Algebraic Theory I

Thomas Fleming

September 20, 2021

Contents

Lecture 1: Review of Group Theory

Mon 23 Aug 2021 11:21

1 Review of Group Theory

Textbook

Algebra I will use Dummitt and Foote and Algebra II will also use Lang and Hungerford.

Definition 1.1 (Group)**.** A **multiplicative group** is a set G with a binary operation mapping the product of two elements from G to an element of G: $\cdot : G \times G \to G$. This operation must be closed, associative, have an identity (1), and have inverses (g^{-1}) for all $g \in G$. Alternatively, a **additive group** uses the operation $+ : G \times G \to G$, this is generally used with commutative groups and we denote the identity 0 and inverse $-g$.

Remark (Commutatitvity)**.** Groups need not be commutative. However, inverses and identities always commute ($1g = g1 = g$ and $gg^{-1} = g^{-1}g = 1$). Groups for which $gh = hg$ for all $g, h \in G$ are denoted abelian.

Definition 1.2 (Subgroup)**.** If $(G, \cdot)$ is a group, a nonempty subset $H \subseteq G$ is a **subgroup** if H forms a group under the same operation $(\cdot)$. We denote this $H \leq G$. In other words, H is closed under $\cdot$ and under inverses. Clearly, associativity and identity are implicitly a part of H if closure and inverses hold. A subgroup for which $H \subset G$ is denoted $H < G$ and is called a **proper subgroup**.

Example. The trivial subgroup $\{1\} \leq G$ is always a subgroup. $\diamond$

Theorem 1.1 (Lagrange's Theorem)**.** If $H \leq G$ and $|G|$ is finite, then $|H| \,|G|$ (The order of H divides the order of G).

Definition 1.3 (Order)**.** The **order** of an element $g \in G$ is the least positive integer n for which $g^n = 1$. We denote this (g) and we define $g^0 \coloneqq 1$ for consistency sake.

Notation (Additive order)**.** Instead of exponent notation, we use $ng = g + g + \ldots + g$, n times, to denote the repeated application of the group operation in an additive group.

Definition 1.4 (Homomorphisms)**.** A **group homomorphism** is a map between two groups $(G, \cdot)$ and $(H, \times)$ which preserves operations. That is, $\varphi : G \to H$ such that for $x, y \in G$, we have $\varphi(x \cdot y) = \varphi(x) \times \varphi(y)$.

Remark. It is a direct result of this definition that $\varphi(1_G) = 1_H$ and $\varphi\left(g^{-1}\right) = \varphi(g)^{-1}$ for all $g \in G$.

Definition 1.5 (Types of Maps)**.** A map $f : A \to B$ for which $f(x) = f(y) \Rightarrow x = y$ for all $x, y \in A$ is called an **injection**. A map such that for all $z \in B$, there exists $x \in A$ such that $f(x) = z$ is called a **surjection**. An equivalent notation is that $f(A) = B$ or to say the range of f is B. A map which is both in injection and a surjection is called a **bijection**.

Remark (Injection creates bijection)**.** As the quality of surjection is more dependant on our codomain than the map itself, we may alter any map which is an injection to create a bijection. Suppose $f : A \to B$ is an injection, then, restricting the codomain of f to be exactly $f(A)$ induces a surjection, and hence a bijection.

Definition 1.6 (Isomorphism)**.** A group homomorphism which is a bijection is called an **group isomorphism**. If two groups G, H have an isomorphism between them, then they are called **isomorphic** and we denote this relation by $G \simeq H$.

Remark. For a group isomorphism it is sufficient to only check that the identity is injective. Restated, φ is injective if $\ker(\varphi) = \{g \in G : \varphi(G) = 1\} = \{1\}$, a trivial subgroup of G (Note that the kernel is always a subgroup of the domain).

Remark. If φ is an isomorphism, then $\varphi^{-1} : H \to G$ is also an isomorphism, hence $H \simeq G$. Isomorphism of two groups essentially implies equivalence of the groups in all algebraic ways. It is of note that it is possible to have subgroups $H, K \leq G$ such that $H \simeq K$ but,H and K possess different properties within G. Hence isomorphism implies equivalence only when the groups which are isomorphic are the whole of the universe under consideration.

Definition 1.7 (Automorphism)**.** If G is a group, we define (G) to be the set of all isomorphism from $G \to G$. This is called the **automorphism group** and it does indeed from a group under the operation of composition. An element $f \in (G)$ is called an **automorphism** of G. The group operation is usually denoted, for $f, g \in (G)$, $x \in G$, as $f(g(x))$ or $(f \circ g)(x)$.

Lecture 2: Review of Group Theory Continued

Wed 25 Aug 2021 11:31

Let $\alpha : G_1 \to G_2$ be a homomorphism and $\beta : G_2 \to G_3$ be another homomorphism. Now, we define the map $\beta\alpha : G_1 \to G_3$ to be the homomorphism induced by the composition of α and β so that $(\beta\alpha(x)) = \beta(\alpha(x))$. In the special case where $G_1 = G_2 = G_3$, we see $\alpha, \beta, \alpha\beta \in (G)$.

Proposition 1.1. If G is a group, $H \leq G$ and $\varphi : G \to G'$, then the image $\varphi(H) \leq G'$.

Definition 1.8 (Cosets)**.** The **left H-coset** is the set of the form $xH = \{xh : h \in H\}$. Similairly, the **right H-coset** is the set of the form $Hx = \{hx : h \in H\}$. We call the number of H-cosets of a group G (this can be left or right cosets as the number is always equal) to be the **index of H in G**. We denote this by $|G : H| = \frac{|G|}{|H|}$.

Remark. The left H-cosets partition G, that being, two cosets are either equal or disjoint and the union of all unique H-cosets covers G. Similairly for the right H-cosets. Hence, we have either $xH = yH$ or $xH \cap yH = \varnothing$. We call x a **representative** for the coset of H and any element $xh \in xH$ is also a representative.

Definition 1.9 (Normal Groups)**.** A subgroup $H \leq G$ is called a **normal subgroup** of G when $xHx^{-1} = H$ for all $x \in G$. This is equivalent to the statement $xH = Hx$ for all $x \in G$. We denote this relation by $H \trianglelefteq G$.

Remark. It is important to know this does not imply commutativity, simply that the sets themselves are equal, but there is not necessarily element-wise equality.

Definition 1.10 (Conjugation Map)**.** For each $x \in G$ we can define the **conjugation map** by x as $d_x : G \to G$, $x \mapsto d_x(x) = xyx^{-1}$. This is an automorphism of G.

Remark (Why are normal subgroups important?)**.** If $\varphi : G \to G$ is a homomorphism, then $\ker(\varphi) = \{x \in G : \varphi(x) = 1\} \trianglelefteq G$.

Definition 1.11 (Quotient Groups)**.** We define the **quotient group** $G/H = \{xH : x \in G\}$. Normal groups allow us to define multiplication for this groups as the left and right cosets are equivalent. Thus, presuming $H \trianglelefteq G$ we have $(xH)(yH) \coloneqq (xyH) \in G/H$. We can think of the quotient G/H as sending all elements of H to the identity, or "modding" out by H.

