preceding result. Suppose $E = F(\alpha_1, \ldots, \alpha_r)/F$ is a finite extension generated by elements $\alpha_1, \ldots, \alpha_r$ that are separable over F. Take $\sigma = id_F$. In the proof of the preceding result, the set of field generators we chose was never changed. So the proof applies in this context to show that E admits $[E : F]$ embeddings into some field extension of F. This property is not true for any inseparable extension, so E/F must be separable. □

Theorem 8.3.2.2 (Primitive element theorem II). *If E/F is a finite separable extension, then E has a primitive element.*

Proof. Since we already established the result in the case where F is finite, we can assume that F is infinite. In that case, the proof we gave in characteristic 0 goes through verbatim. □

8.4 Lecture 30: Separability and embeddings

8.4.1 Further results on separability

Corollary 8.4.1.1. *If $f \in F[x]$ is separable, then a splitting field for f over F is separable over K.*

Proof. Let E/F be a splitting field for f. In that case $L = F(\gamma_1, \dots, \gamma_n)$ where the γ_i's are all roots of f. Therefore, the γ_i are all separable over F, so E is separable as well. □

Corollary 8.4.1.2. *If the finite extension E/F contains intermediate fields E_1 and E_2 that are both separable over F, then their composite E_1E_2 (i.e., the intersection of all subfields containing E_1 and E_2) is also separable over K. In particular, the set of elements that are separable over F forms a subfield of E.*

Proof. By the primitive element theorem, we can write $E_1 = F(\gamma_1)$ and $E_2 = F(\gamma_2)$. In that case, $E_1E_2 = F(\gamma_1, \gamma_2)$, which is separable over F. If α and β are separable over F, then we can take $E_1 = F(\alpha_1)$ and $E_2 = F(\alpha_2)$ to see that $F(\alpha, \beta)$ is separable over F; this extension contains $\alpha \pm \beta$, $\alpha\beta$ and $\frac{1}{\alpha}$ if $\alpha \neq 0$, so separability is preserved under field operations. □

Definition 8.4.1.3. If E/F is a field extension, we write F^{sep} for the subfield of E consisting of elements that are separable over F; this field is called the separable closure of F in E.

Theorem 8.4.1.4 (Transitivity of separability). *If $L/E/F$ is a tower of finite extensions, then L/F is separable if and only if L/E and E/F are separable.*

Proof. If L/F is separable, then every element is separable over F and therefore also over E. Similarly, E/F is separable.

In the other direction, we can again count field embeddings. Write $L = E(\beta)$ and $E = F(\alpha)$ with $m = [L : E]$ and $n = [E : F]$. Let K be a splitting field over F for the minimal polynomial of $\alpha \in F[x]$. Since α is separable over F with degree n, there are n embeddings $\tau_i : E \to K$ that fix F. Likewise, the minimal polynomial of β is separable over E, so its image under τ_i in $K[x]$ is separable. Let K' be an extension of K over which all these polynomials split completely. These polynomials each have m roots in K', so each τ_i has m extensions to an embedding $L \to K'$ that extend $F \to K'$. Thus, the number of extensions is mn, which is precisely $[L : F]$, which means L/F is separable. □

8.4.2 Intermediate fields and automorphisms

If $F \subset K$ is a field extension, then recall that we defined $Aut_F(K)$ to be the group of field automorphisms of K that fix F. Thus, we may attach groups to field extensions. We now analyze this construction in more detail. Suppose first that we have a tower of field extensions $F \subset K \subset L$ is a tower of field extensions. In that case, we may consider the three groups $Aut_F(K)$, $Aut_F(L)$ and $Aut_K(L)$. We will use our results about extending embeddings to analyze the relationships between these groups.

First, observe that since $F \subset K$, any automorphism of L that fixes K necessarily fixes F as well. In other words, $Aut_K(L) \subset Aut_F(L)$. In words, we may characterize the subgroup $Aut_K(L)$ as follows:

$$Aut_K(L) = \{\sigma \in Aut_F(L) | \sigma(\alpha) = \alpha \forall \alpha \in K\}.$$

On the other hand, given any subgroup of $H \subset Aut_F(L)$, we may define

$$L^H := \{\alpha \in L | \sigma(\alpha) = \alpha \forall \sigma \in H\}.$$

It is straightforward to check that L^H is actually a field; we record this observation here.

Lemma 8.4.2.1. *If L is a field, and $H \subset Aut_F(L)$, then L^H is a field. If $H \subset H' \subset Aut_F(L)$, then $L^{H'} \subset L^H$ is an inclusion of fields.*

The set of subgroups of $Aut_F(L)$ forms a partially ordered set under inclusion. This partially ordered set has both initial element the trivial subgroup and final element $Aut_F(L)$. The fixed subgroup of the trivial subgroup is L itself, while the fixed subgroup of $Aut_F(L)$ is F. The collection of subfields of L that contain F also forms a partially ordered set under inclusion. By means of the lemma above, we may define a function from the poset of subgroups of $Aut_F(L)$ to the subfields of L that contain F by sending $H \subset Aut_F(L)$ to $L^H \subset L$. Observe that this bijection reverses order in each poset.

Sending a subfield K of L containing F to the group $Aut_K(L)$ defines a function from the set of subfields of L that contain F to the set of subgroups of $Aut_F(L)$. Once again, the discussion above shows that this function reverses orders. Thus, we have linked the subgroup structure of $Aut_F(L)$ and the structure of intermediate extensions of $F \subset L$.

To make this relationship tighter, we make the following observations. If we send $F \subset K \subset L$ to $Aut_K(L)$ and then consider $L^{Aut_K(L)}$ it follows from the definitions that $K \subset L^{Aut_K(L)}$. Likewise, if $H \subset Aut_F(L)$, then we can form $L^H \subset L$, and then consider $Aut_{L^H}(L)$. Again, it is immediate from the definitions that $H \subset Aut_{L^H}(L)$. The natural question is: can we characterize those situations when the inclusions that occur here are equalities. Before doing that, let us observe that, in general, the two inclusions just mentioned *are not* equalities.

Example 8.4.2.2 ("Not enough roots"). Consider the extension field $E = \mathbb{Q}[2^{\frac{1}{3}}]$ of $\mathbb{Q}$, where $2^{1/3}$ is a real cube root of 2. We claim that $Aut_{\mathbb{Q}}(E)$ is trivial. The extension $E/\mathbb{Q}$ has prime degree so the only subfield of E that contains $\mathbb{Q}$ is necessarily E itself. Suppose we want to build an automorphism of $E \to E$ extending the given embedding $\mathbb{Q} \to E$. Since E is simple, generated by $2^{1/3}$, any such extension is given by sending $2^{1/3}$ to a root of $x^3 - 2$ in E, i.e., any such extension must fix $2^{1/3}$. Thus, any automorphism of E over $\mathbb{Q}$ is trivial.

Example 8.4.2.3 (Inseparability). We observed that $x^2 - t$ was irreducible over $F = \mathbb{F}_2(t)$ and was an inseparable polynomial. More precisely, in a splitting field E of $x^2 - t$, it has precisely 1 root since $x^2 - t = (x - \sqrt{t})^2$ in E. We claim that $Aut_F(E) = 1$. As before, any extension of the embedding $F \to E$ to an embedding $E \to E$ necessarily fixes $\sqrt{t}$ (as the only root of $x^2 - t$ in E. Thus, any automorphism of E over F is trivial.

8.4.3 Automorphism groups of (finite separable) extensions

Definition 8.4.3.1. The roots of an irreducible polynomial in $F[x]$ are called F-conjugates.

Example 8.4.3.2. The roots of $\pm\sqrt{2}$ are $\mathbb{Q}$-conjugate, since they are roots of $x^2 - 2$. These two numbers are *not* $\mathbb{R}$-conjugate since $\sqrt{2}$ has minimal polynomial $x - \sqrt{2}$ over $\mathbb{R}$, while $-\sqrt{2}$ has minimal polynomial $x + \sqrt{2}$ over $\mathbb{R}$.

Example 8.4.3.3. In $\mathbb{C}$, the numbers $\pm i$ are $\mathbb{R}$-conjugate; more generally, $a+bi$ and $a-bi$ are $\mathbb{R}$-conjugate.

Theorem 8.4.3.4. *If E/F is an extension, $f \in F[x]$, and $\sigma \in Aut_F(E)$, then $\sigma(f(\alpha)) = f(\sigma(\alpha))$ for all $\alpha \in E$. In particular, an F-automorphism of E permutes the roots of $f(x)$ in E.*

Proof. Write $f(x) = \sum_i c_i x^i$, with $c_i \in F$. Then $\sigma(c_i) = c_i$, so it follows that $\sigma(f(x)) = f(\sigma(x))$. Thus, if $f(\alpha) = 0$, it follows that $\sigma(f(\alpha)) = f(\sigma(\alpha)) = 0$, i.e., $\sigma(\alpha)$ is a root of f. □

Corollary 8.4.3.5. *The group $Aut_F(E)$ permutes the F-conjugates in E.*

Proposition 8.4.3.6. *If E/F is a finite extension, the group $Aut_F(E)$ is finite.*

Proof. Write $E = F(\alpha_1, \ldots, \alpha_r)$. Any $\sigma \in Aut_F(E)$ is determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_r)$, and $\sigma(\alpha_i)$ is restricted to lie among the finitely many E-conjugates of α_i. □

Chapter 9

Galois extension and the Galois correspondence

9.1 Lecture 31: Separability and Galois extensions

Proposition 9.1.0.7. *If E/F is the splitting field of a separable polynomial, then $Aut_F(E)$ has order $[E : F]$.*

Proof. As f is separable it has distinct roots in a splitting field. We saw above that there are $[E : F]$ distinct F-embeddings $E \to E$. Because E has finite degree over F, every such F-embedding is necessarily an isomorphism. □

Remark 9.1.0.8. Note that the degree of the extension is NOT in general equal to the number of distinct roots. Indeed, as we adjoin roots of the successive irreducible factors of the separable polynomial in the above, we will usually adjoin elements that are not roots of the original polynomial. For example, consider a splitting field of $x^3 - 2$. We first adjoin $2^{1/3}$ and the resulting extension has degree 3. However, not all the elements we adjoin at this stage are roots of $x^3 - 2$, namely $(2^{2/3})^3 = 4$, which is not a root of $x^3 - 2$. If we pass to the extension $E = \mathbb{Q}[2^{1/3}]$, then the polynomial $x^3 - 2$ factors as $(x - 2^{1/3})$ and a quadratic polynomial, which is still irreducible in E. Adjoining a root of that quadratic polynomial to E gives a degree 2 extension E' of E. Summing up, the splitting field of $x^3 - 2$ has degree 6 over $\mathbb{Q}$.

9.1.1 Galois extensions

We now establish a converse to the above result.

Theorem 9.1.1.1. *If E/F is a finite extension and $|Aut_F(E)| = [E : F]$, then*

i) $E^{Aut_F(E)} = F$,

ii) E/F is separable,

iii) for $\alpha \in E$, its F-conjugates are $\sigma(\alpha)$ for $\sigma \in Aut_F(E)$,

iv) every irreducible polynomial in $F[x]$ with a root in E splits completely in $E[x]$, and

v) E is the splitting field over F of a separable polynomial.

Proof. Observe first that (v) is a consequence of (ii) and (iv). Indeed, given (ii), since E/F is finite and separable, we see that $E = F(\alpha_1, \ldots, \alpha_r)$ for finitely many (distinct) elements each of which is separable over F. If μ_{α_i} is the minimal polynomial of α_i in F, then μ_{α_i} is an irreducible polynomial in $F[x]$. Since each μ_{α_i} has a root α_i in E, it follows from (iv) that μ_{α_i} splits completely in E. Since the α_i are distinct, taking the product $\prod_i \mu_{\alpha_i}$, we obtain a separable polynomial for which E is the splitting field.

Now, we establish the other facts. If we set $K = E^{Aut_F(E)}$, then the discussion at the beginning of this lecture guarantees that $F \subset K$. Therefore, $Aut_K(E) \subset Aut_F(E)$. Since K consists precisely of these elements of E that are fixed by $Aut_F(E)$, we see that $Aut_K(E) = Aut_F(E)$. Therefore, $E^{Aut_K(E)} = K$ as well. Therefore, (i) holds with K in place of F. We will now show that (ii), (iii) and (iv) all hold with K in place of F and then go back and show that $F = K$.

Let us show that E/K is separable. To this end, pick any $\alpha \in E$. Consider the set $\{\sigma(\alpha)|\sigma \in Aut_K(E)\}$, and write the distinct elements of this set as $\sigma_1(\alpha), \ldots, \sigma_m(\alpha)$. Consider the polynomial

$$h_\alpha(x) = \prod_{i=1}^{m}(x - \sigma_i(\alpha)),$$

which is separable by construction. (If $\alpha \in K$, then this product consists of a single term, and we can, without loss of generality assume that $\alpha \in E\backslash K$) Observe that the coefficients of h_α are functions of $\sigma_i(\alpha)$ that are invariant under permutation of the σ_i. Since any automorphism σ of E that fixes K necessarily permutes the roots of this polynomial, it follows that $\sigma(\sigma_i(\alpha)) = \sigma_j(\alpha)$. Since the σ_i are distinct, it follows that σ is injective and therefore also surjective. It follows that $h_\alpha(x)$ is fixed by σ and therefore lies in $E^{Aut_F(E)}[x] = K[x]$.

Next, we show that $h_\alpha(x)$ is the minimal polynomial of $\alpha \in K[x]$. Suppose $f(x) \in K[x]$ has α as a root. We will show that $h_\alpha(x)|f(x)$. For any $\sigma \in Aut_K(E)$, observe that $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$, so $f(x)$ is divisible by $x - \sigma(\alpha)$. Therefore, $f(x)$ is divisible by $x - \sigma_i(\alpha)$ for $i = 1, \ldots, m$ and therefore also by $h_\alpha(x)$. Since $f(x)$ was arbitrary, it follows that $h_\alpha(x)$ is the minimal polynomial of $\alpha in K[x]$. From the definition of $h_\alpha(x)$ and its minimality, the K-conjugates of α are precisely the elements $\sigma(\alpha)$ as σ runs through the elements of $Aut_K(E)$, which is (iii), with K in place of F.

To show that any irreducible $g \in K[x]$ with a root in E splits in $E[x]$, let γ be a root of g in E. Since g is irreducible over K, it is the minimal polynomial of $\gamma \in K[x]$, so by our previous construction, we have $g(x) = h_\gamma(x)$. However, $h_\gamma(x)$ splits completely in $E[x]$ by its very construction.

So far, we have established (ii), (iii), and (iv) with F replaced by K. Now, the same ideas at the start of the proof that (ii) and (iv) imply (v) show that E is a splitting field over K of a separable polynomial. Indeed, since E/K is finite, we may write $E = K(\beta_1, \ldots, \beta_n)$ for distinct elements $\beta_1, \ldots, \beta_n \in E \setminus K$. The polynomial h_{β_i} described above is then a separable polynomial satisfied by β_i, and therefore each β_i is separable over K. Thus, E/K is separable and is the splitting field of $\prod_i h_{\beta_i}$. By appeal to Proposition 9.1.0.7, we conclude that $|Aut_K(E)| = [E : K]$.