Definition 1.12 (Normalizer)**.** If $S \subseteq G$, then $N_G(S) = \{x \in G : xSx^{-1} = S\} \leq G$. This is called the **normalizer subgroup** of S in G. Generally, we assume S is a subgroup. If S is a subgroup, then $N_G(S)$ is the largest subgroup of G in which S is normal (though it is not necessarily normal in G). That is, $H \trianglelefteq N_G(H) \leq G$.

Definition 1.13 (Centralizer)**.** We define the **centralizer subgroup** of H in G to be $Z_G(H) = \{x \in G : xh = hx \ \forall \ h \in H\}$. As this requires commuting element-wise instead of set-wise, we see $Z_G(H) \leq N_G(H) \leq G$. We call $Z_G(H)$ the **center** of G.

Notation. Sometimes $Z_G(H) = C_G(H)$ is used alternatively for the centralizer.

Definition 1.14 (Subgroup Generated by a Subset)**.** For $X \subseteq G$ we define $\langle X \rangle \leq G$ to be the **subgroup generated by X**. This is simply the smallest subgroup generated by X. It is clear to see $\langle X \rangle = \{x_1 \cdot x_2 \cdot \ldots \cdot x_n : x_1, x_2, \ldots, x_n \in X \cup X^{-1}, n \geq 9\}$ where $X^{-1} = \{x : x^{-1} \in X\}$.

Definition 1.15 (Commutator)**.** We define the **commutator subgroup** of G to be $G' = [G : G] = \langle X \rangle$ where $X = \{ghg^{-1}h^{-1} : g, h \in G\}$.

Remark. We call this the commutator because G/G' is abelian. Furthermore, if G/H is abelian for a subgroup $H \leq G$, then $G' \leq H$. Hence, G' is the smallest subgroup which must be quotiented to induce an abelian group.

With all of these definitions taken care of we may finally state the most powerful theorems of group theory, the 3 isomoprhism theorems.

Theorem 1.2 (The 3 (4) Isomorphism Theorems)**.**

1. Let $\varphi : G \to G'$ be a surjective homomoprhism, then $\ker(\varphi) \trianglelefteq G$ and $G' = \varphi(G) \simeq G/\ker(\varphi)$.
2. Suppose $H, K \trianglelefteq G$ and $K \leq H$. Then, we have $G/H \simeq (G/K)/(H/K)$.
3. Let $H, K \leq G$ and $H \leq N_G(K)$.
   Then, $HK = \{hk : h \in H, k \in K\} \leq G$. Moreover, $HK/K \simeq H/(H \cap K)$ (Presuming all terms are well defined, hence $K \trianglelefteq HK$ and $H \cap K \trianglelefteq H$).
4. (Lattice Theorem) Suppose $\varphi : G \to G'$ is a surjective homomorphism with $\ker(\varphi) = K$, then there is a bijective correspondance between subgroups of G' and subgroups of G which contain $\ker(\varphi)$. That is, if $K = \ker(\varphi)$, then $H \mapsto H/K = \varphi(H)$ and if $H \leq G'$ has $H \mapsto \varphi^{-1}(H) \leq G$ where $\ker(\varphi) \subseteq \varphi^{-1}(H)$. Furthermore, if we use the first isomorphism theorem to write $G' \simeq G/K$, then the subgroups of G/K are H/K with $K \leq H \leq G$. Finally, this correspondance preserves normality.

Lecture 3: Group Actions

Fri 27 Aug 2021 11:31

2 Group Actions

Recall (The Lattice Theorem)**.** Recall that if $\varphi : G \to G'$ is a surjective homomorphism, then there is a bijective correspondance between subgroups of G which contain $\ker(\varphi)$ and subgroups of G' which preserves normality.

Definition 2.1 (Permuatation Group)**.** Recall

$$(\Omega) = \{f : f : \Omega \to \Omega \text{ such that f is a bijection.}\}$$

is the **permutation group** of Ω. This is essentially a shuffling of elements of Ω. If $|\Omega| = n < \infty$, then $(\Omega) \simeq S_n$.

Definition 2.2 (Group Action)**.** Let G be a group and Ω to be a collection of elements of G (a set). Then a **group** action of G on Ω is a homomoprhism $\alpha : G \to (\Omega)$. We say G acts on Ω.

Notation.

1. We generally use the exponential notation $x^g := (\alpha(g))(x)$ for $g \in G$ and $x \in \Omega$).
2. Some authors, such as Dummit and Foote, use multiplicative notation gx or $g \cdot x$ for the same action.

Intuition. Our homomorphism α essentially characterized how an element within G will "move around" the elements of Ω in some way.

The defining property of a group action is that $(x^g)^h = x^{hg}$ for all $h, g \in G$

and $x \in \Omega$. That is, group actions turn composition into multiplication. In the function notation this is,

$$\begin{aligned}(x^g)^h &= ((\alpha(g)(x)))^h \\ &= \alpha(h)(\alpha(g)(x)) \\ &= (\alpha(h)\alpha(g))(x) \text{ as } \alpha(g)(x) \in (\Omega). \\ &= (\alpha(hg)(x)) \text{ By } \alpha \text{ being a homomorphism.} \\ &= x^{hg}.\end{aligned}$$

Remark. We know $x^1 = x$ for $x \in \Omega$ as $\alpha(1) = 1$ by homomorphism. This corresponds to the map which leaves all elements of Ω in place.

Example (Conjugation Map)**.** Let G act on itself by conjugation, that is $\Omega = G$ and let

$$\begin{aligned}\alpha : G &\longrightarrow (G) \\ g &\longmapsto \alpha(g) = gxg^{-1} \in (G) \leq (G).\end{aligned}$$

We see this is simply the cnonjugation by g map. Let us verify this is a group action. $x^1 = 1x1^{-1} = x$. Similarly,

$$\begin{aligned}(x^g)^h &= \left(gxg^{-1}\right)^h \\ &= h\left(gxg^{-1}\right)h^{-1} \\ &= (hg)xg^{-1}h^{-1} \\ &= (hg)x(hg)^{-1} \\ &= x^{hg}.\end{aligned}$$

Hence, we have confirmed α is a group action. ◇

Now, let us examine $\ker(\alpha) \trianglelefteq G$.

$$\begin{aligned}\ker(\alpha) &= \{g \in G : x^g = x \ \forall \ x \in G\} \\ &= \{g \in G : gxg^{-1} = x \ \forall \ x \in G\} \\ &= \{g \in G : gx = xg \ \forall \ x \in G\} \text{ multiplying by } g \text{ from the right} \\ &= C_G(G) = Z_G(G), \text{ the center of } G.\end{aligned}$$

Definition 2.3 (Inner Automorphisms)**.** We call $\alpha(G)$ the **inner automorphisms of** G.

Example (Conjugation Map on Sets)**.** Let G act on the subsets $A \subseteq G$ by conjugation, that is $\Omega = \{H : H \subseteq G\}$. For $X \subseteq G$ and $g \in G$, let

$$X^g = gXg^{-1} \qquad = \{gxg^{-1} : x \in X\}.$$

Here, g is a bijection of the sets as the map g^{-1} is an inverse map to g. (hence it is a permutation and thus a group action.). That is,

$$X \to_g X^g \to_{g^{-1}} (X^g)^{g^{-1}} = X$$

. ◇

Remark (Permutations)**.** The two properties $(x^g)^h = x^{hg}$ and $x^1 = x$ completely characterizes a group action (and hence a permutation), but sometimes it is easier to check for an inverse map as we did in the example previous.