In the second paragraph above, we showed $Aut_K(E) = Aut_F(E)$ and by hypothesis $Aut_F(E) = [E : F]$. Combining these observations with the conclusion of the preceding paragraph, we conclude that $[E : K] = [E : F]$. Since $F \subset K \subset E$, we know that $[E : F][K : F] = [E : F]$, and therefore, we conclude that $[K : F] = 1$, i.e., $F = K$, which is precisely what we wanted to show. □

9.2 Lecture 32: Normal and Galois extensions

9.2.1 Normal extension

Definition 9.2.1.1. An algebraic extension E/F is called *normal* if any irreducible polynomial with coefficients in F that has a root in E splits completely in E.

Example 9.2.1.2. Any quadratic extension (separable or not!) is normal. Indeed, if $[E : F] = 2$, then any element of E has a minimal polynomial in $F[x]$ of degree 1 or 2, so only monic irreducibles in $F[x]$ of degree 1 or 2 could have a root in L. There isn't anything to say in the linear case, so consider $x^2 + bx + c \in F[x]$. If this polynomial has a root $r \in E$, then $r^2 + br + c = 0$. In that case, if we factor our $x - r$, long division shows us that

$$x^2 + bx + c = (x - r)(x + b + r).$$

This computation shows that the polynomial has a full set of roots in E.

Example 9.2.1.3. The field $\mathbb{Q}[2^{1/3}]$ is not normal, since $x^3 - 2$ has a root here but does not split.

Example 9.2.1.4. The splitting field of a separable polynomial is a normal extension.

Theorem 9.2.1.5. *For a finite extension E/F, the following conditions are equivalent.*

i) The equality $|Aut(E/F)| = [E : F]$ holds.
ii) The equality $E^{Aut_F(E)} = F$ holds.
iii) The extension E/F is separable and normal.
iv) The field E is the splitting field of a separable polynomial over F.

Proof. All of these assertions are reformulations of things we have established above. □

Definition 9.2.1.6. An extension E/F is called *Galois* if it satisfies any of the equivalent conditions of the previous theorem. In this case, the group $Aut_F(E)$ will be written $Gal(E/F)$ and called the Galois group of the extension.

Example 9.2.1.7. If F is a field having characteristic unequal to 2, then any extension E of degree 2 is a Galois extension. Indeed, since E has degree 2, it is generated over F by a single element, and we can conclude that the minimal polynomial of this element has degree 2. This element is of the form x^2+bx+c. Since F has characteristic unequal to 2, we may complete the square to see that x can be written as $x^2 - d$ for some $d \in F$. In this case, $Gal(E/F)$ has order 2 and the non-trivial element sends $+\sqrt{d}$ to $-\sqrt{d}$; this element is usually called the *conjugation*.

9.2.2 Some properties of Galois extensions

Proposition 9.2.2.1. *Any finite separable extension can be enlarged to a finite Galois extension.*

Proof. If E/F is a finite separable extension, then by the primitive element theorem, we may write $E = F(\gamma)$ for some element $\gamma \in E \setminus F$. In that case, we can take E' to be a splitting field for γ. Since γ is separable, it follows that the its splitting field is Galois by the equivalent characterizations of Galois extensions.

One may prove this result without appeal to the primitive element theorem as well. Indeed, write $E = F(\alpha_1, \ldots, \alpha_n)$ for some distinct elements α_i that are separable over F. Any splitting field for the product of the minimal polynomials of α_i, which is a separable polynomial, is necessarily Galois. □

Example 9.2.2.2. Consider the splitting field E of the polynomial $x^3 - 2$ over $\mathbb{Q}$. After adjoining $2^{1/3}$, this can be rewritten

$$(\frac{x}{2^{1/3}})^3 - 1 = (\frac{x}{2^{1/3}} - 1)((\frac{x}{2^{1/3}})^2 + \frac{x}{2^{1/3}} + 1).$$

If $u = \frac{x}{2^{1/3}}$, then the roots u^2+u+1 are of the form $u = \frac{-1\pm\sqrt{-3}}{2}$. While the extension $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is *NOT* a Galois extension, observe that the extension $E/\mathbb{Q}(2^{1/3})$ *is* Galois. Indeed, it is precisely the splitting field of $x^3 + 1$ (or, just the irreducible quadratic factor $1 - x + x^2$ of this polynomial) over $\mathbb{Q}(2^{1/3})$. This phenomenon is rather general.

Proposition 9.2.2.3. *If E/F is a Galois extension and $F \subset K \subset E$ is an intermediate extension, then E/K is Galois as well.*

Proof. An extension is Galois if it is normal and separable. Therefore it suffices to check that E/K has these properties. Given an arbitrary element $\alpha \in E$, we can consider its minimal polynomial over F and over K. Since the minimal polynomial over K divides the minimal polynomial over F, both separability and normality are preserved in passing from E/F to E/K. □

Example 9.2.2.4. Before moving on, let us work out a more complicated example in detail. Consider the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Over $\mathbb{R}$ this factors as $(x^2 - \sqrt{2})(x^2 + \sqrt{2})$, and the former factors as $(x - 2^{1/4})(x + 2^{1/4})$ while the latter factors as $(x - i2^{1/4})(x + i2^{1/4})$. Therefore, if we adjoin $2^{1/4}$ and i to $\mathbb{Q}$, we obtain a splitting field for $x^4 - 2$. Consider the field $E = \mathbb{Q}(2^{1/4}, i)$. There are some natural subfields here: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(i2^{1/4})$, and $\mathbb{Q}(2^{1/4})$.

Any element of $Gal(E/\mathbb{Q})$ permutes the 4 roots of $x^4 - 2$, but not all 24 permutations of the roots are realized by the Galois group. For example, since $2^{1/4}$ and $-2^{1/4}$ add to 0, and any automorphism fixing $\mathbb{Q}$ fixes 0, it follows that these two roots must be mapped to roots that are also negatives of each other. In particular, no field automorphism of E over $\mathbb{Q}$ can send $2^{1/4}$ to $i2^{1/4}$ and $-2^{1/4}$ to $2^{1/4}$.

To describe the Galois group explicitly, we think about what automorphisms σ of E do to $2^{1/4}$ and i. Since $\sigma(2^{1/4})$ has to be a root of $x^4 - 2$ (4 choices), and $\sigma(i)$ has to be a root of $x^2 + 1$ (2 choices), there at most $8 = 4 \cdot 2$ automorphisms of E over $\mathbb{Q}$. Since the degree of the extension $E/\mathbb{Q} = 8$, we conclude that $Gal(E/\mathbb{Q})$ has size 8 and thus all assignments of $\sigma(2^{1/4})$ and $\sigma(i)$ to roots of $x^4 - 2$ and $x^2 + 1$ must be realized by field automorphisms.

Let r and s be automorphisms of $E/\mathbb{Q}$ determined by $r(2^{1/4}) = i2^{1/4}$, $r(i) = i$, and $s(2^{1/4}) = 2^{1/4}$, $s(i) = -i$. By taking powers and products (i.e., composites) of automorphisms, we obtain the following table:

σ	id	r	r^2	r^3	s	rs	r^2s	r^3s
$\sigma(2^{1/4})$	$2^{1/4}$	$i2^{1/4}$	$-2^{1/4}$	$-i2^{1/4}$	$2^{1/4}$	$i2^{1/4}$	$-2^{1/4}$	$-i2^{1/4}$
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

And the table takes this form because you can check that $r^4 - id$ and $s^2 = id$. Likewise, we can observe from the table that $rs = sr^{-1}$ is isomorphic to D_4.

Since E is a Galois extension of $\mathbb{Q}$, the minimal polynomial over $\mathbb{Q}$ of any element in E splits completely over E. For example, if $\alpha = 2^{1/4} + \sqrt{2} + 1$. The $\mathbb{Q}$-conjugates of α are found by applying the elements of $Gal(E/\mathbb{Q})$ to α and seeing what different numbers come out. Since each automorphism acts by a ring homomorphism, this amounts to replacing $2^{1/4}$ in the expression for α by the 4 different 4-th roots of 2 and replacing $\sqrt{2} = 2^{1/4^2}$ in the expression for α by the squares of those 4-th roots of 2. Thus, the list takes the form:

$$2^{1/4} + \sqrt{2} + 1, i2^{1/4} - \sqrt{2} + 1, -2^{1/4} + \sqrt{2} + 1, -i2^{1/4} - \sqrt{2} + 1.$$

Although the Galois group has order 8, this Galois orbit has size 4. Note that $\mathbb{Q}(\alpha)$ thus has degree 4 and since $\mathbb{Q}(\alpha) \subset \mathbb{Q}(2^{1/4})$ a degree comparison shows that $\mathbb{Q}(\alpha) = \mathbb{Q}(2^{1/4})$.

For the extension $E/\mathbb{Q}$, the intermediate fields $\mathbb{Q}(2^{1/4})$ and $\mathbb{Q}(i2^{1/4})$ are isomorphic over $\mathbb{Q}$ since each is obtained by adjoining to $\mathbb{Q}$ of one root of $x^4 - 2$. There is a $\mathbb{Q}$-isomorphism given explicitly by $\sigma(2^{1/4}) = i2^{1/4}$. Now, some $\varphi \in Gal(E/\mathbb{Q})$ restricts to σ. Observe that r induces this isomorphism, but so does rs.

9.3 Lecture 33: The Galois correspondence and examples

9.3.1 Isomorphisms of intermediate fields

Lemma 9.3.1.1. *Suppose E/F is a Galois extension and K and K' are two intermediate subfields. The subfields K and K' are F-isomorphic if and only if $K' = \sigma(K)$ for some $\sigma \in Gal(E/F)$.*

Proof. If $K' = \sigma(K)$ for some $\sigma \in Gal(E/F)$, then σ is an F-isomorphism from K to K'. Conversely, suppose K and K' are F-isomorphic and fix an F-isomorphism $\varphi : K \to K'$. We want to show that φ, which is defined on K is the restriction to K of some element of the Galois group. By the primitive element theorem, $K = F(\gamma)$ for some γ. Consider the field $F(\varphi(\gamma))$. Since $\varphi(\gamma) \in K'$, it follows that $F(\varphi(\gamma)) \subset K'$, but a priori we don't know if $\varphi(\gamma)$ is a primitive element of K'.

Since φ fixes F, $\varphi(\gamma) \in K'$ has the same minimal polynomial over F as γ. In particular, the extensions generated by γ and $\varphi(\gamma)$ have the same degree over F. Since K and K' are isomorphic over F, we know that $[K : F] = [K' : F]$. On the other hand, $[K' : F] = [K' : F(\varphi(\gamma))][F(\varphi(\gamma)) : F]$. The observation just made about minimal polynomials shows that $[F(\varphi(\gamma)) : F] = [K : F]$, and therefore we conclude that $[K' : F(\varphi(\gamma))] = 1$, i.e., $K' = F(\varphi(\gamma))$.

Next, since $\varphi(\gamma)$ and γ have the same minimal polynomial, they are both roots of the minimal polynomial in a splitting field, i.e., they are F-conjugates in E. Since the extension E/F is a finite Galois extension, it follows from point (iii) of Theorem 9.1.1.1 that the F-conjugates of γ are precisely the expressions $\sigma(\gamma)$ as σ runs through the elements of $Gal(E/F)$. Thus, there exists an element $\sigma \in Gal(E/F)$ such that $\varphi(\gamma) = \sigma(\gamma)$. Since φ and σ agree upon restriction to F and take the same value on γ, they agree on $F(\gamma) = K$, i.e., $\sigma|_K = \varphi$. □

9.3.2 Artin's theorem

Theorem 9.3.2.1 (Artin's theorem)**.** *Let F be a field, and H a finite group of automorphisms of F. If $[F : F^H]$ is finite, then F/F^H is a Galois extension and $Gal(F/F^H) = H$.*

Proof. First we show that F/F^H is separable using the same idea as the proof above. Pick any $\alpha \in F$. Consider the finite set $\sigma(\alpha), \sigma \in H$ and list the distinct elements as $\{\sigma_1(\alpha), \dots, \sigma_m(\alpha)\}$. By construction, α is a root of $h_\alpha := \prod_{i=1}^m (X - \sigma_i(\alpha))$, and the roots of this polynomial are distinct and lie in F. By construction the degree of h_α is m, which is at most $|H|$.

The coefficients of $h_\alpha(x)$ all lie in F^H, since expanding out this polynomial, the coefficient of x^i is invariant under H. Therefore, F/F^H is an algebraic extension that is separable over F^H, and every element $\alpha \in F$ has degree at most $|H|$ over F^H.

Now, F/F^H is a finite separable extension of degree at most $|H|$, by the primitive element theorem $F = F^H(\alpha)$ for some α, so $[F : F^H] = [F^H(\alpha), F^H] \leq deg h_\alpha \leq |H|$. Since h_α splits over F, F/F^H is necessarily a Galois extension, so $Gal(F/F^H) = [F : F^H] \leq |H|$. Since H is a subgroup of $Gal(F/F^H)$, we see that $|H| \leq |Gal(F/F^H)|$, and this gives the required equality. □

9.3.3 The fundamental theorem of Galois theory

Theorem 9.3.3.1 (Fundamental theorem of Galois theory)**.** *Let E/F be a finite galois extension and set $G = Gal(E/F)$. The inclusion reversing mappings $K \mapsto Gal(E/K)$ and $H \mapsto E^H$ between intermediate subfields of E and subgroups of G are mutually inverse bijections and satisfy the following properties when K and H correspond (i.e., $K = E^H$ or $H = Gal(E/K)$).*

i) The equalities $|H| = [E : K]$ and $[K : F] = [G : H]$ hold.

ii) Two intermediate fields K and K' with corresponding H and H' are isomorphic over F if and only if H and H' are conjugate subgroups of G.

iii) The extension K/F is Galois if and only if H is a normal subgroup of G, in which case the restriction map $G \to Gal(K/F)$ sending σ to $\sigma|_K$ is surjective with kernel H, i.e., $G/H \cong Gal(K/F)$.

Proof. First, let us check that the correspondences are inverses. Going from fields to subgroups to fields, we need $K^{Gal(L/K)} = K$, and going from subgroups to fields to subgroups requires $Gal(E/E^H) = H$. The first equality follows by our equivalent characterizations of Galois extensions from last time, and the statement above about intermediate extensions. For the second statement, equality comes form Artin's theorem (note that E/E^H is finite and $K \subset E^H$ guarantees finiteness).

For (i), suppose K and H correspond. In that case, we have $K = E^H$, so $|H| = [E : E^H]$ by Artin's theorem.

For (ii), recall that two intermediate subfields K and K' are F-isomorphic if and only if there is $\sigma \in Gal(E/F)$ such that $\sigma(K) = K'$. Then, write any F-isomorphic copy of K in E as $\sigma(K)$ for some $\sigma \in Gal(E/F)$. Then, for any $\tau \in Gal(E/F)$, observe that

$$\begin{aligned}\tau \in Gal(E/\sigma(K)) &\iff \tau(\sigma(\alpha)) = \sigma(\alpha)\forall\alpha \in K,\\ &\iff \sigma^{-1}\tau\sigma(\alpha) = \alpha\forall\alpha \in K,\\ &\iff \sigma^{-1}\tau\sigma \in Gal(E/K) = H,\\ &\iff \tau \in \sigma H\sigma^{-1}.\end{aligned}$$

Therefore, $Gal(E/\sigma(K)) = \sigma H\sigma^{-1} = \sigma Gal(E/F)\sigma^{-1}$.

For (iii), note that an intermediate extension is automatically separable since every element of a Galois extension is separable over the base field. Therefore K/F is Galois if and only if K/F is normal. Since K sits inside the Galois extension E/F, the F-conjugates of any element of K are precisely its orbit under $Gal(E/F)$. Therefore, K/F is normal if and only if $\sigma(K) \subset K$ for all $\sigma \in G$. Since $\sigma(K)$ and K have the same degree over F (by the argument in Lemma 9.3.1.1), the inclusion $\sigma(K) \subset K$ implies $\sigma(K) = K$. In other words, K/F is normal if and only if $\sigma(K) = K$ for every $\sigma \in Gal(E/F)$ which in turn is true if and only if $\sigma H\sigma^{-1} = H$ for every $\sigma \in Gal(E/F)$, but this is precisely the statment that H is normal in G.

Restricting elements of $Gal(E/F)$ viewed as F-automorphisms of E to K defines a function $Gal(E/F) \to Gal(K/F)$ which is a group homomomorphism with kernel equal to $Gal(E/K) = H$. Thus, we obtain an embedding $G/H \hookrightarrow Gal(K/F)$. Since $|G/H| = [Gal(E/F) : H] = [K : F] = |Gal(K/F)|$ (where the last equality uses the fact that K/F is Galois). Thus, $G/H \cong Gal(K/F)$. □

9.3.4 The Galois correspondence in action

Example 9.3.4.1. Consider the splitting field E of the polynomial $x^4 - 2$ over $\mathbb{Q}$. Last time, we observed that E is a Galois extension of $\mathbb{Q}$ of degree 8, and its Galois group is isomorphic to D_8 as follows: we identified $E = \mathbb{Q}(2^{1/4}, i)$ and then set r to be the automorphism of E fixing $\mathbb{Q}$, sending $2^{1/4}$ to $i2^{1/4}$ and acting as the identity on i, and s to be the automorphism of E that fixes $\mathbb{Q}$, acts as the identity as $2^{1/4}$ and sends i to $-i$.

Now, we analyze the Galois correspondence in this example. First, we write down the partially ordered set of subgroups of D_4. In terms of the generators and relations we have the trivial subgroup, the subgroups generated by a single element are: $\langle s\rangle$, $\langle r\rangle$, $\langle r^2\rangle$, $\langle r^3\rangle = \langle r\rangle$, $\langle rs\rangle$, $\langle r^2s\rangle$ and $\langle r^3s\rangle$. The subgroups generated by a pair of elements are D_4 itself, the subgroups $\langle r^2, s\rangle$ and $\langle r^2, rs\rangle$. Note that $\langle s\rangle$, $\langle r^2\rangle$, $\langle rs\rangle$, $\langle r^2s\rangle$ and $\langle r^3s\rangle$ all have order 2, while $\langle r\rangle$ is cyclic of order 4, and $\langle r^2, s\rangle$ and $\langle r^2, rs\rangle$ are both isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$. Listing these by inclusion (and ignoring the trivial subgroup which includes into all the groups in the first row) yields the following picture:

$$\begin{tikzcd}
\langle s \rangle \arrow[dr, hook] & \langle r^2 s \rangle \arrow[d, hook] & \langle r^2 \rangle \arrow[d, hook] & \langle rs \rangle \arrow[d, hook] & \langle r^3 s \rangle \arrow[dl, hook'] \\
 & \langle r^2, s \rangle \arrow[dr, hook] & \langle r \rangle \arrow[d, hook] & \langle r^2, rs \rangle \arrow[dl, hook'] & \\
 & & D_4 & &
\end{tikzcd}$$

We would now like to identify the corresponding intermediate field extensions. The fixed field of the whole Galois group is $\mathbb{Q}$ itself. Now, we turn to the groups in the next row up. Consider first $\langle r^2, s\rangle$. Since s acts by sending i to $-i$, and r^2 acts by sending $2^{1/4}$ to $-2^{1/4}$ and $i2^{1/4}$ to $-i2^{1/4}$, you can convince yourself that the fixed field is $\mathbb{Q}[\sqrt{2}]$. Likewise, the fixed field of $\langle r \rangle$ is simply $\mathbb{Q}(i)$. The fixed field of $\langle r^2, rs\rangle$ has degree 2 over $\mathbb{Q}$ as well and therefore corresponds to a quadratic extension; you can check that it corresponds to $\mathbb{Q}[i\sqrt{2}]$.

Proceeding to the next row up, we see that the fixed field of $\langle s \rangle$ has degree 4 over $\mathbb{Q}$ and is $\mathbb{Q}[2^{1/4}]$. Likewise, the fixed field of $\langle r^2, s\rangle$ necessarily contains both $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$ and since it has degree 4 over $\mathbb{Q}$, you can check it is equal to $\mathbb{Q}(\sqrt{2}, i)$. This leaves 3 fields to determine: the fixed fields of $\langle rs \rangle$, $\langle r^2 s\rangle$ and $r^3 s\rangle$. To figure these out, we can proceed as follows.

Write a general element of E in the form

$$a + b2^{1/4} + c2^{1/2} + d2^{3/4} + ei + fi2^{1/4} + gi2^{1/2} + hi2^{3/4}.$$

We computed before that rs sends this element to

$$a + bi2^{1/4} - c2^{1/2} - di2^{3/4} - ei + f2^{1/4} + gi2^{1/2} - h2^{3/4}.$$

Therefore, the condition that a vector is fixed by rs amounts to saying that $b = f, c = 0, e = 0, d = -h$. In other words, a general element fixed by rs takes the form

$$\alpha = a + b(2^{1/4} + i2^{1/4}) + d(2^{3/4} - i2^{3/4}) + gi2^{1/2}.$$

Thus, we have obtained a $\mathbb{Q}$-basis of the fixed field. Here, we can write $2^{1/4} + i2^{1/4}$ as $(1+i)2^{1/4}$ and can check that this element is primitive. Similar techniques can be used for the other examples.

Observe here that the subgroups$\langle s \rangle$ and $\langle r^2 s\rangle$ are conjugate: indeed, since $sr = r^{-1}s$, $rsr^{-1} = rsr^3 = rr^{-1}sr^2 = sr^2 = r^{-1}sr = r^{-2}s = r^2 s$, so the corresponding subfields are $\mathbb{Q}$-isomorphic. Likewise, $srss^{-1} = sr = r^3 s$, so the subfields corresponding to $\langle rs \rangle$ and $\langle r^3 s\rangle$ are isomorphic. The only normal subgroup of D_4 of index 2 is $\mathbb{Z}/4$, generated by $\langle r \rangle$, and we already saw the fixed field is $\mathbb{Q}(i)$. Likewise, the fixed field of $\langle r^2 \rangle$ is $\mathbb{Q}(\sqrt{2}, i)$ and these are the only Galois extensions of $\mathbb{Q}$ inside E.

Chapter 10

Irreducibility and cyclotomic extensions

10.1 More on irreducibility

10.1.1 Irreducibility

So far, we've been avoiding the issue of checking whether a polynomial is irreducible: in simple cases this could be done by ad hoc methods, but it's useful to have more general methods.

Theorem 10.1.1.1 (Schoenemann-Eisenstein)**.** *Suppose $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$, i.e., $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. If all of the coefficients a_i are divisible by a prime p, but a_0 is not divisible by p^2. then f is irreducible in $\mathbb{Z}[x]$.*

Proof. Assume to the contrary that f is not irreducible, i.e., $f = f_1 f_2$ with $f_1 = x^r + b_{r-1}x^{r-1} + \cdots + b_0$ and $f_2 = x^s + c_{s-1}x^{s-1} + \cdots + c_0$ with $0 < r, s < n$. Take i to be the smallest index such that p does not divide b_i (note that i can be equal to r with $b_r = 1$). Similarly, let j be the smallest index such that p does not divide c_j. In that case, the $i+j$-th coefficient a_{i+j} of the product is

$$a_{i+j} = b_i c_j + (b_{i-1}c_{j+1} + \cdots) + (b_{i+1}c_{j-1} + \cdots).$$

Thus, a_{i+j} is a sum of $b_i c_j$ and terms that are divisible by p. Since p does not divide $b_i c_j$, it follows that p does not divide a_{i+j}.

On the other hand, since by assumption p^2 does not divide $a_0 = b_0 c_0$ it follows that p cannot divide both b_0 and c_0. Therefore, either $i = 0$ or $j = 0$ and we see that $i + j < n$. However, this contradicts the assumption that a_r is divisible by p. Thus, we conclude that f is irreducible in $\mathbb{Z}[x]$. □

Corollary 10.1.1.2. *If p is a prime number, then the polynomial $\phi(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + 1$ is irreducible in $\mathbb{Z}[x]$.*

Proof. Observe that $\phi(x)$ is irreducible if and only if $\phi(x+1)$ is irreducible. However, by the binomial formula

$$\begin{aligned}\phi(x+1) &= (x+1)^{p-1} + \cdots + 1 \\ &= \sum_{i=0}^{p-1} (\binom{p-1}{i} + \binom{p-2}{i-1} + \cdots + \binom{p-1-i}{0}) x^{p-1-i} \\ &= \sum_{i=0}^{p-1} \binom{p}{i} x^{p-1-i}.\end{aligned}$$

Thus, p divides all coefficients but the first, and p^2 does not divide the last. Therefore, by the Eisenstein irreducibility criterion, we conclude that this polynomial is irreducible. □

Remark 10.1.1.3. Now, the above result is not "good enough" for our applications because even if a polynomial in $\mathbb{Z}[x]$ is irreducible, *a priori* it could become reducible in $\mathbb{Q}[x]$. Therefore, we need to improve our result to guarantee irreducibility in $\mathbb{Q}[x]$.

If f is a polynomial with integer coefficients, then there could be an integer that divides all the coefficients, and that would give us a factorization of f that is "irrelevant" in $\mathbb{Q}[x]$. Given a polynomial f, let $c(f)$ be the greatest common divisor of the coefficients of f. If $f \in \mathbb{Z}[x]$, we can write $f = c(f)\bar{f}$, and we will call the polynomial $\bar{f}$ *primitive*. We could replace $c(f)$ by $-c(f)$ and $\bar{f}$ by $-barf$ without changing anything, so $c(f)$ is only really well-defined up to multiplication by a unit in $\mathbb{Z}$.

Lemma 10.1.1.4. *The product of two primitive polynomials in $\mathbb{Z}[x]$ is again a primitive polynomial.*

Proof. This is a variation on the proof above. Suppose f and g are primitive polynomials, and that fg is not primitive. In that case, there exists a prime number p that is a common divisor of all coefficients of the product. Since $f(x)$ and $g(x)$ are primitive, p cannot divide either all the coefficients of f or all those of g. Let i be the index of the highest degree coefficient of f that is not divisible by p and let j be the index of the highest degree coefficient of g that is not divisible by p. The coefficient of x^{r+s} can then be written as $a_i b_j$ and terms that are divisible by p. However, this contradicts the assertion that all coefficients of fg are divisible by p. Thus, the coefficients of fg have no common divisor and fg is primitive. □

Corollary 10.1.1.5. *If f is a polynomial in $\mathbb{Z}[x]$ that factorizes in $\mathbb{Q}[x]$ as a product of two polynomials of lower degree, then f factors in $\mathbb{Z}[x]$.*

Proof. Assume $f = gh$ for some $gh \in \mathbb{Q}[x]$. Write $f = c(f)\bar{f}$. Now, by "clearing the denominators" of the coefficients of g, we can write $dg = g'$ where g' is an integral polynomial. Therefore, writing $g' = c(g)\bar{g}$, we see that g can be written as $\frac{c(g)}{d}\bar{g}$ for a primitive polynomial $\bar{g}$. Similarly, h can be written as $\frac{c(h)}{e}\bar{h}$ for a primitive polynomial $\bar{h}$. Then, $c(f)\bar{f} = \frac{c(f)c(g)}{de}\bar{g}\bar{h}$, i.e., $dec(f)\bar{f} = c(f)c(g)\bar{g}\bar{h}$. Now $\bar{f}$ is primitive, and $\bar{g}\bar{h}$ is primitive by the lemma above. If p divides the right and side, then it divides $c(f)c(g)$ and if it divides the right hand side, then it divides $dec(f)$. We conclude from this that $dec(f)|c(f)c(g)$ and $c(f)c(g)|dec(f)$. In that case, we obtain the required factorization of f in $\mathbb{Z}[x]$. □

Thus, the above corollary shows that if f is a polynomial that is irreducible in $\mathbb{Z}[x]$, it is necessarily irreducible in $\mathbb{Q}[x]$.

Corollary 10.1.1.6. *The polynomial $\frac{x^p-1}{x-1}$ is irreducible in $\mathbb{Q}[x]$.*

10.2 Cyclotomic extensions and abelian Galois groups

10.2.1 Cyclotomic extensions

The polynomials $x^n - 1$ are, of course, not irreducible in general; the roots of this polynomial are the n-th roots of 1 in the field under consideration. Note, nevertheless, that the set of elements satisfying the above condition form a subgroup of the multiplicative group of the field.

Theorem 10.2.1.1. *The group of n-th roots of unity in a field is cyclic. More generally, any finite subgroup of non-zero elements of a field is a cyclic group.*

Proof. The proof is the same as in the finite field case. Let F be a field and let G be a finite subgroup of $F^{\times}$. If x_1 and x_2 are elements in G with orders n_1 and n_2, then element x_1x_2 has order equal to $lcm(n_1n_2)$. Let n be the maximal order of an element in G. In that case, the order of every element divides n: if $g \in G$ has order n, and g' has order n', then there is an element of G of order $lcm(n, n') \geq n$. Since n is the maximum of the orders, we conclude that $lcm(n, n') \leq n$, which implies $lcm(n', n) = n$, i.e., $n'|n$. Since all orders divide the maximal order, every element of G is a root of $x^n - 1$. This also implies $|G| \leq n$ since $x^n - 1$ has at most n roots in F. Since $n||G|$ this means that $n = |G|$. □

If $x^n - 1$ is separable in $F[x]$, its roots in a splitting field form a cyclic group, denoted μ_n. A choice of generator of μ_n, denoted ζ_n is called a primitive n-th root of unity. We write $F[\mu_n]$ for a splitting field of $x^n - 1$ over F. Such an extension can be written as $F[\zeta_n]$: adjoining a primitive root of unity is the same as adjoining all roots of unity. Extensions of this form are called *cyclotomic extensions*. Our goal is to understand the Galois group of such an extension.