In general, if G acts on Ω and $\Omega' \subseteq \Omega$ is a subset which is closed (meaning $x \in \Omega'$, $g \in G$ implies $x^g \in \Omega'$), then we can simply restrict the codomain of the group action, hence G can act on Ω' in exactly the same way.

Example (Left Multiplication)**.** Let G act on itself by left multiplication. (right multiplication will be essentially equivalent). Hence $\Omega = G$ and $x^g \coloneqq gx$ for $x, g \in G$. Of course, $x^1 = 1x = x$ and

$$\begin{aligned}(x^g)^h &= (gx)^h \\ &= h\,(gx) \\ &- (hg)\,x \\ &= x^{hg}.\end{aligned}$$

Hence, this is a group action, but it will not be an automorphism (as it is not necessarily a bijection). There is, however, an inverse map, simply multiplication by g^{-1}, so we see it really does map to a permutation of G. ◇

Lecture 4: Group Actions (2)

Mon 30 Aug 2021 11:26

Recall (Group Actions)**.** The canonical definition of a group action was a map from $G \to \Omega$ satisfying $x^1 = x$ and $(x^g)^h = x^{hg}$. Formally, we defined a homomorphism $\alpha : G \to (G)\,,\ x \mapsto (\alpha(g))\,(x) \coloneqq x^g$, where the homomorphism condition implies the identity condition and the "left action" combined with the rules of composition implies the second condition.
Recall also, that we had for a subset $X \subseteq \Omega$ then $G_X = \{g \in G : X^g = X\}$ where $X^G = \{x^g : x \in X\}$ is called the stabilizer of X. A common case of this is where $X = \{x\}$, where we have $G_x = \{g \in G : x^g = x\} \leq G$, denoted the **point stabilizer** of x.

Point Wise Stabilizer

$\bigcap_{x \in X} G_x \leq G_X$ is called the **point wise stabilizer** of X. Essentially, the point stabilizer of a point x must leave x in its position, taking the intersection of these yields all of the $g \in G$ which leaves every element of X exactly in its place. On the other hand, G_X can permute the elements within X provided they stay within X.

Definition 2.4 (Properties of Actions)**.**

1. A group action, α, is **transitive** if for all $x, y \in \Omega$ there is a $g \in G$ such that $x^g = y$
2. The action is **faithful** if $\ker(\alpha)$ is trivial, that is, $x^g = x^h$ for all $x \in \Omega$ implies $g = h$
3. That is, each element of G provides a distinct map
4. A **fixed point** of Ω is an element $x \in \Omega$ such that $x^g = x$ for all $g \in G$ (hence $G_x = G$)
5. If $X \subseteq \Omega$, then the **orbit** of X is the set $\mathscr{O}_X = \{x^g : x \in X, g \in G\}$

Remark. If the action is transitive, then $\mathscr{O}_X = \Omega$ for all nonempty $X \subseteq \Omega$.

Example. Let G act no itself by conjugation ($x^g = gxg^{-1}$). Then, $G_x = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = Z_G(\langle x \rangle)$. ◇

Theorem 2.1. Let G act on Ω, then $G_{xg} = gG_xg^{-1}$ for all $x \in \Omega$, $g \in G$.

Proof.

$$\begin{aligned}
G_{xg} &= \{h \in G : (x^g)^h = x^g\} \\
&= \{h \in G : x^{hg} = x^g\}. \\
&\text{Now, let us change variables, let } h' = ghg^{-1}, \text{ then} \\
&= \{gh'g^{-1} \in G : x^{gh'g^{-1}g} = x^g\} \\
&= \{gh'g^{-1} \in G : x^{gh'} = x^g\} \\
&\text{Now, note } x^{h'} = x \Leftrightarrow x^{gh'} = x^g. \text{ So,} \\
&= \{gh'g^{-1} \in G : x^{h'} = x\} \\
&= g\{h' \in G : x^{h'} = x\}g^{-1} \\
&= gG_xg^{-1}.
\end{aligned}$$

□

Theorem 2.2. Suppose G acts on Ω and let $x \in \Omega$, $g, h \in C$. Then, $x^g = x^h \Leftrightarrow x, y$ are in the same left G_x-coset.

Proof. Suppose $x^g = x^h$ and apply the inverse map, h^{-1} to both sides. This yields

$$\underbrace{(x^g)^{h^{-1}}}_{=x^{h^{-1}g}} = \underbrace{x^{hh^{-1}}}_{=1}.$$

Thus, $h^{-1}g \in G_x$, so $g \in hG_x$.

Now, Conversely, if $g \in hG_x$ we have

$$\begin{aligned} h^{-1}g &\in G_x \\ \Rightarrow x^{h^{-1}g} &= x \\ \Rightarrow \underbrace{\left(x^{h^{-1}g}\right)^h}_{=x^{hh^{-1}g=x^g}} &= x^h \\ \Rightarrow x^g &= x^h. \end{aligned}$$

This concludes the proof. □

Theorem 2.3 (Orbit-Stabilizer Theorem)**.** Suppose G acts on Ω, then $|\mathscr{O}_x| = |G : G_x|$ for all $x \in \Omega$. That is, the size of the orbit of x is equal to the index of the point stabilizer of x.

Proof. Let us induce a bijection between $\mathscr{O}_x$ and $[G : G_x]$. Define a map

$$\begin{aligned} f : \{gG_x : g \in G\} &\longrightarrow \Omega \\ x &\longmapsto f(x) = f(gG_x)) = x^g. \end{aligned}$$

By the previous theorem, we know if $h \in gG_x$, then $x^h = x^g$, so this map is in fact well defined (it doesn't matter which representative we choose). We see $(f) = \mathscr{O}_x$. Now, if we prove the map is injective, we have a bijection from the $[G : G_x] \to \mathscr{O}_x$. Now, suppose $f(gG_x) = f(hG_x)$, then as $x^g = x^h \Leftrightarrow gG_x = hG_x$, then we have the map is injective (as the output being equal implies the input is equal), hence we have a bijection, so the cardinalities are equal, $|\mathscr{O}_x| = |G : G_x|$. □

3 Conjugacy and Normality Proofs

Lecture 5: Mathematical Justification of Conjugacy

Wed 01 Sep 2021 11:24

Recall (Orbit Stabilizer Lemma)**.** If G acts on a set Ω and $x \in \Omega$, then $|\mathscr{O}_x| = |G : G_x|$. This meant, we could write $|\Omega| = \sum_{x \in A} |\mathscr{O}_x| = \sum_{x \in A} |G : G_x|$, where $A \subseteq X$ was a subset of Ω containing one representatives for each orbit.