Lemma 10.2.1.2. *For $\sigma \in Gal(F(\zeta_n)/F)$, there is an integer $a = a(\sigma)$ that is relatively prime to n such that $\sigma(\zeta) = \zeta^a$ for all $\zeta \in \mu_n$.*

Proof. Let ζ_n be a generator of μ_n, i.e., $\zeta^n = 1$ and $\zeta_n^j \neq 1$ for $1 \leq j < n$. In that case, $\sigma(\zeta_n)^n = 1$ and $\sigma(\zeta_n)^j \neq 1$ for $1 \leq j < n$, so $\sigma(\zeta_n)$ is again a primitive n-th root of unity. Therefore, $\sigma(\zeta_n) = \zeta_n^a$ where $(a, n) = 1$. Now, any element $\zeta \in \mu_n$ has the form ζ_n^k for some k. Therefore,

$$\sigma(\zeta) = \sigma(\zeta_n^k) = \sigma(\zeta_n)^k = (\zeta_n^a)^k = (\zeta_n^k)^a = \zeta^a.$$

□

The exponent a in the above lemma is well-defined modulo n, since $\zeta_n^a = \zeta_n^b$ implies $a \equiv b \mod n$. Therefore, we can think of $a(\sigma)$ as an element of $(\mathbb{Z}/n)^{\times}$.

Remark 10.2.1.3. Consider the polynomial $x^5 - 1$ over $\mathbb{Q}$. The primitive 5-th roots of unity are precisely the non-trivial 5-th roots of unity, i.e., the roots of $1 + x + \cdots + x^4$. The latter polynomial is irreducible over $\mathbb{Q}$ as we saw above. Thus, if ζ_5 is a generator, then, e.g., ζ_5 and ζ_5^2 have the same minimal polynomial. Since $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_5^2)$, the above lemma guarantees that there is an automorphism σ fixing $\mathbb{Q}$ such that $\sigma(\zeta) = \zeta^2$ for all $\zeta \in \mu_5$. This is *false* for arbitrary elements of $\mathbb{Q}(\zeta_5)$, since squaring is not additive.

10.2.2 Galois groups of cyclotomic extensions of $\mathbb{Q}$

We now use the results we deduced last time to study the Galois groups of cyclotomic extensions of $\mathbb{Q}$.

Theorem 10.2.2.1. *The map $\sigma \mapsto a(\sigma) \mod n$, where $\sigma(\zeta) = \zeta^{a(\sigma)}$ for all $\zeta \in \mu_n$ is an injective group homomomorphism*

$$Gal(F(\mu_n)/F) \longrightarrow (\mathbb{Z}/n)^{\times}.$$

Proof. Pick σ and τ in $Gal(F(\mu_n)/F)$. Choose a primitive n-th root of unity ζ_n. In that case,

$$(\sigma\tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{a(\tau)}) = \sigma(\zeta_n)^{a(\tau)} = ((\zeta_n)^{a(\sigma)})^{a(\tau)} = \zeta_n^{a(\sigma)a(\tau)}.$$

Also, $(\sigma\tau)(\zeta_n) = {\zeta_n}^{a(\sigma\tau)}$, so $\zeta_n^{a(\sigma\tau)} = \zeta_n^{a(\sigma)a(\tau)}$. Since ζ_n has order n, $a(\sigma\tau) \equiv a(\sigma)a(\tau) \mod n$, and thus sending σ to $a(\sigma)$ is a group homomorphism.

To see that it is injective, suppose σ lies in the kernel. In that case, $a(\sigma) \equiv 1 \mod n$, so $\sigma(\zeta_n) = \zeta_n$. Since $F(\mu_n) = F(\zeta_n)$, and σ is the identity on F, it follows that σ is the identity automorphism. □

Corollary 10.2.2.2. *The extension $Gal(F(\mu_n)/F)$ has abelian Galois group.*

Remark 10.2.2.3. The homomorphism above is not surjective in general. Indeed, take $F = \mathbb{R}$ and $n \geq 3$.

It is natural to ask whether we can give hypotheses guaranteeing surjectivity. The first case to consider is the case where $F = \mathbb{Q}$.

Theorem 10.2.2.4. *If ζ is a primitive n-th root of unity in some extension of $\mathbb{Q}$, then the homomorphism $Gal(\mathbb{Q}(\mu_n)/Q) \to \mathbb{Z}/n\mathbb{Z}^\times$ constructed last time is an isomorphism.*

Proof. If $\phi(n)$ is Euler's ϕ-function, i.e., the number of natural numbers $\leq n$ that are relatively prime to n, then one knows that $\phi(n)$ is precisely $|\mathbb{Z}/n^\times|$. Thus, to establish the result, it suffices by the fundamental theorem of Galois theory to establish that $|Gal(\mathbb{Q}(\mu_n)/Q)| = \phi(n)$.

Let $\Phi(x)$ be the minimal polynomial of ζ. Since ζ is a root of $x^n - 1$, it follows that $x^n - 1 = \Phi(x)\Psi(x)$, where we can assume that $\Psi(x)$ and $\Phi(x)$ are monic with coefficients with $\mathbb{Z}$ (and even primitive). We will show that every primitive root ζ^i (with $gcd(i,n) = 1$) is also a root of $\Phi(x)$ and it will follow that $[Q(\zeta) : \mathbb{Q}] = deg\Phi(x) \geq \phi(n)$. Since we already know that $[\mathbb{Q}(\zeta) : \mathbb{Q}]|\phi(n)$ by the theorem we proved last time, the equality of the theorem will follow. □

To establish the last fact, it suffices to prove the following.

Theorem 10.2.2.5. *If a is an integer with $gcd(a,n) = 1$, then ζ and ζ_n^a have the same minimal polynomial over $\mathbb{Q}$.*

Proof. Since ζ^a only depends on a modulo n, we can assume $a > 0$ and, in fact, $a > 1$. Write $a = p_1 p_2 \cdots p_r$ as a product of primes p_i (each not dividing n, but the p_i may coincide). To show that ζ and ζ^a have the same minimal polynomial over $\mathbb{Q}$, it suffices to show that for each prime p not dividing n that any primitive n-th root of unity and its p-th power have the same minimal polynomial over $\mathbb{Q}$, since in that case, the successive pairs of primitive n-th roots of unity

$$\zeta, \zeta^{p_1}, \zeta^{p_1 p_2}, \ldots$$

have the same minimal polynomial because each is a prime power of the previous one.

Let $f(x)$ be the minimal polynomial of ζ over $\mathbb{Q}$, where ζ is a primitive n-th root of unity. Assume that ζ and ζ^p are not $\mathbb{Q}$-conjugate for some prime p not dividing n. Let $g(x)$ be the minimal polynomial of ζ^p in $\mathbb{Q}[x]$, so $g(x) \neq f(x)$. The polynomials $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$ since they both divide $x^n - 1$ and any monic factor of $x^n - 1$ in $\mathbb{Q}[x]$ actually lies in $\mathbb{Z}[x]$ by what we established last time.

Since $f(x)$ and $g(x)$ are different monic irreducible factors of $x^n - 1$ in $\mathbb{Q}[x]$, we see that $x^n - 1 = f(x)g(x)h(x)$ for some monic $h(x) \in Q[x]$. Again, $h(x) \in \mathbb{Z}[x]$ by the lemma from last time. Now, consider the reduction modulo p homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/p[x]$. Write $\bar{f}$ for the image of $f \in \mathbb{Z}[x]$ under this homomorphism and similarly for the other polynomials that appear. In that case,

$$x^n - \bar{1} = \bar{f}\bar{g}\bar{h}$$

in $\mathbb{Z}/p[x]$. The polynomial $x^n - \bar{1}$ is separable in $\mathbb{Z}/p[x]$ since p does not divide n, and therefore we conlcude also that $\bar{f}$ and $\bar{g}$ are relatively prime in $\mathbb{Z}/p[x]$. Since $f(x)$ and $g(x)$ are monic, their reductions $\bar{f}$ and $\bar{g}$ have the same degrees as $f(x)$ and $g(x)$ so their reductions modulo p are necessarily non-constant.

Since $g(\zeta^p) = 0$, we know that $g(x^p)$ has ζ as a root. Therefore, $f(x)|g(x^p)$ in $\mathbb{Q}[x]$. Write $g(x^p) = f(x)k(x)$ for some monic $k(x) \in \mathbb{Q}[x]$. Again, $k(x) \in \mathbb{Z}[x]$ by the lemma from last time. Reducing the equation $g(x^p) = f(x)k(x)$ modulo p and using the formula $\bar{g}(x^p) = \bar{g}(x)^p$ in $\mathbb{Z}/p[x]$, we get the equality

$$\bar{g}(x)^p = \bar{f}(x)\bar{k}(x)$$

in $\mathbb{Z}/p[x]$. Then, any irreducible factor of $\bar{f}$ in $\mathbb{Z}/p[x]$ is a factor of $\bar{g}$ (and there are irreducible factors since $\bar{f}$ is non-constant). However, that contradicts the relative primality of $\bar{f}$ and $\bar{g}$. □

10.2.3 Subgroups and quotients of finite abelian groups

Proposition 10.2.3.1. *If A is a finite abelian group, and $A' \subset A$ is a subgroup, then there exists a subgroup $A'' \subset A$ such that $A/A'' \cong A$.*

Proof. By the structure theory, A is isomorphic to a direct sum of cyclic groups of prime power order. The image of A' in A breaks up into subgroups of each of these prime power factors and therefore it suffices to prove the result for groups of prime power order. Thus, suppose $A = \mathbb{Z}/p^r$ and $A' \subset A$. In that case, simply observe that there is an exact sequence of the form

$$0 \longrightarrow \mathbb{Z}/p^a \longrightarrow \mathbb{Z}/p^{a+b} \longrightarrow \mathbb{Z}/p^b \longrightarrow 0$$

for any $a, b \geq 0$. □

10.2.4 Finite abelian groups as Galois groups

Theorem 10.2.4.1. *Every finite abelian group can be realized as a Galois group over $\mathbb{Q}$.*

Sketch. We know that $Gal(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong \mathbb{Z}/n^\times$ by the previous result. Let us now observe that, by the Galois correspondence, any finite subgroup A of $\mathbb{Z}/n^\times$ can also be realized as a Galois group over $\mathbb{Q}$. By the proposition above, we choose a subgroup H of $\mathbb{Z}/n^\times$ such that $Zn^\times/H \cong A$. By the Galois correspondence, A is precisely the Galois group of the extension $\mathbb{Q}(\mu_n)^H$.

Now, the order of the group $\mathbb{Z}/n^\times$ is $\phi(n)$. If $n = ab$ with a and b coprime, then $\phi(n) = \phi(a)\phi(b)$. In that case, $\mathbb{Z}/n \cong \mathbb{Z}/a \times \mathbb{Z}/b$ as *rings* by the Chinese remainder theorem, and one can similarly show that $\mathbb{Z}/n^\times \cong \mathbb{Z}/a^\times \times \mathbb{Z}/b^\times$. By induction, one can conclude that $\mathbb{Z}/n^\times$ is a product of factors of the form $(\mathbb{Z}/{p_i}^{a_i})^\times$. In particular, if $n = p_1 \cdots p_r$, then $\mathbb{Z}/n^\times \cong \prod_{i=1}^r \mathbb{Z}/(p_i - 1)$. It suffices to show that for $n_1, \ldots, n_r$ as above, we can find primes $p_1, \ldots, p_r$ such that $n_i | p_i - 1$. This follows from the following result of Dirichlet. □

Theorem 10.2.4.2 (Dirichlet)**.** *For a fixed positive integer n, there are infinitely many primes p such that $p \equiv 1 \mod n$.*

Appendix A

Additional material

A.1 Category theory

In this appendix, we introduce some terminology involving categories and functors. There are various possible definitions of categories.

A.1.1 Basic definitions

Before making the definition, we want to remember the examples whose properties we would like to abstract:

i) the class of sets, and functions between sets,

ii) the class of groups and homomorphisms between them,

iii) the class of abelian groups and homomorphisms between them,

iv) the class of topological spaces and continuous functions between them,

v) the class of smooth manifolds and smooth maps between them, and

vi) the class of all vector spaces and linear transformations between them,

In each situation above, we have written "class": there are difficulties in speaking of the set of all sets, and these difficulties propagate to each of the other notions. For these reasons, we have to be a bit careful writing about categories when using the language of set theory because we can very quickly leave the world of set theory.

Definition A.1.1.1. A *category* is a quadruple $\mathbf{C} = (Ob, Mor, id, \circ)$ consisting of

i) a class Ob whose members are called *objects in* $\mathbf{C}$,

ii) for each pair (A, B) of objects in $\mathbf{C}$, a set $Mor(A, B)$ whose members are called morphisms (in $\mathbf{C}$) from A to B,

iii) for each object A in $\mathbf{C}$, a morphism $id_A \in Mor(A, A)$ called the identity morphism, and

iv) for each triple (A, B, C) of objects in $\mathbf{C}$, a function $Mor(A, B) \times Mor(B, C) \to Mor(A, C)$ called *composition*

subject to the following axioms:

i) composition is associative, i.e., for any quadruple of objects (A, B, C, D) the following diagram commutes:

$$\begin{tikzcd}
Mor(A,B) \times Mor(B,C) \times Mor(C,D) \arrow[r, "id\times(-\circ-)"] \arrow[d, "(-\circ-)\times id"] & Mor(A,C) \times Mor(C,D) \arrow[d, "-\circ-"] \\
Mor(A,B) \times Mor(B,D) \arrow[r, "-\circ-"] & Mor(A,D).
\end{tikzcd}$$

ii) the morphism id_A acts as the identity with respect to composition, i.e., for any pair of objects (A, B) the following diagrams commute:

$$\begin{tikzcd}
Mor(A,B) \arrow[r, "id\times id_B"] \arrow[dr, "id"'] & Mor(A,B) \times Mor(B,B) \arrow[d, "\circ"] \\
& Mor(A,B)
\end{tikzcd}$$

and,

$$\begin{tikzcd}
Mor(A,B) \arrow[r, "id_A\times id"] \arrow[dr, "id"'] & Mor(A,A) \times Mor(A,B) \arrow[d, "\circ"] \\
& Mor(A,B)
\end{tikzcd}$$

iii) the sets $\mathrm{Hom}(A, B)$ are pairwise disjoint.

Remark A.1.1.2. There are various set-theoretic issues with the definitions that have been proposed above, and I would prefer at this stage if you think of the notion of category as simply an organizing principle, i.e., a way to talk about a kind of structure in a number of different settings. We have not required that the collection of objects forms a set and indeed it need not! E.g., if we look at $\mathbf{Set}$, we see that this need not be the case. Nevertheless, we have required that there is a set of morphisms between two objects; for practical reasons, we will sometimes relax this condition as well. Categories as we have defined them above are called *locally small*.

Example A.1.1.3. The empty category is the category with no objects and no morphisms. We write $\mathbf{1}$ for the category with exactly 1 object and only the identity morphism. Any partially ordered set P can be viewed as a category $\mathbf{P}$: objects of $\mathbf{P}$ correspond to elements of the set, and (besides the identity morphisms) given two elements x and y, there is a unique morphism $x \to y$ whenever $x < y$.