Example. If G acts on itself by conjugation. We call the orbits of this action the **conjugacy classes** of G. So $\mathscr{O}_x = \{gxg^{-1} : g \in G\}$ and
$G_x = \{g \in G : gxg^{-1} = x^g = x\} = Z_G(\langle x \rangle)$.
Hence,

$$|\Omega| = |G| = \sum_{x \in \mathscr{C}} |G : Z_g(x)| = |Z(G)| + \sum_{x \in \mathscr{C}'} |G : Z(x)|$$

where $\mathscr{C}$ is a set containing 1 representative from each conjugacy class and $\mathscr{C}'$ is a set containing 1 representative from each conjugacy class of size ≥ 2.
This final equivalence comes from the fact that the orbit being of size 1 implies that $gxg^{-1} = x$ for all g, hence the centralizer $Z(x) = Z(G)$. ◇

Definition 3.1 (Subgroup Conjugacy)**.** Two subgroups $H, K \leq G$ are **conjugate** when $K = gHg^{-1}$ for some $g \in G$. So, K is the image of H under the conjugation by g automorphism for some $g \in G$. Since K is an isomorphic image of H, we have $H \simeq K$ for conjugate groups $H, K \leq G$.

We may wish to count the number of conjugate subgroups. For this, let G act by conjugation on the set of all subgroups conjugate to H, denoted Ω. This is a transitive group action by definition (there is only 1 orbit). So, by the orbit stabilizer lemma, the number of conjugate subgroups which is precisely $|\Omega| = |G : G_H| = |G : N_G(H)|$. This is true as

$$\begin{aligned} G_H &= \{g \in G : H^g = H\} \\ &= \{g \in G : gHg^{-1} = H\} \\ &= N_G(H). \end{aligned}$$

Theorem 3.1. Let G be a group with $H \leq G$ and $|G : H| = 2$. Then, H is normal.

Proof. Let G act on all conjugate subgroups to H by conjugation. Then, the number of conjugate subgroups is simply $|G : N_G(H)|$ by the previous remark. Let us note, $H \leq N_G(H) \leq G$ and $|G : H| = 2$. If $H < N_G(H)$, then $N_G(H)$ would contain 2 H-cosets, whose union would be G by the index 2 assumption. Thus, wither $N_G(H) = H$ or G. If $N_G(H) = G$, then H is normal by definition since $H \trianglelefteq N_G(H)$.
Hence, assume the contrary, that $N_G(H) = H$. Thus, there are $|G : N_G(H)| = |G : H| = 2$ conjugate subgroups to H, denoted $\Omega = \{H, K\}$. Thus G is acting on the two element set Ω, hence there is a homomorphism $\alpha : G \to (G) \simeq S_2$. Let $\ker(\alpha) = H_0$.
By definition, we have $H_0 = \{g \in G : H^g = H \text{ and } K^g = K\}$, but as g is a permutation, we see mapping $H \mapsto H$ implies $K \mapsto K$. Hence, $H_0 = \{g \in G : H^g = H\} = N_G(H) = H$. As H is the kernel of a homomorphism it is normal. Hence H is normal in either case, so $H \trianglelefteq G$. □

Many of the ideas of this proof will be used frequently, such as showing something is the kernel in order to show its normal.

Note on the Midterm

The midterm will consist of 2 parts, the first part will consist of novel problems which only require mashing together the theorems and lemmas we already to know in order to make a short (1 paragraph) proof) and the second part will consist of recitation of the proofs of some of the more important theorems.

Let G be a finite group and let $p \mid |G|$ be the smallest prime divisor of $|G|$. Let H be a subgroup such that $|G : H| = p$. Then $H \trianglelefteq G$. We see this is a generalization of the previous result as 2 is the "smallest smallest" prime divisor

of all. The one caveat is that this can only be applied to finite groups as $|G|$ must be well defined.

Proof. Let Ω be the set of conjugate subgroups to H and let G act on Ω by conjugation. As before, as this action is transitive, we know
$|\Omega| = |G : G_H| = |G : N_G(H)|$. we need to use $|G : H| = p$ to conclude $N_G(H) = H$. In general, we know $H \leq N_G(H) \leq G$, hence as $|G : H| = p$, then we have

$$p = |G : H| = |G : N_G(H)| \cdot |N_G(H) : H|.$$

Thus, $|G : N_G(H)| = 1$ or p as p is prime so there are no divisors. If $|G : N_G(H)| = 1$, then $N_G(H) = G$, so $H \trianglelefteq G$. Hence, let us conclude the contrary, that $|G : N_G(H)| = p$. Hence, $|N_G(H)| = 1$ by the earlier product, hence $N_G(H) = H$. The rest of the proof follows directly from the earlier arguments with some minor augmentations, we will show that H is the kernel of the associated homomorphism, making use of the fact that p was the smallest prime divisor. □

Lecture 6: Conclusion of Lecture 5 and Sylow Theorems

Fri 03 Sep 2021 11:30

Recall. We had shown that if G acts by conjugation on the conjugate subgroups of H, then the normalizer $N_G(H) = H$.

continued. Let $\alpha : G \to (\Omega) \simeq S_p$ be the associated homomorphism with the group action. Recall $|\Omega| = |G : N_G(H)| = |G : H| = p$ by the orbit stabilizer theorem. Let align* $\mathrm{H}_0 = \ker(\alpha)$
$= \{g \in G : K^g = K \ \forall \ k \in \Omega\}$
$= \bigcap_{K \in \Omega} \{g \in G : K^g = K\}$
$= \bigcap_{K \in \Omega} N_G(K)$ by definition of normalizer
$\Rightarrow H_0 \leq H = N_G(H)$ as $H \in \Omega$.

We see $|\Im(\alpha)| = \left|\frac{G}{H_0}\right|$ as $\Im(\alpha) \leq S_p$. This implies $\left|\frac{G}{H_0}\right| \mid |S_p| = p!$.
Also, $\frac{|G|}{|H_0|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|H_0|} = |G : H| \cdot |H : H_0| = p \cdot |H : H_0|$.
Simplifying, we see $p\,|H : H_0| = \left|\frac{G}{H_0}\right|$ and as this divides $p!$, we obtain

$$p\,|H : H_0| \mid p! \Rightarrow |H : H_0| \mid (p-1)!.$$

But, $|H : H_0| \mid |H| \mid |G|$, but as p is the smallest prime divisor of $|G|$, all prime divisors are $\geq p$ and thus, they would not divide $(p-1)!$. Hence, we see $|H : H_0| = 1$, hence $H = H_0 = \ker(\alpha)$. As the kernel is a normal subgroup, this yields $H \trianglelefteq G$. □

4 Sylow Theorems

Definition 4.1 (P-groups)**.** A group G is a **p-group** where p is prime if the order of every $g \in G$ is a power of p

Theorem 4.1 (Cauchy's Theorem)**.** If G is a (nontrivial) finite group and $p \mid |G|$ is a prime, then there is a $g \in G$ such that $(g) = p$ and hence there is a subgroup $[g]$ of order p.

Proof. We will break the proof into 2 cases.