Example A.1.1.4. I leave it to you to check that the motivating "examples" are in fact examples of categories. We will write $\mathbf{Set}$ for the category of sets and functions, $\mathbf{Grp}$ for the category of groups and homomorphism, $\mathbf{Ab}$ for the category of abelian groups and homomorphism, $\mathbf{Top}$ for the category of topological spaces and continuous maps and we will introduce further categories as we proceed.

Example A.1.1.5 (The ordinal category). Let Δ be the category for which there is a single object $\mathbf{n}$ associated with each natural number n, and morphisms $\mathbf{m} \to \mathbf{n}$ are the order preserving functions from the totally ordered set $(0 < 1 < \cdots < m)$ to the totally ordered set $(0 < 1 < \cdots < n)$.

Example A.1.1.6 (The opposite category). If $\mathbf{C}$ is a category, then $\mathbf{C}^{\circ}$ is the category where "all morphisms are reversed." More precisely, the objects of $\mathbf{C}^{\circ}$ are precisely the objects of $\mathbf{C}$, but $hom_{\mathbf{C}^{\circ}}(A, B) = \mathrm{Hom}_{\mathbf{C}}(B, A)$ with composition in the opposite order.

Example A.1.1.7. Given any two categories $\mathbf{C}$ and $\mathbf{C}'$, one can form the product category $\mathbf{C} \times \mathbf{C}'$. The objects of $\mathbf{C} \times \mathbf{C}'$ are pairs (A, A') consisting of an object A in $\mathbf{C}$ and an object A' in $\mathbf{C}'$, and morphisms are pairs of morphisms (f, f') with $f : A \to B$ a morphism in $\mathbf{C}$ and $f' : A' \to B'$ a morphism in $\mathbf{C}'$. More generally, one can form the product of finitely many categories.

Definition A.1.1.8. If $\mathbf{C}$ is a category, a morphism $f : A \to B$ in $\mathbf{C}$ is called an isomorphism if there exists a morphism $f' : B \to A$ such that $f' \circ f = id_A$ and $f \circ f' = id_B$; in this case, f' will be called an *inverse* to f.

Lemma A.1.1.9. *If f is an isomorphism, then inverses are unique, i.e., if f' and f'' are inverses to f, then $f' = f''$.*

Example A.1.1.10. The identity morphism is always an isomorphism. In the category $\mathbf{Set}$, the isomorphisms are precisely the bijections. In the category $\mathbf{Grp}$ or $\mathbf{Ab}$, the isomorphisms are precisely the bijective group homomorphisms. In the category $\mathbf{Top}$, the isomorphisms are homeomorphisms, i.e., continuous functions with continuous inverse.

Example A.1.1.11. In $\mathbf{Top}$, there are bijective continuous maps with no continuous inverse. E.g., take $id : \mathbb{R} \to \mathbb{R}$, where the first copy is given the discrete topology and the second copy is given the usual topology. Since the only possible inverse here is the identity function, and the identity function takes singleton sets to singleton sets, it follows that the inverse function is not continuous.

Lemma A.1.1.12. *Composites of isomorphisms are isomorphisms.*

Remark A.1.1.13. It follows from what we've established above that "is isomorphic to" is an equivalence relation on objects.

Example A.1.1.14. Any group G may itself be viewed as a category: there is one object $*$, there is one isomorphism of $*$ for each element of G, and the composition is given by the multiplication in G.

A.1.2 Functors

The basic idea of category theory is that it gives a framework in which to consider objects of a particular type together. To allow us to do more than make "analogous" constructions in different settings, we should try to identify some idea of how to compare categories. Ideally, we would like to form a category whose objects are themselves categories! To do this, we need a way to relate different categories.

Definition A.1.2.1. If $\mathbf{C}$ and $\mathbf{C}'$ are categories, then a *functor* $F : \mathbf{C} \to \mathbf{C}'$ is a function that assigns to each object $A \in \mathbf{C}$ an object $F(A) \in \mathbf{C}'$, and to each morphism $f : A \to B$ in $\mathbf{C}$, a morphism $F(f) : F(A) \to F(B)$ in $\mathbf{C}'$, in such a way that

i) F preserves identity morphisms, i.e., for any object A, $F(id_A) = id_{F(A)}$, and

ii) F preserves composition, i.e., whenever given morphisms f and g such that $f \circ g$ is defined, $F(f \circ g) = F(f) \circ F(g)$.

Example A.1.2.2. If $\mathbf{C}$ is any category, there is always the identity functor $id_{\mathbf{C}} : \mathbf{C} \to \mathbf{C}$: assign to each object the same object, and to each morphism, the same morphism.

Example A.1.2.3. Consider $\mathbf{Grp}$ and the rule that assigns to a group G its underlying set, and to a homomorphism $f : G \to G'$ the underlying function of sets. This construction defines a functor $\mathbf{Grp} \to \mathbf{Set}$; this functor is called a "forgetful" functor because it forgets the additional structure on a group. Likewise, there are forgetful functors $\mathbf{Ab} \to \mathbf{Set}$, $\mathbf{Top} \to \mathbf{Set}$ (forget the topology), and $\mathbf{Ab} \to \mathbf{Grp}$ (forget that an abelian group is abelian).

Given two functors, we can compose them. For example, if we consider the functors $\mathbf{Ab} \to \mathbf{Grp}$ (forget that a group is abelian) and $\mathbf{Grp} \to \mathbf{Set}$ (forget the group structure), then we obtain a rule $\mathbf{Ab} \to \mathbf{Set}$ that coincides with the forgetful functor just mentioned.

Definition A.1.2.4. If $F : \mathbf{C} \to \mathbf{C}'$ and $F' : \mathbf{C}' \to \mathbf{C}''$ are functors, then the composite $F' \circ F : \mathbf{C} \to \mathbf{C}''$ defined by

$$(F' \circ F)(A \xrightarrow{f} B) := F'(F(A)) \overset{F'(F(f))}{\longrightarrow} F'(F(A'))$$

is also a functor.

Definition A.1.2.5. A functor $F : \mathbf{C} \to \mathbf{C}'$ is an isomorphism of categories, provided there is a functor $F' : \mathbf{C}' \to \mathbf{C}$ such that $F' \circ F = id_{\mathbf{C}}$ and..

Definition A.1.2.6. A functor $F : \mathbf{C} \to \mathbf{C}'$ is called *an embedding* provided that F is injective on morphisms,*faithful* (resp. full) if for any two objects A, A', the functions $F : \mathrm{Hom}(A, A') \to hom(F(A), F(A'))$ are injective (resp. surjective).

Example A.1.2.7. The forgetful functors $\mathbf{Grp} \to \mathbf{Set}$ and $\mathbf{Ab} \to \mathbf{Set}$ are both faithful, but neither is full (there are functions of the underlying sets that are not group homomorphisms). On the other hand, the functor $\mathbf{Ab} \to \mathbf{Grp}$ that forgets that a group is abelian is both full and faithful since the morphisms between two abelian groups are precisely group homomorphisms. Moreover, this latter functor is also an embedding.

Definition A.1.2.8. Given two categories $\mathbf{C}$ and $\mathbf{C}'$ and two functors $F_1, F_2 : \mathbf{C} \to \mathbf{C}'$, a *natural transformation* $\theta : F_1 \to F_2$ (or, equivalently, a morphism of functors) is a rule that assigns to each $A \in \mathbf{C}$, a morphism $\theta_A : F_1(A) \to F_2(A)$, such that for any morphism $f : A \to B$ in $\mathbf{C}$, the diagram

$$\begin{tikzcd} F_1(A) \arrow[r, "\theta_A"] \arrow[d, "F_1(f)"] & F_2(A) \arrow[d, "F_2(f)"] \\ F_1(B) \arrow[r, "\theta_B"] & F_2(B) \end{tikzcd}$$

commutes. Given a third functor $F_3 : \mathbf{C} \to \mathbf{C}'$ and a natural transformation $\theta' : F_2 \to \mathbf{F_3}$, we can define the composite natural transformation $\theta' \circ \theta : F_1 \to F_3$ by $(\theta' \circ \theta)_A := \theta'_A \circ \theta_A$.

Remark A.1.2.9. If $\mathbf{C}$ and $\mathbf{C}'$ are two categories, then we can consider $\mathbf{Fun}(\mathbf{C}, \mathbf{C}')$: objects are functors from $\mathbf{C}$ to $\mathbf{C}'$ and morphisms are natural transformations. This construct need not be a category in the sense that we have defined it for reasons of size. If the category $\mathbf{C}$ is restricted by requiring that it has a set of objects (i.e., it is small), then $\mathbf{Fun}(\mathbf{C}, \mathbf{C}')$ will actually be a category.

Example A.1.2.10. If $\mathbf{C}$ is any (small) category, then we can consider $\mathbf{Fun}(\mathbf{C}, \mathbf{Set})$. If A is any object of $\mathbf{C}$, then we know that $\mathrm{Hom}_{\mathbf{C}}(A, -)$ is a set. Moreover, given any morphism $f : D \to D'$ in $\mathbf{C}$, there is an induced function $\mathrm{Hom}_{\mathbf{C}}(A, D) \to \mathrm{Hom}_{\mathbf{C}}(A, D')$ induced by composition with f. Thus, any object in $\mathbf{C}$ defines a functor $\mathrm{Hom}(A, -) : \mathbf{C} \to \mathbf{Set}$.

If $f : A \to B$ is any morphism in $\mathbf{C}$, then there is an induced function

$$\mathrm{Hom}(f, -) : \mathrm{Hom}_{\mathbf{C}}(-, B) \longrightarrow \mathrm{Hom}_{\mathbf{C}}(-, A)$$

obtained by composing with f. It is straightforward to check that sending A to $\mathrm{Hom}_{\mathbf{C}}(A, -)$ and morphisms $f : A \to B$ to $\mathrm{Hom}_{\mathbf{C}}(f, -)$ defines a functor

$$\mathbf{C}^{\circ} \to \mathbf{Fun}(\mathbf{C}, \mathbf{Set}).$$

An object of $\mathbf{Fun}(\mathbf{C}, \mathbf{Set})$ isomorphic to one of the form $\mathrm{Hom}(A, -)$ is called a *representable* functor and A is called a representing object.

Lemma A.1.2.11. *The forgetful functor $F : \mathbf{Grp} \to \mathbf{Set}$ is representable by $\mathbb{Z}$.*

Proof. The forgetful functor sends a group H to its underlying set of elements and a group homomorphism $f : H \to H'$ to the underlying function of sets. The question: is the forgetful functor representable amounts to asking several questions. First: is there a group G such that for any group H, the set underlying H, i.e., the set of elements of H can be realized as the set of homomorphisms from G to H. The answer to this question already suggests that $\mathbb{Z}$ is the only possible answer (if the question can even be answered). Indeed, any element $h \in H$ determines a unique homomorphism $\mathbb{Z} \to H$, i.e., we form the cyclic subgroup generated by the element. Now, there are just many conditions to check. □

Definition A.1.2.12. A functor $F : \mathbf{C} \to \mathbf{C}'$ is called an *equivalence of categories* if there exists a functor $G : \mathbf{C}' \to \mathbf{C}$ and two isomorphisms of functors $\epsilon : FG \to Id_{\mathbf{C}'}$ and $\eta : Id_{\mathbf{C}} \to GF$. In this case, G is called a quasi-inverse of F, and F and G are together said to form a *mutually inverse equivalence of categories.*

Remark A.1.2.13. Using an appropriate form of the axiom of choice, one can show that if F is a functor that is full, faithful, and *essentially surjective*, i.e., if every object of $\mathbf{C}'$ is isomorphic to one of the form $F(A)$ for some $A \in \mathbf{C}$, then there exists a functor G and natural transformations ϵ and η making F an equivalence of categories. However, as is suggested by this sentences, there will be choices involved in the construction of these data, and so it is usually better to explicitly specify a quasi-inverse, if possible.

Example A.1.2.14. Suppose $\mathbf{C}$ is a category with 2 isomorphic objects (call them 1 and 2). Then the subcategory consisting of any single object is equivalent to the full category, but not isomorphic to it.

Adjoint functors

In Definition 1.5.2.1 and Theorem 1.5.2.3 we constructed a functor

$$F : \mathbf{Set} \longrightarrow \mathbf{Grp}$$

that assigns to a set S the free group $F(S)$ and to a function $f : S \to S'$ the (unique) homomorphism $F(f) : F(S) \to F(S')$. We also observed that for any group G,

$$\mathrm{Hom}_{\mathbf{Grp}}(F(S), G) = \mathrm{Hom}_{\mathbf{Set}}(S, G)$$

and suggested that this was an example of a pair of *adjoint functors*; we introduce this notion momentarily, after discussing some additional features of this example.

One may further observe that the identification just mentioned is *itself* suitably functorial. Indeed, suppose $f : S' \to S$ is a function, and $\varphi : G \to G'$ is a group homomorphism. The induced function $F(S') \to F(S)$ yields a natural transformation of functors $\mathrm{Hom}_{\mathbf{Grp}}(F(S), -) \longrightarrow \mathrm{Hom}_{\mathbf{Grp}}(F(S'), -)$. Then one may check that the following diagram commutes:

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbf{Grp}}(F(S), G) \arrow[r, equal] \arrow[d, "\mathrm{Hom}(F(f),\varphi)"] & \mathrm{Hom}_{\mathbf{Set}}(S, G) \arrow[d, "\mathrm{Hom}(f,\varphi)"] \\
\mathrm{Hom}_{\mathbf{Grp}}(F(S'), G') \arrow[r, equal] & \mathrm{Hom}_{\mathbf{Set}}(S', G);
\end{tikzcd}$$

the vertical arrows in this diagram are those obtained by composition. We may view $\mathrm{Hom}_{\mathbf{Grp}}(F(-), -)$ and $\mathrm{Hom}_{\mathbf{Set}}(-, -)$ as functors $\mathbf{Set}^{\circ} \times \mathbf{Grp} \to \mathbf{Set}$. The identifications of the above diagram then amount to an isomorphism of functors $\mathrm{Hom}_{\mathbf{Grp}}(F(-), -) \cong \mathrm{Hom}_{\mathbf{Set}}(-, -)$ in the sense of Definition A.1.2.8. With this observation, observe that the functors $F(-)$ (free group) and the forgetful functor yield an adjunction in the following sense.

Definition A.1.2.15. If $\mathbf{C}$ and $\mathbf{D}$ are two categories, an adjunction between $\mathbf{C}$ and $\mathbf{D}$ consists of a functor $F : \mathbf{D} \to \mathbf{C}$ (called the left adjoint) and $G : \mathbf{C} \to \mathbf{D}$ (called the right adjoint) together with an isomorphism of functors

$$\Phi : \mathrm{Hom}_{\mathbf{D}}(F(-), -) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{C}}(-, G(-)).$$

Remark A.1.2.16. The construction of free groups in Theorem 1.5.2.3 is actually a special case of a general results about the construction of adjoints to a given functor called *Freyd's adjoint functor theorem*. The two key steps in the proof of existence of free groups are (i) showing that $\mathfrak{D}$ is a set and (ii) constructing the free group as a subgroup of a huge direct product. In fact, variants of these two steps are the key ideas in proving the general adjoint functor theorem.