1. G is abelian.
2. G is nonabelian.

Note that we will use 0 as the identity for this part of the proof as the groups are abelian. For the first case we will proceed by induction. If $|G| = p$, then any nonzero element of $x \in G$ has $(x) = p$ as $(x) \mid |G|$ and the order is not 1 so it must be p.
We will use this as the base case. Let $x \in G$ be a nonzero elemnt and let $H = \langle x \rangle$, so $|H| = (x)$. So, $\{H = x, x^2, \ldots, x^{(x)}\}$. If $p \mid |H|$, then $\left(x^{|H|/p}\right) = p$, so such an element exists. In the other case ($p \nmid |H|$). Then, $p \mid |G/H|$ as $p \mid |G| = |G/H| \cdot |H|$. This is well defined as G is abelian, so H must be normal. Let $\varphi_H : G \to G/H$ be the cannonical homomorphism, then $|G/H| < |G|$as H is nontrivial and $p \mid |G/H|$ so the inductive hypothesis implies there is a $y \in G$ such that $(\varphi_H(y)) = p$. Let $m = (y)$. Then, $y^m = 1$, so $\varphi(y^m) = \varphi(y)^m = 1$, so $(\varphi(y)) = p \mid m$ (and $m = \alpha p$). Hence, $(y^\alpha) = p$. This completes the proof of this case.

For the nonabelian case, we will make use of the class equation, so let us recall:

$$|G| = |Z(H)| + \sum_{X \in \mathscr{C}} |G : Z_G(x)|$$

where $\mathscr{C} \leq G$ is simply a set of representatives for all conjugacy classes in G of size ≥ 2. Now, $Z(G)$ is the center of G, so it is abelian by definition. If $p \mid |Z(G)|$ then we may simply apply the abelian case to yield an element, $x \in Z(G) \leq G$, of order p. Hence, assume $p \nmid |Z(G)|$. Then, we see there must be atleast one $x \in \mathscr{C}$ such that $p \nmid |G : Z_G(x)|$ (else we would have all parts of the right size of the class equation are divisible by p except the centralizer, so $|G| = |Z(G)|(\mod p) \neq 0(\mod p)$). So, $p \nmid |G : Z_G(\langle x \rangle)| = \frac{|G|}{|Z_G(x)|}$. But, $p \mid |G| = \left(\frac{|G|}{|Z_G(x)|}\right)|Z_G(x)|$, so $p \mid |Z_G(x)|$.
If $Z_G(x) < G$, then we could proceed by induction on $|G|$ and apply the inductive hypothesis to $Z_G(x)$ to complete the proof (with base case $|G| = p$). Hence, we must have $Z_G(x) = G \Rightarrow x \in Z(G)$. This is a contradiction, as we assumed $|G : Z_G(x)| = \frac{|G|}{|Z_G(x)|} \geq 2$. That is, x was chosen to be an element not in the center, but if $Z_G(x) = G$, then x commutes with everything, so $x \in Z(G)$. $\lightning$. Hence, we must have that $p \mid |Z(G)|$ or $Z_G(x)$ is a proper subgroup of G, so this completes the proof. □

Corollary 1. If H is a finite p-group, then $|H| = p^n$ for some $n \geq 1$.

Proof. If this fails, then there is a $q \mid |H|$ with $q \neq p$ being prime. Then, cauchy's theorem implies there is an element of order $q \neq p$, so H is not a p-group. $\lightning$. $\square$

Definition 4.2 (Sylow Subgroup)**.** If G is a finite group, p is a prime, and p^n is the maximal power of p such that $p^n \mid |G|$. Then, any subgroup $H \leq G$ with $|H| = p^n$ is called a **sylow p-subgroup**.

Example. If $|G| = 8 \cdot 9 \cdot 7$. Then a subgroup with $|H| = 8$ is a sylow 2-group. Similairly, $|H| = 9$ implies H is a sylow 3-group and $|H| = 7$ implies H is a sylow 7-group. $\diamond$

Lecture 7: Sylow Groups (2)

Wed 08 Sep 2021 11:20

Recall. If G is a finite group, then a subgroup of G such that p^n is the maximal power of p such that $p^n \mid |G|$, then H is a sylow p-group.

Theorem 4.2. If G is a finite group and p is a prime, then G has a sylow p-group.

Proof. We will use induction. For the first cases, if $|G| = p^n$ then the subgroup $H = G$ is a sylow p-group. Also if $p \nmid |G|$, then the trivial subgroup is a sylow p-group. Hence, we can assume $p \mid |G|$ with $\hat{p} \mid |G|$ for some prime $\hat{p} \neq p$.

First, recall the class equation, $|G| = |Z(G)| + \sum_{x \in I} |G : G_x|$ where I is a set of representatives of each orbit of size ≥ 2 when G acts on itself by conjugation.

Observation. If $K < G$, then we can assume $p^n \nmid |K|$ else a sylow $p-$group for K would also be a sylow p-group for G, which we would know to exist by induction hypothesis. Hence, we can assume $p \mid |G : K|$.

Now, note that every G_x with $x \in I$ has that $G_x < G$, else its index would be 1 and x would not be in I. Hence, we have $p \mid |G : G_x|$ for all $x \in I$. And, as $p \mid |G|$, we see $p \mid |Z(G)|$ by the class equation. This implies the center is nontrivial.
Hence, by cauchy's theorem, there is an $x \in Z(G)$ such that $(x) = p$. Then, $\langle x \rangle \leq Z(G) \trianglelefteq G$. Furthermore, every subgroup of $Z(G)$ is normal by definition of the center, hence $\langle x \rangle \trianglelefteq G$.
Let us now examine $G/\langle x \rangle$. We see $|G/\langle x \rangle| = \frac{|G|}{p}$, hence p^{n-1} is the highest power which divides $G/\langle x \rangle$. Using the induction hypothesis yields a sylow p-group of $G/\langle x \rangle$ and by the lattice theorem, we know the p-group has the form $H/\langle x \rangle$ for a subgroup $H \leq G$ such that $\langle x \rangle \leq H$. Again, we see $|H/\langle x \rangle| = \frac{|H|}{p} = p^{n-1} \Rightarrow |H| = p^n$. $\square$

Lemma 4.1. If G is a p-group acting on the finite set Ω, then the number of fixed points in Ω, denoted n, has $n \equiv |\Omega| \,(\mod p)$

Proof. Recall

$$|\Omega| = \sum_{x \in I} |G : G_x|$$

where I is a set of representatives for the orbit of each action. As x is a fixed point, we see $G_x = G$, hence let us separate the equation and define $\mathscr{O}$ to be the set of representatives from each orbit of size ≥ 2 and n to be the aforementioned number of fixed points.. Then

$$|\Omega| = n \sum_{x \in I} |G : G_x| \,.$$

As G is a finite p-group, we know $|G : G_x| \geq 2$, hence $|G : G_x| = p^m$ for some m, hence $p \mid |G : G^x|$, so

$$\begin{aligned} |\Omega| &\equiv n + \sum_{x \in \mathscr{O}} |G : G_x| \,(\mod p) \\ &\equiv n + 0 \,(\mod p) \\ &\equiv n \,(\mod p) \,. \end{aligned}$$

□

Lemma 4.2. Let G be finite group, p be prime, P is a sylow p-group in G. If $H \leq N_G(P)$ then $H \leq P$.