Example A.1.2.17. Just as with groups, the forgetful functor $\mathbf{Ab} \to \mathbf{Set}$ and the "free abelian group functor" $\mathbb{Z}[-] : \mathbf{Set} \to \mathbf{Ab}$ yield an adjunction between $\mathbf{Ab}$ and $\mathbf{Set}$.

Example A.1.2.18. The forgetful functor $\mathbf{Top} \to \mathbf{Set}$ admits both a left and right adjoint. For the left adjoint, define a functor as follows: send a set S to S viewed as a topological space with the discrete topology; since any function between two sets is a continuous map of discretely topologized spaces this is actually a functor. In fact, if S is a set and X is a topological space, then there is a bijection between functions $S \to X$ (forgetting the topology on X), and continuous maps $S \to X$ where S is given the discrete topology.

On the other hand, the forgetful functor also admits a *right* adjoint. To construct this, consider the functor that sends a set S to S equipped with the trivial topology (the only open sets are $\emptyset$ and S itself). In this case, continuous maps from a topological space X into a trivially topologized set S are in bijection between functions from X (forgetting the topology) to the set S.

Given an adjunction as in Definition A.1.2.15, for a given object $X \in \mathbf{C}$, the identity morphism of $id_{F(X)}$ thus corresponds to a morphism $X \to G(F(X))$; this morphism is functorial in X and yields a morphism of functors

$$\eta : id_{\mathbf{C}} \to G \circ F$$

called the *unit* of the adjunction. Similarly, for $Y \in D$, the identity map $id_{G(Y)}$ corresponds to a morphism $F(G(Y)) \to Y$; this morphism is again functorial in Y and corresponds to a natural transformation of functors

$$\epsilon : G \circ F \to id_{\mathbf{D}}$$

called the *counit* of the adjunction. These notions may be used to give a useful reformulation of a functor being fully-faithful.

Proposition A.1.2.19. *Suppose $F : \mathbf{C} \to \mathbf{D}$ and $G : \mathbf{D} \to \mathbf{C}$ and Φ is an adjunction between F and G.*

1. *The functor F is fully-faithful if and only if the unit of the adjunction is an isomorphism of functors.*
2. *The functor G is fully-faithful if and only if the counit of the adjunction is an isomorphism of functors.*

Proof. First, let us assume F is fully-faithful and show that the unit is an isomorphism of functors. If $X' \to G(F(X))$ is any morphism in $\mathbf{C}$, by adjunction, this corresponds to a morphism $F(X') \to F(X)$. Since F is fully-faithful, there exists a unique morphism $X' \to X$ yielding $F(X') \to F(X)$ after applying F. In other words, we conclude that $\mathrm{Hom}_{\mathbf{C}}(X', X) \to \mathrm{Hom}_{\mathbf{C}}(X', G(F(X)))$ is a bijection. Conversely, assume $id_{\mathbf{C}} \to G \circ F$ is a natural isomorphism. Then, $\mathrm{Hom}_{\mathbf{C}}(X, X') \to \mathrm{Hom}_{\mathbf{C}}(G(F(X)), G(F(X')))$ is a bijection. However, this function factors through the function $\mathrm{Hom}_{\mathbf{C}}(X, X') \to \mathrm{Hom}_{\mathbf{D}}(F(X), F(X'))$. Since the composite function is injective, it follows that $\mathrm{Hom}_{\mathbf{C}}(X, X') \to \mathrm{Hom}_{\mathbf{D}}(F(X), F(X'))$ is injective, i.e.., F is faithful. To conclude F is full, we need to construct a preimage for a given morphism $\gamma : F(X) \to F(X')$. I leave it as an exercise to write this down in terms of the unit and counit. □

Products and coproducts

In the category of sets, two basic constructions are Cartesian product and disjoin union of sets. One may characterize these sets in terms of universal properties, and observe that similar constructions exist in many categories.

Definition A.1.2.20. If $\mathbf{C}$ is a category, and X_1 and X_2 are two objects in $\mathbf{C}$, a *product* of X_1 and X_2 is an object $X_1 \times X_2$ such that there exist two morphisms $p_1 : X_1 \times X_2 \to X_1$ and $p_2 : X_1 \times X_2 \to X_2$ satisfying the following property: given any object Y in $\mathbf{C}$ and morphisms $f_1 : Y \to X_1$ and $f_2 : Y \to X_2$, there is a unique morphism $f : Y \to X_1 \times X_2$ such that the composite maps $Y \to \times X_1 \times X_2 \to X_i$ coincide with f_i, i.e., the following diagram commutes:

$$\begin{tikzcd}
& Y \arrow[dl, "f_2"'] \arrow[d, "f"] \arrow[dr, "f_1"] & \\
X_1 & X_1 \times X_2 \arrow[l, "p_1"] \arrow[r, "p_2"] & X_2.
\end{tikzcd}$$

More generally, if S is a set, then given objects $\{X_s\}_{s \in S}$ (i.e., a family of objects of $\mathbf{C}$ indexed by S), then an object $\prod_{s \in S} X_s$ is a product of $\{X_s\}_{s \in S}$ if there exist morphisms $p_s : \prod_{s \in S} X_s \to X_s$ such that for any object Y and morphisms $f_s : Y \to X_s$, there exists a unique morphism $f : Y \to \prod_{s \in S} X_s$ such that $f_s = p_s \circ f$ for every $s \in S$.

Example A.1.2.21. In the category of topological spaces, the Cartesian product (equipped with the product topology) is a product.

Example A.1.2.22. The Cartesian product is a product in the categories $\mathbf{Grp}$ and $\mathbf{Ab}$.

Example A.1.2.23. The product of two objects need not exist in a category. For example, in the category of fields, there exist no product between fields having different characteristic. In fact, even restricting attention to fields of the same characteristic, the a product of a field with itself does not exist in the category of fields.

Definition A.1.2.24. If $\mathbf{C}$ is a category, and X_1 and X_2 are objects of $\mathbf{C}$, then an object $X_1 \sqcup X_2$ is called a *coproduct* or *sum* of X_1 and X_2 if there exist morphisms $i_1 : X_1 \to X_1 \sqcup X_2$ and $i_2 : X_2 \to X_1 \sqcup X_2$ such that for any object Y and morphisms $f_1 : X_1 \to Y$ and $f_2 : X_2 \to Y$, there exists a unique morphism $X_1 \sqcup X_2 \to Y$ such that $X_i \to X_1 \sqcup X_2 \to Y$ coincides with f_i, i.e., the following diagram commutes:

$$\begin{tikzcd}
X_1 \arrow[r, "i_1"] \arrow[dr, "f_1"'] & X_1 \sqcup X_2 \arrow[d, "f"] & X_2 \arrow[l, "i_2"'] \arrow[dl, "f_2"] \\
& Y. &
\end{tikzcd}$$

More generally, if S is a set, then given objects $\{X_s\}_{s\in S}$ (i.e., a family of objects of $\mathbf{C}$ indexed by S), then an object $\coprod_{s\in S} X_s$ is a coproduct of $\{X_s\}_{s\in S}$ if there exist morphisms $i_s : X_s \to \coprod_{s\in S} X_s$ such that for any object Y and morphisms $f_s : X_s \to Y$, there exists a unique morphism $f : \coprod_{s\in S} X_s \to Y$ such that $f_s = f \circ i_s$ for every $s \in S$.

Example A.1.2.25. The coproduct of abelian groups is the direct sum, and usually denoted $\oplus$ instead of $\sqcup$. The coproduct in the category of groups is the amalgamated sum (or free product with amalgamation), denoted $G_1 * G_2$.

A.1.3 Additive categories

It frequently happens that the set of morphisms between two objects in a category has additional structure and that maps between morphism sets preserve this additional structure. For example, if we work in the category $\mathbf{Ab}$, then the set of homomorphisms between two abelian groups has the structure of an abelian group with respect to pointwise addition. The maps between morphism sets will, additionally, be group homomorphisms. For another example, consider the category $\mathbf{Top}$. In the case, the set of continuous maps $f : X \to Y$ can be topologized and thus the morphism sets can be equipped with the structure of topological spaces themselves. Systematizing this "additional structure" in a category is the domain of enriched category theory.

Definition A.1.3.1. A category $\mathbf{C}$ is called an $\mathbf{Ab}$-*category* if, given any two objects $A, A' \in \mathbf{C}$, $\mathrm{Hom}_{\mathbf{C}}(A, A')$ is an abelian group, and given any three objects A, A', A'', the composition map

$$- \circ - : \mathrm{Hom}_{\mathbf{C}}(A, A') \times \mathrm{Hom}_{\mathbf{C}}(A', A'') \longrightarrow \mathrm{Hom}_{\mathbf{C}}(A, A'')$$

is $\mathbb{Z}$-bilinear, i.e., given any pair of integers n_1, n_2 and morphisms $f_1, f_2 : A \to A'$ and morphisms $g_1, g_2 : A' \to A''$, we have $(n_1 f_1 + n_2 f_2) \circ - = n_1(f_1 \circ -) + n_2(f_2 \circ -)$ and $- \circ (n_1 g_1 + n_2 g_2) = n_1(- \circ g_1) + n_2(- \circ g_2)$.

Example A.1.3.2. The category of abelian groups is, by construction, an $\mathbf{Ab}$-category. However, we can also consider $\mathbf{Ab}^{fg}$ of finitely generated abelian groups, $\mathbf{Ab}^{tor}$ of torsion groups or $\mathbf{Ab}^{f}$ of finite abelian groups.

In the category of abelian groups, we can form sums and products of abelian groups. The universal property of the cartesian product makes sense in any category.

Definition A.1.3.3. Suppose $\mathbf{C}$ is a category and A and B are two objects of $\mathbf{C}$. An object P is called a *product* of A and B, if there exist two morphisms $p_A : P \to A$ and $p_B : P \to B$ (called projections) such that, given any object D and two morphisms $f_A : D \to A$ and $f_B : D \to B$, there exists a unique morphism $\varphi : D \to P$ such that map $D \to A$ is the composite $D \to P \to A$ and the map $D \to B$ is the composite $D \to P \to B$. An object S is called a *coproduct* (or *sum*) of A and B, if there exist two morphisms $i_A : A \to S$ and $i_B : B \to S$ such that, given any object D and two morphisms $f_A : A \to D$ and $f_B : B \to D$, there exists a unique morphism $S \to D$ such that f_A is the composite $A \to S \to D$ and f_B is the composite $B \to S \to D$.

Remark A.1.3.4. Slightly more generally, one can define the fiber product of two morphisms $f_1 : A_1 \to B$ and $f_2 : A_2 \to B$...

Example A.1.3.5. In the category $\mathbf{Grp}$, we showed that the Cartesian product is a product, while the amalgamated sum is a sum. If $\mathbf{Grp}^{fin}$ is the category of finite groups, then it is straightforward to check that products of pairs of elements always exist in $\mathbf{Grp}^{fin}$. However, it is harder to see that this category does not always have sums.

The category of abelian groups also has a distinguished object, namely the abelian group 0. Given any abelian group A, there is a unique morphism from the trivial group 0 to A and, conversely, a unique morphism from A to the trivial group. The trivial group also has the property that is product or sum with any other abelian group is the identity.

Definition A.1.3.6. Suppose $\mathbf{C}$ is a category. An object I is called an *initial object of* $\mathbf{C}$ if, given any object $A \in \mathbf{C}$, there is a unique morphism $I \to A$. An object T is called *a terminal object of* $\mathbf{C}$ if, given any object $A \in \mathbf{C}$, there is a unique morphism $A \to T$. An object 0 of $\mathbf{C}$ is called a zero object if it is both initial and terminal.

Example A.1.3.7. In the category of groups, the trivial group is a zero object. In the category of sets, the empty set is the initial object and any singleton set is a final object. In the category of topological spaces, the empty category is an initial object and the singleton topological space is a final object. The latter two categories do not possess a zero object.

Definition A.1.3.8. An $\mathbf{Ab}$-category $\mathbf{C}$ is called *additive* if (i) it has a zero object, and (ii) the sum and product of any pair of objects exists.

Remark A.1.3.9. Note that $\mathbf{Grp}$ satisfies (i) and (ii) above. You can show that there is no way to equip $\mathbf{Grp}$ with the structure of an additive category.

Example A.1.3.10. Of course, the category of abelian groups is an additive category.

Example A.1.3.11. Show that the category of finite abelian groups, the category of finitely generated abelian groups, and the category of torsion abelian groups are all additive categories.

Definition A.1.3.12. If $\mathbf{C}$ and $\mathbf{C}'$ are additive categories, a functor $F : \mathbf{C} \to \mathbf{C}'$ is called *additive* if, given any two morphisms $u, v : A \to B$, $F(u + v) = F(u) + F(v) \in \mathrm{Hom}_{\mathbf{C}'}(F(A), F(B))$. If $\mathbf{C}$ is small, write $\mathbf{Fun}^{add}(\mathbf{C}, \mathbf{C}')$ for the category of additive functors from $\mathbf{C}$ to $\mathbf{C}'$.

Lemma A.1.3.13. *If $\mathbf{C}$ is a small category, the functor category $\mathbf{Fun}(\mathbf{C}^{\circ}, \mathbf{Ab})$ has the structure of an additive category.*

A.1.4 Abelian categories

If $f : A \to B$ is a homomorphism of abelian groups, then f has a kernel, which is an object that allows us to determine whether f is a monomorphism.

If a category $\mathbf{C}$ has a zero object, then given any pair of objects A and B, there is always a distinguished morphism from A to B, namely the morphism $A \to 0 \to B$; this morphism will be referred to as the zero morphism and we will sometimes write $0 : A \to B$ for this morphism.

Definition A.1.4.1. If $\mathbf{C}$ is a category with a zero object, and $f : A \to B$ is a morphism in $\mathbf{C}$, a kernel of f is any morphism $k : K \to A$ such that (i) $f \circ k$ is the zero morphism from $K \to B$, and (ii) given any morphism $k' : K \to A$ such that $f \circ k'$ is the zero morphism, there is a unique morphism $u : K' \to K$ such that $k \circ u = k'$.

Example A.1.4.2. The kernel of a homomorphism of abelian groups is a kernel in the above sense.

Lemma A.1.4.3. *If $\mathbf{C}$ is a category with a zero object, and $f : A \to B$ is any morphism in $\mathbf{C}$, then the kernel of f, if it exists, is the fiber product of $f : A \to B$ and $0 : A \to B$.*

In the definition above, you can reverse the order of the arrows as well and obtain the following definition.

Definition A.1.4.4. If $\mathbf{C}$ is a category with zero object, and $f : A \to B$ is a morphism in $\mathbf{C}$, a *cokernel* of f is any morphism $c : B \to C$ such that (i) $c \circ f$ is the zero morphism from $A \to C$, and (ii) given any morphism $c' : B \to C'$ such that $c' \circ f$ is the zero morphism, there is a unique morphism $u : C \to C'$ such that $u \circ c = c'$.