Proof. Since $H \leq N_G(P)$ we must have $HP \leq G$ with $P \trianglelefteq HP$. Hene $\frac{HP}{P} \simeq \frac{H}{H \cap P}$ by the 2nd isomorphim theorem. Thus, $\underbrace{\left|\frac{HP}{P}\right|}_{= \frac{|HP|}{|P|}} = \left|\frac{H}{H \cap P}\right| = \frac{|H|}{|H \cap P|}$. This yields $|HP| = \frac{|H| \cdot |P|}{|H \cap P|}$.
Since $|H|$ and $|P|$ are both powers of p, we have $|H| \cdot |P|$ is also a power of p. By definition $p^n = |P|$ is the maximum power of p dividing $|G|$, so $|HP| \leq p^n = |P|$ by lagranges theorem, but $p \leq HP$, so $|P| \leq |HP| \leq |P|$, hence $|P| = |HP|$ and since there is only 1 P-coset, we see $HP = P$ implies $H \leq P$. □

Theorem 4.3 (Sylow Theorems)**.** Let G be a finite group, p a prime with n_p being the number of sylow p-groups in G.

1. $n_p \geq 1$ for all p.
2. If $H \leq G$ is a p-group, then there exists a sylow p-group, $P \leq G$ with $H \leq P$.
3. All sylow p-groups are conjugate.
4. $n_p \equiv 1 \,(\mod p)$.
5. $n_p = |G : N_G(P)|$ where P is a sylow p-group in G. In partiuclar, $n_p \mid \frac{|G|}{p^n}$.

Proof. 1. We have already proved this theorem

2. Let P be a sylow p-group in G (which we know to exist). Let $\Omega = \{A : A \text{ is a subgroup conjugate to } P\}$. Let G act by conjugation on Ω. Then, as Ω is simply one orbit, $|\Omega| = |G : G_P|$ where $G_P = \{g \in G : gPg^{-1} = P\} = N_G(P)$. Hence, $|\Omega| = |G : N_G(P)|$. As $P \leq N_G(P)$ and $|P| = p^n$ is the maximum power of p such that $p^n \mid |G|$, then by definition of a sylow group, $p \nmid |\Omega| = |G : N_G(P)|$. Let $H \leq G$ be a p-group in G. Then, restrict the action of G on Ω to an action of H on Ω. By the previous lemma, we have the number of fixed points in Ω under the action of H, denoted m is $m0 \,(\mod p)$.
   Thus, there is some $P' \in \Omega$ that is a fixed point for H, meaning $hP'h^{-1} = P'$ for all $h \in H$, hence $H \leq N_G(P')$. Now, P' is conjugate to P as $P' \in \Omega$, so $P' \simeq P$ with $|P'| = |P| = p^n$. So, P' is also a sylow p-group in G.
   Taking the preivous lemma and applying it to P' yields $H \leq P'$, so this completes the proof of (2). □

The rest of the proofs will be completed next lecture.

Lecture 8: Sylow Groups (3)

Fri 10 Sep 2021 11:23

Recall. We proved Sylow's 2nd theorem, that every p-group in G is contained within some p-group.

3rd and 4th theorems. 3. Recall we let G act on Ω, being the set of all subgroups conjugate to P, be conjugation and we shoed any p-group $P' \leq G$ has some $p'' \in \Omega$ such that $p' \leq p''$.
   Now, let p' be an arbitrary sylow p-group. By the above we have the existence of a $p'' \in \Omega$ such that $p' \leq p''$. But $|p'| = |P''| = p^n$ as this is the maximum power of p dividing $|G|$ by definition of sylow groups.
   Hence $p' = p'' \in \Omega$, so p' is conjugate. Hence, every sylow p-group is conjugate to the fixed sylow p-group so they are all conjugate by transitivity.

4 Now that we know all sylow p-groups are conjugate, we know there is a $n_p = |\Omega|$ with Ω being a single orbit in the action of G on Ω. So, the orbit

stabilizer lemma yields

$$n_p = |\Omega| = |G : G_p| \text{ where } G_P = \{x \in G : P^x = P\} \quad = \{x \in G : xPx^{-1} = P\}$$
$$= N_G(P).$$

Now, we restrict the action of G on Ω to an action of P on Ω. Hence, P is a p-group, hence finite, acting on the finite set Ω. And, as we know the number of fixed points $n_p = |\Omega| \pmod p$.
So, we must only examine the fixed points now. Let $P' \in \Omega$ be an arbitrary subgroup such that P' is fixed by all $x \in P$. That is, $xP'x^{-1} = P'$. If $P' = P$ this is clearly true. By definition, we know $P \in N_G(P')$, but by an earlier lemma, we know that $P \leq P'$, both were p-groups of maximal cardinality so both sylow groups are equal. Hence, $P' = P$ is the only fixed point. This completes the proof as $n_p \equiv 1 \pmod p$.

□

Theorem 4.4. Let G be a group with $|G| = p^2$ with p being prime. Then, G is abelian.

Remark. This is a generalization of the theorem that every group of order p is cyclic, hence abelian.

Lemma 4.3. If G is a finite nontrivial p-group, then $Z(G)$ is nontrivial.

Proof of lemma. By the class equation

$$|G| = |Z(G)| + \sum_{x \in I} |G : Z_G(x)|.$$

But, as each $Z_G(x)$ with $x \in I$ has $p \mid |Z_G(x)|$ hence $p \mid |Z(G)|$. We have actually already argued this same fact before, so the details are omitted. Hence, as $p \mid |Z(G)|$, then $Z(G)$ is nontrivial. □

Proof of theorem. $Z(G)$ is nontrivial by the lemma, hence $|Z(G)| = p$ or $|Z(G)| = p^2$ by lagrange's theorem. In the second case G is abelian hence we need only examine the case $|Z(G)| = p$. As groups of order p are cyclic, any nonidentity element $x \in Z(G)$ will be a generator. Now, we know $Z(G) \trianglelefteq G$ and $|G/Z(G)| = \frac{p^2}{p} = p$, so $G/Z(G)$ is also a group of order p, let it be generated by $xZ(G)$, where $x \in G$. Then, $G = \langle Z(G), x \rangle$. So, any arbitrary element of g is a product xy with $y \in Z(G)$, and as x commutes with everything in $Z(G)$, we have $xy = yx$. □

Theorem 4.5. Suppose G is a group and $|G| = pq$ for distinct primes $p < q$ with $p \nmid q - 1$. Then, G is abelian.

Proof. Let P, Q be sylow p-groups and q-groups respectively. Let n_p to be the number of sylow p-groups in G and similarly for n_q. By sylow's theorems, we know $n_{p \mid \frac{|G|}{p}}$. So, $n_p = 1$ or q and $n_p \equiv 1 \pmod p$. If $n_p \equiv q \equiv 1 \pmod p$,

this is a contradiction as $p|q-1$. $\lightning$ Hence, $n_p = 1$. Likewise, $n_q|\frac{|G|}{q} = p$, so $q \equiv 1$ or $p\,(\mod p)$ and if $n_q \equiv p \equiv 1\,(\mod q) = 1$, then $p = xq+1$ for some positive x, hence $p \geq q+1$. $\lightning$. So $n_q = 1$.
This means every $g \in G$ fixes the unique sylow q-grop Q by conjugation ($gQg^{-1} = Q$), hence $Q \trianglelefteq G$ and likewise $P \trianglelefteq G$.
Consider the subgroup PQ. Since P, Q are normal $P \leq N_G(Q) = G$ and $Q \leq N_G(P) = G$, so PQ is a subgroup by the 2nd homomorphism theorem. Furthermore, $|P| \mid |PQ|$ and $|Q| \mid |PQ|$. Hence, $pq \mid |PQ| \leq pq$. Thus, $PQ = G$. Now, $|P| = P$, so $P = \langle x \rangle$ for some $x \in G$ and $|Q| = q$, so $Q = \langle y \rangle$ for some $y \in C$. As p, q are prime these groups are cyclic hence abelan. So, we need only show $xy = yx$. We see $yxy^{-1} = x' \in P$ as $P \trianglelefteq G$. Hence, $yx = x'y = y'x'$ for some $y' \in Q$ as $Q \trianglelefteq G$. As $PQ = G$ with $|P| = p$ and $|Q| = q$, hence $|G| = pq$ so each element $x \in G$ has a unique expression $x = ab$ with $a \in P$ and $b \in Q$. Hence $x = x'$ and $y = y'$, so $xy = yx$. □

Remark. It is a general technique that if a sylow group is unique, it is normal in G.

Lecture 9: Semidirect Products and Basic Results

Mon 13 Sep 2021 11:26

5 Semidirect Products

Definition 5.1 (Direct Product)**.** Let H, N be groups. Their (external) **direct product** is $N \times N = \{(x,h) : x \in N, h \in H\}$ with $(x_1,h_1)(x_2,h_2) = (x_1x_2, h_1h_2)$.

Definition 5.2 (Semidirect Product)**.** Let H, N be groups and let $\alpha : H \to (N)$. Thus H acts on N by $x^h = \alpha(h)(x)$. We define the (external) **semidirect product** to be $N \rtimes_\alpha H = \{(x, h : x \in N, h \in H)\}$. This forms a group with $(x_1,h_1)(x_2,h_2) = \left(x_1, x_2^{h_1}, h_1h_2\right)$

Let us verify this is a group. We see this is a well defined map as H is closed and $x_2^{h_1} \in N$ and N is closed. Now, let us find the identity. We see $(1,1)$ has $(x,h)(1,1) = \left(x1^h = h_1\right) = (x,h)$ and $(1,1)(x,h) = \left(1x^1, 1h\right) = (x,h)$. Hence,

$(1,1) = e$ is the identity. Next, the inverse of (x,y) is $\left(x^{-1}\right)^{h^{-1}}, h^{-1}$. We see

$$\begin{aligned}
(x,y)\left(\left(x^{-1}\right)^{h^{-1}}, h^{-1}\right) &= \left(x\left[\left(x^{-1}\right)^{h^{-1}}\right]^{h}, hh^{-1}\right) \\
&= \left(x\left(x^{-1}\right)^{hh^{-1}}, 1\right) \\
&= \left(x\left(x^{-1}\right)^{1}, 1\right) \\
&= \left(xx^{-1}, 1\right) \\
&= (1,1) \text{ and} \\
\left(\left(x^{-1}\right)^{h^{-1}}, h^{-1}\right)(x,h) &= \left(\left(x^{-1}\right)^{h^{-1}} x^{h^{-1}}, h^{-1}h\right) \\
&= \left(\left(x^{-1}x\right)^{h^{-1}}, 1\right) \text{ By } h^{-1} \text{ being an homo(auto)morphism} \\
&= \left(1^{h^{-1}}, 1\right) \\
&= (1,1)
\end{aligned}$$

.

We see this holds as $(xy)^h = \alpha(h)(xy) = \alpha(h)(x)\,\alpha(h)(y) = x^h y^h$.
Lastly, let us show associativity. Let $(x_1,h_1),(x_2,h_2)(x_3,h_3) \in N \rtimes H$. Then,

$$\begin{aligned}
((x_1,h_1)(x_2,h_2))(x_3,h_3) &= \left(x_1 x_2^{h_1}, h_1h_2\right)(x_3,h_3) \\
&= \left(x_1 x_2^{h_1}(x_3)^{h_1h_2}, h_1h_2h_3\right) \\
(x_1,h_1)((x_2,h_2)(x_3,h_3)) &= (x_1,h_2)\left(x_2x_3^{h_2}, h_2h_3\right) \\
&= \left(x_1\left(x_2x_3^{h_2}\right)^{h_1}, h_1h_2h_3\right) \\
&= \left(x_1x_2^{h_1}x_3^{h_1h_2}, h_1h_2h_3\right).
\end{aligned}$$

Hence this is indeed a group. Lastly, let us observe $|N \rtimes H| = |N|\,|H|$.
Now, note that $N \times \{1\}$ has $(x,1)(y,1) = \left(xy^1, 1\cdot_1\right) = (xy,1)$ so $N \times \{1 \simeq N\}$.
Hence, we often refer to N as having $N \leq N \times H$ even though it is techinically $N \times \{1\} \leq N \rtimes H$. Likewise $\{1\} \rtimes H$ has $H \leq N \times H$.
The reason this is of interest is that N is normal in $N \rtimes H$, with the notation being purposely similar to $N \lhd H$ in order to remind one which group will be

normal. We see for $(x,1) \in N$ and $(y,h) \in N \rtimes H$ we have

$$\begin{aligned}
(y,h)(x,1)(y,h)^{-1} &= (y,h)(x,1)\left(\left(y^{-1}\right)^{h^{-1}}, h^{-1}\right) \\
&= \left(yx^h, h\right)\left(\left(y^{-1}\right)h^{-1}, h^{-1}\right) \\
&= \left(yx^h\left(\left(y^{-1}\right)^{h^{-1}}\right)^h, hh^{-1}\right) \\
&= \left(yx^h\left(y^{-1}\right)^{hh^{-1}}, 1\right) \\
&= \left(yx^hy^{-1}, 1\right) \\
&\in N.
\end{aligned}$$

Se N is indeed normal in $N \rtimes H$.
If $\alpha : H \to (N)$ being the trivial homomorphism, we see every element is the identity map, hence $N \rtimes H = N \times H$.

Theorem 5.1. Let H, N be groups with $\alpha : H \to (N)$ being a homomorphism. $H \trianglelefteq N \rtimes_\alpha H \Leftrightarrow N \rtimes_{alpha} H = N \times H$.

Proof. Assume $H \trianglelefteq N \rtimes_\alpha H$. So, $(x,1)(1,h)\left(x^{-1},1\right) = (1,h') \in H$ for all $x \in N$ and $h \in H$. Then,

$$\begin{aligned}
(x,1)(1,h)\left(x^{-1},1\right) &= \left(x \cdot 1^1, 1 \cdot h\right)\left(x^{-1},1\right) \\
&= (x,h)\left(x^{-1},1\right) \\
&= \left(x\left(x^{-1}\right)^h, h\right) \\
&= (1,h') \\
&.
\end{aligned}$$

Implying $h = h'$ and $\left(x^{-1}\right)^h = x^{-1}$, for all $h \in H$. Then, as every h acts as the trivial map, we see this is simply the special case yielding the direct product. The other direction of the proof is left as an exercise. □

Definition 5.3 (Internal Semidirect Products)**.** Let G be a group with $H, N \leq G$ and suppose $H \leq N_G(N)$ and $H \cap N = \{1\}$. Then $NH \simeq N \rtimes_\alpha H$ where $\alpha : H \to (N), h(x) \mapsto \alpha(h)(x) = hxh^{-1}$. We define this to be the **internal semidirect product**.