Lemma A.1.4.5. *If $f : A \to B$ is a homomorphism of abelian groups, the map $B \to B/im(A)$ is a cokernel for f.*

Example A.1.4.6. With this modified definition, in the category of groups, kernels of morphisms exist and are given by the inclusion of the group theoretic kernel. Cokernels exist here as well: given a homomorphism $f : G \to H$, there is always a map $H \to H/N(im(G))$ (the quotient of H by the normal closure of the image).

In the category of abelian groups, given a morphism $f : A \to B$, we can speak of the image of f, which is a subgroup of B. By means of the isomorphism theorems, we can identify $im(f)$ with $A/\ker(f)$. This suggests the following definition of the image of a morphism.

Definition A.1.4.7. If $\mathbf{C}$ is an additive category, then suppose $f : A \to B$ is a morphism and that a kernel k of f exists. The coimage of f, denoted $coim(f)$, is a cokernel of k, if it exists.

Again, we can reverse the arrows to get a related definition.

Definition A.1.4.8. If $\mathbf{C}$ is an additive category, then suppose $f : A \to B$ is a morphism and that a cokernel c of f exists. The *image* of f, denoted $im(f)$ is a kernel of c, if it exists.

Lemma A.1.4.9. *If $\mathbf{C}$ is an additive category, and $f : A \to B$ is a morphism in $\mathbf{C}$, then the following statements hold.*

1. *If a kernel of f exists, then this kernel is a monomorphism.*
2. *If a cokernel of f exists, then this cokernel is an epimorphism.*
3. *If a kernel and coimage of f exist, then the coimage is an epimorphism.*
4. *If a cokernel and image of f exist, then the image is a monomorphism.*

Proof. Exercise. □

Lemma A.1.4.10. *If* $\mathbf{C}$ *is an additive category, and if* $f : A \to B$ *is a morphism such that* $im(f)$ *and* $coim(f)$ *both exist, then there exists a unique morphism* $coim(f) \to im(f)$ *such that* f *factors as* $A \to coim(f) \to im(f) \to B$*.*

Proof. Exercise. □

Definition A.1.4.11. An additive category $\mathbf{C}$ is called *abelian* if

i) Any morphism $f \in \mathbf{C}$ has a kernel and a cokernel, and

ii) The unique map $coim(f) \to im(f)$ (guaranteed to exist by the preceding lemma) is an isomorphism.

Proposition A.1.4.12. *The category of (finite, finitely generated, torsion,* p*-torsion) abelian groups is an abelian category.*

Proposition A.1.4.13. *If* F *is a field, the category* $\mathbf{Vec}_F$ *of (finite-dimensional)* F*-vector spaces is an abelian category.*

Proposition A.1.4.14. *If* $\mathbf{C}$ *is any small category, the functor category* $\mathbf{Fun}(\mathbf{C}^\circ, \mathbf{Ab})$ *is an abelian category.*

A.1.5 Exact sequences

In the category of abelian groups, every injective homomorphism is the kernel of a group homomorphism. We can formalize this observation as the following definition.

Definition A.1.5.1. If $\mathbf{C}$ is an additive category, and $f : A \to B$ is a morphism that is the kernel of some morphism $B \to C$, then A is called a normal subobject of A. We will say that $\mathbf{C}$ is *normal* if every monomorphism is the kernel of some morphism.

There is a corresponding dual definition.

Definition A.1.5.2. If $\mathbf{C}$ is an additive category, and $f : B \to C$ is a morphism that is the cokernel of some morphism $A \to B$, then C is called a conormal quotient object of B. We will say that $\mathbf{C}$ is *conormal* if every epimorphism is the cokernel of some morphism.

A.2 Group cohomology and Schreier's theory of extensions

The goal of this section is to complete the analysis of extensions that was started in Lecture 5.2. To do this, we need some more information from group cohomology.

A.2.1 Group cohomology with abelian coefficients

Suppose G is a group, A is an abelian group, and $\omega : G \to Aut(A)$ is an action of G on A. We defined the cohomology group $H^2(G, A, \omega)$ earlier, and the notation was chosen because the object under consideration was a special case of a more general construction, which we now expose. First, let us fix some notation.

Group cohomology: first definitions

As before, if S is a set and H is any group, we write $Fun(S, H)$ for the set of functions from $S \to H$; this set inherits a group structure with multiplication and inversion defined "pointwise", i.e., via the formula $(f_1f_2)(s) = f_1(s)f_2(s)$ and $(f_1^{-1})(s) = f_1(s)^{-1}$, and unit given by the constant function $1(s) = 1 \in H$. When H is abelian, we will write 0 for the identity element of $Fun(s, H)$.

Assume now that G is a group, and A is an abelian group equipped with an action of G via a homomorphism $\omega : G \to Aut(A)$. For each $n \geq 0$, set $C^n(G, A, \omega) := Fun(G^n, A)$, and define a function

$$d^n : C^n(G, A, \omega) \longrightarrow C^{n+1}(G, A, \omega)$$

by means of the formula

$$\begin{aligned} d^n(\varphi)(g_1, \ldots, g_n) =& \omega_{g_1}\varphi(g_2, \ldots, g_{n+1}) \\ &+ \sum_{i=1}^{n}(-1)^i\varphi(g_1, \ldots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \ldots, g_{n+1}) \\ &+ (-1)^{n+1}\varphi(g_1, \ldots, g_n). \end{aligned}$$

This formula makes sense for $n = 0$ as well if one takes it to mean that the sum in the middle does not appear. We will explain this in more detail in Example A.2.1.4. The formula for $n = 1$ and 2 was discussed in (5.2.2) and (5.2.1). The proof of Lemma 5.2.1.1 shows that d^n is always a homomorphism of abelian groups. Generalizing the observation that $d^2 \circ d^1 = 0$, we have the following result.

Lemma A.2.1.1. *The composite $d^{n+1} \circ d^n = 0$.*

Proof. We check this by directly plugging into the formulas. □

The pair $(C^*(G, A), d^*)$ is an example of a *cochain complex* of abelian groups: the morphisms d^i are called the differentials of the chain complex. Because the formula $d^{n+1} \circ d^n = 0$ holds, it follows that the image of d^{n-1} is contained in the kernel of d^n. Expanding the purview of Definition 5.2.1.4 we make the following definition.

Definition A.2.1.2. Suppose G is a group, and A is an abelian group on which G acts by means of a homomorphism $\omega : G \to A$ (briefly, we will say that A is a G-module). We define the group of *n-cocycles of G with coefficients in* (A, ω), the group of *n-coboundaries of G with coefficients in* (A, ω) and the *n-th cohomology of G with coefficients in* (A, ω) by means of the following formulas:

$$\begin{aligned} Z^n(G, A, \omega) &:= Ker(d^n : C^n(G, A, \omega) \to C^{n+1}(G, A, \omega)), \\ B^n(G, A, \omega) &:= Im(d^{n-1} : C^{n-1}(G, A) \to C^n(G, A)), \text{ and} \\ H^n(G, A, \omega) &:= Z^n(G, A, \omega)/B^n(G, A, \omega). \end{aligned}$$

Remark A.2.1.3. In fact, cohomology as defined above is naturally functorial in several ways. First, if $f : S \to S'$ is any function of sets, then precomposition with f defines a function $Fun(S', A) \to Fun(S, A)$. Given a homomorphism $\varphi : G \to G'$, there are induced homomorphisms $G^n \to (G')^n$ given by φ^n. Thus, φ defines homomorphisms $C^n(G', A, \omega) \to C^n(G, A, \omega)$. On the other hand, any G'-module (A, ω) gives rise to a G-module $(A, \varphi \circ \omega)$. The homomorphisms d^n for (G, A, ω) commute with those for (G', A, ω) in the sense that for any integer n the following diagram commutes

$$\begin{tikzcd}
C^n(G', A, \omega) \arrow[r, "d^n"] \arrow[d, "\varphi^n"] & C^{n+1}(G', A, \omega) \arrow[d, "\varphi^{n+1}"] \\
C^n(G, A, \omega) \arrow[r, "d^n"] & C^{n+1}(G, A, \omega).
\end{tikzcd}$$

One checks that there are induced homomorphisms $\varphi^* : H^n(G', A, \omega) \to H^n(G, A, \varphi \circ \omega)$, which are suitably compatible with composition of group homomorphisms.

Cohomology in low degrees

Example A.2.1.4. Note that $G^0 = 1$, so $Fun(1, A)$ is isomorphic to A since specifying an element of $Fun(1, A)$ is equivalent to specifying an element of A. In this case, the differential d^0 is given by the formula

$$d^0(\varphi) = \omega_{g_1}\varphi - \varphi.$$

The kernel of $d^0(\varphi)$ thus consists of elements of A (considered with action of G via ω) that satisfy $\omega_{g_1}\varphi = \varphi$ for every $g_1 \in G$, i.e., it consists of elements in A that are *fixed* by G; this subgroup of A is typically denoted A^G.

The semi-direct product is an example of an extension. Indeed, suppose $\omega : Q \to Aut(A)$ is a homomorphism, and we form $A \rtimes_\varphi Q$. By construction, A is a normal subgroup of $A \rtimes_\varphi Q$ with quotient Q. As a set $A \rtimes_\varphi Q$ is simply a Cartesian product. Now, suppose we choose a section $s : Q \to A \rtimes_\varphi Q$ that is a group homomorphism (we know that such things always exist).

Suppose $s' : Q \to A \rtimes_\varphi Q$ is another section that is also a group homomorphism. In that case, there exists a function $h : Q \to A$ such that $s' = hs$: indeed, the section gives an element of each coset, and two elements in a coset differ by an element of A. Now, let us observe that properties h necessarily has.

$$s'(qq') = s'(q)s'(q') = h(q)s(q)h(q')s(q') = h(q)s(q)h(q')s(q)^{-1}s(q)s(q') = h(q)\omega_q h(q')s(qq').$$

On the other hand, $s'(qq') = h(qq')s(qq')$. Thus, we conclude that $h(qq') = h(q)\omega_q(h(q'))$. Now, h is a function $Q \to A$. Since the factor set associated with s or s' is trivial, we conclude that 2-cocycle associated with h is trivial. Thus, $h : Q \to A$ is an example of what we call a 1-cocycle.

If we conjugate s by an element $a \in A$, we obtain another section $s' : Q \to A \rtimes_\varphi Q$ which is again a homomorphism. In that case $s'(q) = as(q)a^{-1} = h(a)s(q)$. Thus,

$$as(q)a^{-1} = as(q)a^{-1}s(q)^{-1}s(q) = a\omega_q(a^{-1})s(q),$$

and so $h(q) = a\omega_q(a^{-1})$.

Theorem A.2.1.5. *If Q is a group, and $\omega : G \to Aut(A)$ is a homomorphism, then $H^1(Q, A, \omega)$ is the set of splittings of $A \rtimes_\varphi Q \to Q$, modulo sections that differ by conjugation by an element of A.*

A.2.2 Extensions, and generalized cocycles

We begin by associating some data with an arbitrary extension. Given a short exact sequence of groups of the form

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} Q \longrightarrow 1,$$

the conjugation action of G on N gives rise to a homomorphism $G \to Aut(N)$. If we pick a (set-theoretic) section $\theta : Q \to G$ of the homomorphism π, then there is an associated function $\tilde{\omega} : Q \to Aut(N)$ given by the formula

$$\tilde{\omega}_q(n) = \theta(q)n\theta(q)^{-1}.$$

Note that if θ' is another section, then we get a possibly different $\tilde{\omega}' : Q \to Aut(N)$.

Let us compare $\tilde{\omega}$ and $\tilde{\omega}'$. To this end, define ψ to measure the difference between θ and θ': $\theta(q) = \psi(q)\theta'(q)$. Since $\theta(q)$ and $\theta'(q)$ are both sent to q under π, it follows that

$$1_Q = \pi(\theta(q)\theta'(q)^{-1}) = \pi(\psi(q)),$$

i.e., $\psi(q)$ is contained in $N = \ker(\pi)$.

In that case,

$$\tilde{\omega}_q(n) = \theta(q)n\theta(q)^{-1} = \psi(q)\theta'(q)n\theta'(q)^{-1}\psi^{-1}(q),$$

and therefore $\tilde{\omega}_q$ is $\tilde{\omega}'_q$ followed by conjugation by $\psi(q)$, which as we observed above lies in N.

If N is a group, then $Inn(N)$ is the subgroup of $Aut(N)$ given by conjugation by elements of N. The group $Inn(N)$ is a normal subgroup of $Aut(N)$, and we set $Out(N) := Aut(N)/Inn(N)$; elements of $Out(N)$ are referred to as outer automorphisms. When N is abelian, conjugation is trivial, i.e., $Inn(N)$ is trivial, so the map $Aut(N) \to Out(N)$ is an isomorphism. The computation of the previous paragraph shows that while ω and ω' define *a priori* different functions $Q \to Aut(N)$, the composites of ω and ω' with the homomorphism $Aut(N) \to Out(N)$ are independent of the choice of section θ. We summarize what we have established in the following lemma.

Lemma A.2.2.1. *Suppose $1 \to N \to G \xrightarrow{\pi} Q \to 1$ is a short exact sequence of abelian groups. A choice of (set-theoretic) section $\theta : Q \to G$ of the homomorphism π defines a function $\tilde{\omega} : Q \to Aut(N)$, and the class ω of the composite of $\tilde{\omega}$ with $Aut(N) \to Out(N)$ is independent of the choice of θ (i.e., any other choice of set-theoretic section gives rise to the same function).*

As in class, we may measure the extent to which θ fails to be a group homomorphism by defining a function f that measures this failure, i.e., we define

$$f(q_1, q_2) := \theta(q_1)\theta(q_2)\theta(q_1q_2)^{-1}.$$

or, equivalently,

$$\theta(q_1)\theta(q_2) = f(q_1, q_2)\theta(q_1q_2),$$

Since θ is a section of π, we conclude that $\pi(f(q_1, q_2)) = 1$ and thus that f is a function $Q \times Q \to N$.

Since θ is not assumed to be a group homomorphism, there is no reason for the composite map $Q \xrightarrow{\theta} G \longrightarrow Aut(N)$ to be one either. Thus, let us also measure the extent to which this composite fails to be a group homomorphism. Since $\theta(q_1)\theta(q_2) = f(q_1, q_2)\theta(q_1q_2)$ by definition, it follows that

$$\begin{aligned}\tilde{\omega}_{\theta(q_1)}\tilde{\omega}_{\theta(q_2)}(n) &= \theta(q_1)\theta(q_2)n\theta(q_2)^{-1}\theta(q_1)^{-1} = f(q_1, q_2)\theta(q_1q_2)n\theta(q_1q_2)^{-1}f(q_1, q_2)^{-1} \\ &= \tilde{\omega}_{f(q_1,q_2)}\tilde{\omega}_{q_1q_2}(n),\end{aligned}$$

in other words,

$$\tilde{\omega}_{\theta(q_1)}\tilde{\omega}_{\theta(q_2)} = \tilde{\omega}_{f(q_1,q_2)}\tilde{\omega}_{q_1q_2}$$

Since $f(q_1, q_2)$ lies in N it follows $\tilde{\omega}_{f(q_1,q_2)}$ is an inner automorphism in N. In other words, the composite $\omega : Q \to Out(N)$ of $\tilde{\omega}$ and $Aut(N) \to Out(N)$ *is* a group homomorphism; we summarize this in the following result.

Lemma A.2.2.2. *If* $1 \to N \to G \xrightarrow{\pi} Q \to 1$ *is a short exact sequence of abelian groups, then the associated function* $\omega : G \to Out(N)$ *from* Lemma A.2.2.1 *is a homomorphism.*

Remark A.2.2.3. When N is abelian, it follows that $Aut(N) = Out(N)$, and so $\omega : G \to Out(N)$ is the same homomorphism we considered in the text.

We now want to analyze restrictions on f as in the main body of the text. The discussion is slightly more subtle than what in the case N is abelian because the "intrinsic" homomorphism ω that appears in Lemma A.2.2.2 is a function $Q \to Out(N)$. Unlike the abelian case, it is not this "intrinsic" homomorphism that appears in the condition on f imposed by associativity of the group structure in the extension. Instead, that cocycle condition depends on the function $\tilde{\omega} : G \to Aut(N)$ (that one obtains from choice of a splitting) that induces $\omega : G \to Out(N)$.

Let us repeat the computation involving associativity of the group operation, which yielded a condition on f:

$$\begin{aligned}\theta(q_1)\theta(q_2)\theta(q_3) &= f(q_1, q_2)\theta(q_1q_2)\theta(q_3) = f(q_1, q_2)f(q_1q_2, q_3)\theta(q_1q_2q_3) \\ &= \theta(q_1)f(q_2, q_3)\theta(q_2q_3) = \theta(q_1)f(q_2, q_3)\theta(q_1)^{-1}\theta(q_1)\theta(q_2q_3) \\ &= \tilde{\omega}_{q_1}(f(q_2, q_3))(f(q_1, q_2q_3))\theta(q_1q_2q_3).\end{aligned}$$

In other words, the formula

$$f(q_1, q_2)f(q_1q_2, q_3) = \tilde{\omega}_{q_1}(f(q_2, q_3))(f(q_1, q_2q_3))$$

holds.

If we pick a different section θ', with $\tilde{\omega}'$ the associated function $Q \to Aut(N)$, then there is an associated function $f' : Q \times Q \to N$. If ψ measures the difference between θ and θ', i.e., if $\theta(q) = \psi(q)\theta'(q)$, then as we saw before, $\tilde{\omega}_q$ is equal to $\tilde{\omega}'_q$ followed by conjugation by $\psi(q)$.

Observe that

$$\begin{aligned}f(q_1, q_2)\psi(q_1q_2)\theta'(q_1q_2) &= \psi(q_1)\theta'(q_1)\psi(q_2)\theta'(q_2) = \psi(q_1)\theta'(q_1)\psi(q_2)\theta'(q_1)^{-1}\theta'(q_1)\theta'(q_2) \\ &= \psi(q_1)\tilde{\omega}'_{q_1}(\psi(q_2))f'(q_1, q_2)\theta'(q_1q_2).\end{aligned}$$

In other words, the formula

$$f(q_1, q_2) = \psi(q_1)\tilde{\omega}'_{q_1}(\psi(q_2))f'(q_1, q_2)\psi(q_1q_2)^{-1} \tag{A.2.1}$$

holds.

We can summarize the discussion so far as follows. If

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} Q \longrightarrow 1$$

is an extension, then choice of a section θ of π allows us to attach to the extension a pair $(\tilde{\omega}, f)$ where

- $\tilde{\omega} : Q \to Aut(N)$ is a function such that the induced function $\omega : Q \to Out(N)$ obtained by composition with $Aut(N) \to Out(N)$ is a homomorphism and

- $f : Q \times Q \to N$ is a function satisfying the generalized cocycle condition
  - $f(q_1, q_2)f(q_1q_2, q_3) = \tilde{\omega}_{q_1}(f(q_2, q_3))(f(q_1, q_2q_3))$.

A different choice of section θ' yields a different pair $(\tilde{\omega}', f')$ related to the original pair in the following way: there is a function $\psi : Q \to N$, such that $\tilde{\omega}$ is equal to $\tilde{\omega}'$ followed by composition with conjugation by $\psi(q)$, and the composite $\omega' : Q \to Aut(N)$ coincides with ω and f is related to f' by the condition in (A.2.1).

We may see that the relation implicit in the above is an equivalence relation. In fact, we will construct a group action on the data described above. Let $r(Q, N)$ be the set of functions $\tilde{\omega} : Q \to Aut(N)$ such that $\omega : Q \to Out(N)$ is a group homomorphism. We claim that $Fun(Q, N)$ acts naturally on $r(Q, N)$. Indeed, given ψ, there is an induced function $Q \to Inn(N)$ sending ψ to its composite with the homomorphism $N \to Inn(N)$; we write c_ψ for this function. One checks that this formula defines an action of $Fun(Q, N)$ on $Fun(Q, Aut(N))$, and since the composite of c_ψ with the function $Aut(N) \to Out(N)$ is the trivial function, it follows that the action preserves the subset $r(Q, N)$ of $Fun(Q, Aut(N))$ and thus restricts to an action on this subset.

Similarly, the formula of (A.2.1) yields an action of $Fun(Q, N)$ on $Fun(Q \times Q, N)$, and it is straightforward to check that granted the action of $Fun(Q, N)$ on $r(Q, N)$ described in the previous paragraph, there is an induced action of $Fun(Q, N)$ on the set of pairs $(\tilde{\omega}, f)$ where $\tilde{\omega}$ is an element of $r(Q, N)$ and f satisfies the generalized cocycle condition. When N is abelian, this action corresponds to the differential d^2 defined above.

In fact, the action of $Fun(Q, N)$ on the set of such pairs defines an equivalence relation: two pairs $(\tilde{\omega}, f)$ and $(\tilde{\omega'}, f')$ are equivalent if $\tilde{\omega}$ and $\tilde{\omega'}$ both yield the same homomorphism $\omega : Q \to Out(N)$, and if they lie in the same orbit for the action of $Fun(Q, N)$. Putting everything together, we have thus established the following result.

Theorem A.2.2.4. *There is an equivalence between the set of extensions of the form*

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} Q \longrightarrow 1$$

inducing a fixed $\omega : Q \to Out(N)$, and the set of orbits of $Fun(Q, N)$ on the set of pairs $(\tilde{\omega}, f)$, where $\tilde{\omega} : Q \to Aut(N)$ is a function such that the composite with $Aut(N) \to Out(N)$ coincides with ω, and $f : Q \times Q \to N$ is a function satisfying the generalized cocycle condition.

A.2.3 Obstructions and cohomological descriptions of extensions

This description is explicit, but lacks the calculational power present in the situation when N is abelian. Furthermore, a couple of questions arise naturally from the form of the answer. First, which homomorphisms $\omega : Q \to Out(N)$ arise from an extension of Q by N? Second, is there a more tractable description of the set of extensions than that given above in terms of generalized cocycles? In fact, we can answer both of these questions rather explicitly.

Obstructions to the existence of extensions

Suppose we begin with a homomorphism $\omega : Q \to Out(N)$. Since the homomorphism $Aut(N) \to Out(N)$ is surjective, we may always choose a function $\tilde{\omega} : Q \to Aut(N)$ lifting ω.

Now, $\tilde{\omega}$ may fail to be a group homomorphism, but we may measure its failure to do so by defining

$$c(q_1, q_2) = \tilde{\omega}_{q_1}\tilde{\omega}_{q_2}\tilde{\omega}^{-1}_{q_1q_2}.$$

Since ω is a group homomorphism, we conclude that $c(q_1, q_2)$ is an element of $Inn(N)$. In other words, $c(q_1, q_2)$ defines a function

$$c : Q \times Q \to Inn(N).$$

In the situation where we actually had an extension of Q by N, the function $c(q_1, q_2)$ was precisely the inner automorphism defined by conjugation by $f : Q \times Q \to N$.

Note that $Aut(N)$ acts on $Inn(N)$ by conjugation since $Inn(N)$ is a normal subgroup of $Aut(N)$. We claim that $c(q_1, q_2)$ satisfies the generalized cocycle condition. Indeed,

$$c(q_1, q_2)c(q_1q_2, q_3) = (\tilde{\omega}_{q_1}\tilde{\omega}_{q_2}\tilde{\omega}^{-1}_{q_1q_2})(\tilde{\omega}_{q_1q_2}\tilde{\omega}_{q_3}\tilde{\omega}^{-1}_{q_1q_2q_3})$$

while

$$\tilde{\omega}_{q_1}(c(q_2, q_3))(c(q_1, q_2q_3)) = (\tilde{\omega}_{q_1}(\tilde{\omega}_{q_2}\tilde{\omega}_{q_3}\tilde{\omega}^{-1}_{q_2q_3}))\tilde{\omega}^{-1}_{q_1})(\tilde{\omega}_{q_1}\tilde{\omega}_{q_2q_3}\tilde{\omega}^{-1}_{q_1q_2q_3})$$

and simplifying we see that both sides are equal to $\tilde{\omega}_{q_1}\tilde{\omega}_{q_2}\tilde{\omega}_{q_3}\tilde{\omega}^{-1}_{q_1q_2q_3}$. However, this observation does not solve our problem in general because $H \to Inn(H)$ is not always an isomorphism.

Indeed, there is a surjective group homomorphism $N \to Inn(N)$ sending $n \in N$ to the inner automorphism defined by conjugation by n. This surjective homomorphism sits in an exact sequence of the form

$$1 \longrightarrow Z(N) \longrightarrow N \longrightarrow Inn(N) \longrightarrow 1.$$

Given the function $c : Q \times Q \to Inn(N)$, we may always lift it to a function $\tilde{c} : Q \times Q \to N$. Even though the function c satisfies the cocycle condition, $\tilde{c}$ may *fail* to do so. However, as before, we may define a function o measuring the failure of $\tilde{c}$ to satisfy the generalized cocycle condition. More precisely, define $o(\tilde{c})$ by means of the formula

$$o(q_1, q_2, q_3) := \tilde{c}(q_1, q_2)\tilde{c}(q_1q_2, q_3)\tilde{c}(q_1, q_2q_3)\tilde{\omega}_{q_1}(q_2, q_3)^{-1}.$$

A priori $o : Q \times Q \times Q \to N$, but since we know that c satisfies the cocycle condition, o actually takes values in $Z(N)$, i.e., o is a function $Q^3 \to Z(N)$, i.e., defines an element of $C^3(Q, Z(N))$ as described at the beginning of this section.

When we considered the extension problem with A abelian, we observed that the function f we wrote down measuring failure of our section to be a group homomorphism satisfied a natural compatibility condition coming from associativity of the group action. Thus, it is natural to ask whether the function o described in the previous paragraph satisfies any additional compatibility condition. If we try to define a group structure by means of $\tilde{c}$, then saying the cocycle condition fails is tantamount to saying that the product we would try to equip the set $N \times Q$ with fails to be associative. However, there are natural higher-order associativity constraints that one can consider. For example, there are 5 ways to parenthesize a product of 4 elements. Bearing this analogy in mind, recall from above that we defined the differential d^3 by the formula

$$d^3(o)(q_1, q_2, g_3) = \omega_{q_1}o(q_2, q_3, q_4) - o(q_1q_2, q_3, q_4) + o(q_1, q_2q_3, q_4) - o(q_1, q_2, q_3q_4) + o(q_1, q_2, q_3).$$

The extra compatibility satisfied by o can be expressed in terms of d^3.

Proposition A.2.3.1. *The function $o(\tilde{c}) : Q \times Q \times Q \to Z(N)$ defined above lies in the kernel of $d^3 : C^3(Q, Z(N), \tilde{\omega}) \to C^4(Q, Z(N), \tilde{\omega})$, i.e., $o(\tilde{c})$ is a $Z(N)$-valued 3-cocycle on Q. If $\tilde{c}'$ is another lift of $\tilde{c}$, then $o(\tilde{c'}) - o(\tilde{c})$ lies in $im(d^2 : C^2(Q, Z(N), \tilde{\omega}) \to C^3(Q, Z(N), \tilde{\omega}))$.*

Proof. This is a straightforward, but tedious computation. □

It follows that the possible non-triviality of $o(\tilde{c}) \in H^3(Q, Z(N))$ yields an *obstruction* to the existence of an extension supporting a given $\omega : Q \to Out(N)$ and $o(\tilde{c})$ is called the *obstruction class* associated with $\tilde{c}$. If the obstruction class $o(\tilde{c})$ defines the trivial element in $H^3(Q, Z(N))$, we will say the obstruction vanishes.

Classification of extensions

If the obstruction $o(\tilde{c})$ vanishes, then $\tilde{c}$ necessarily defines a function $Q \times Q \to N$ satisfying an analog of the cocycle condition. In general, there are many such functions that even give rise to the same function c we wrote down initially. Indeed, if $\tilde{c}(q_1, q_2) = \tau(q_1, q_2)\tilde{c}'(q_1, q_2)$ and both give rise to $c(q_1, q_2)$, it follows that $\tau(q_1, q_2)$ is a function $Q \times Q \to Z(N)$. If both $\tilde{c}$ and $\tilde{c'}$ satisfy the generalized cocycle condition, it follows that $\tau(q_1, q_2)$ is a 2-cocycle on Q with values in $Z(N)$ in the usual sense. In fact, given any fixed lift $\tilde{c}(q_1, q_2)$ satisfying the generalized cocycle condition, there is an action of $Z^2(Q, Z(N)) := \ker(d^2)$ on the space of functions $Q \times Q \to N$ satisfying the generaliezd cocycle condition sending $\tau \in Z^2(Q, Z(N))$ to $\tilde{c}(q_1, q_2)$ to $\tau\tilde{c}$. The observation of the previous sentence then shows that the action of $Z^2(Q, Z(N))$ on the set of pairs $\tilde{c} : Q \times Q \to N$ of c that satisfy the generalized cocycle condition is transitive. The stabilizer of $\tilde{c}(q_1, q_2)$ consists precisely of $Im(d^1) := B^2(Q, Z(N))$ and thus, one obtains the following result.

Theorem A.2.3.2. *Suppose Q and N are groups, and $\omega : Q \to Out(N)$ is a fixed function. Let $\tilde{\omega} : Q \to Aut(N)$ be a fixed lift of ω, and let $c : Q \times Q \to Inn(N)$ be the function measuring the failure of $\tilde{\omega}$ to be a homomorphism.*

1. *There exists an extension of Q by N inducing ω if and only if the obstruction class $o(\tilde{c})$ attached to some $\tilde{c} : Q \times Q \to N$ of c in $H^3(Q, Z(N))$ vanishes.*
2. *If the obstruction class $o(\tilde{c})$ vanishes, then the set of extensions of Q by N inducing ω admits a transitive action of $Z^2(Q, Z(N))$. Upon choice of a fixed element $\tilde{c}$ lifting c and satisfying the generalized cocycle condition, we conclude that the set of such extensions is in bijection with $H^2(Q, Z(N))$.*