Lecture 10: Semidirect Products (2)

Wed 15 Sep 2021 11:26

Recall. We introduced the semidirect product $G \rtimes_\alpha H$ with $(x,h)(y,g) = \left(xy^h, hg\right)$.

Theorem 5.2. Let G be a group with $H, N \leq G$ and $H \leq N_G(N)$ and $H \cap N = \{1\}$.. Then, $NH \simeq N \rtimes_\alpha H$ is a group when

$$\begin{aligned} \alpha : H &\longrightarrow (N) \\ h &\longmapsto \alpha(h) = \text{conjugation by } h. \end{aligned}$$

Proof. Since $H \leq N_G(N)$ this implies $NH \leq G$ with $N \trianglelefteq NH$ (by the 2nd isomorphism theorem). Furthermore, $\frac{NH}{N} \simeq \frac{H}{N \cap H}$. As the intersection is trivial, we see $|NH : N| = \frac{|NH|}{|N|} = |H|$, hence $|NH| = |N|\,|H|$. So, there are $|H|$ N-cosets in NH.
But $NH = \{xh : x \in Nh \in H\} = \bigcup_{h \in H} Nh$ and as there are $|H|$ N-cosets, we see each Nh is distinct. Hence, every element has a unique representation of the form xh with $x \in N$ and $h \in H$. Thus, the map $\varphi : NH \to N \rtimes_\alpha H$, with $xh \mapsto (x, h)$ is well defined (as there is only 1 way to represent each element) and bijective. Last, we must show it is a homomorphism. Let $x_1h_1, x_2h_2 \in NH$ be arbitrary elements with $x_1, x_2 \in N$ and $h_1, h_2 \in H$.
Then

$$\begin{aligned} x_1h_1x_2h_2 &= x_1h_1x_2h_1^{-1}h_1h_2 \\ &= x_1x_2^{h_1}(h_1h_2) \\ \text{where } x^h &\coloneqq hxh^{-1} = \alpha(h)(x) \\ \text{furthermore, } x_1x_2^{h_1} &\in N \text{ and } h_1h_2 \in H \\ \text{so, } x_1x_2h_1h_2 &= x_1x_2^{h_1}h_1h_2 \in NH. \\ \text{Hence } x_1h_1x_2h_2 \mapsto \varphi(x_1h_1x_2h_2) &= \left(x_1x_2^{h_1}, h_1h_2\right) \\ &= (x_1, h_1)(x_2, h_2) \\ &= \varphi(x_1h_1)\,\varphi(x_2h_2). \end{aligned}$$

We know G can act on itself by conjugation with

$$\begin{aligned} \alpha : G &\longrightarrow (G) \\ g &\longmapsto \alpha(g) = \text{ conjugation by } g. \end{aligned}$$

So, $\alpha : H \to (G)$ is also a homomorphism as each $\alpha(h)\,|_N$ is an automorphism of N as $N \trianglelefteq HN$ and $H \leq NH$ as $H \leq N_G(N)$.
Hence our original bijective map φ is also a homomorphism, hence $NH \simeq N \rtimes_\alpha H$. □

This implies the semidirect product, $N \rtimes_\alpha H$ is completely characterized by

- What is N isomorphic to?
- What is H isomorphic to?
- What possibilities for a homomorphism $\alpha : H \to (N)$ exist?

Hence semidirect products are a robust way to construct new nonabelian groups from a given N, H.

Example. $D_{2n} \simeq C_n \rtimes_\alpha C_2$ ◇

Definition 5.4 (Simple Groups)**.** A group G is **simple** if the only normal subgroups are $\{1\}$ and G itself (It has no proper nontrivial normal subgroups).

This definition clearly implies there are no nontrivial quotients of a simple group. The main use of simple groups is as a sort of "prime" group which allows us to decompose arbitrary groups by decomposition into simple groups by the quotient of a normal subgroup.

Example. Finite groups of prime order $\mathbb{Z}_p$ are simple. Furthermore, there are many families of finite simple groups as well as some particular sporadic groups which form the complete classification of finite simple groups. $\diamond$

Lecture 11: Homework Review and Sylow Groups (4)

Fri 17 Sep 2021 11:36

Solution to Questions 4 and 5 From Homework I

1. For question 4 part 1 we needed to show $\mathscr{O}_i^g \in \mathscr{O}$ for all i and $g \in G$. We note that if $x \in \mathscr{O}_i$, then $\mathscr{O}_i = x^H$, hence $\mathscr{O}_i^g = x^{Hg} = x^{gH} = (x^g)^H = \mathscr{O}_j$ for whichever $\mathscr{O}_j \ni g$.
2. For question 5 part 3 we needed to show that G_x being a maximal subgroup for every $x \in G$ is equivalent to the existence of no trivial blocks $B \subseteq \Omega$. One direction was simple, so we only show the other. Assume there is a $x \in \Omega$ such that $G_x < H < G$ for some $H \leq G$, then we wish to find a nontrivial block B.
   Define $B = x^H = \{x^h : h \in H\}$. First, we show this is a block. Suppose $B \cap B^g \neq \varnothing$, then $\exists x^{h_1} \in B$ and $x^{gh_2} \in B^g$ for some $h_1, h_2 \in H$ with $x^{gh_2} = x^{h_1}$, implying $x^{h_1^{-1}gh_2} = x^{h_1^{-1}h_1} = x$. Hence, $h^{-1}gh_2 \in G_x \leq H$, so $g \in h_1 H h_2^{-1} = H$. But, if $g \in H$, we have $B^g = \left(x^H\right)^g = x^{gH} = x^H = B$, hence B is a block and furthermore, $G_B = H$.
   Now, if $B = \{x\}$, then $G_B = H = G_x$, $\lightning$. Furthermore, if $B = \Omega$, then $B_G = H = G$, $\lightning$. Hence B is a proper nontrivial block.

Proposition 5.1. Let G be a group of order $|G| = 7 \cdot 3^3$. Then, G is not simple.

Proof. Let n_3, n_7 be the number of sylow 3-groups and 7-groups respectively. Then, by Sylow's Theorems $n_7 | \frac{|G|}{7} = 3^3$, and $n_7 = 1 (\mod 7)$. So, $n_7 = 1, 3, 9, 27$ by the first requirement, and the second requirement implies $n_7 = 1$. Hence there is a unique Sylow 7-group, hence it is normal by an earlier proposition. Thus, there is a normal subgroup of order 7, so G is not simple. Note that had we dried with n_3 instead of n_7, we would get $n_3 | 7$ and $n_3 = 1 (\mod 3)$ implying that n_3 could be 7, hence only 1 direction worked. □

Example. We can show that no group of $|G| = 30$ is simple. Suppose $|G| = 2 \cdot 3 \cdot 5$, using n_2 yields essentially no results as all other primes are odd. Hence, we try with n_3, this yields possibilities $n_3 = 1$ or $n_3 = 10$. If $n_3 = 10$, we know G is not simple, so let us assume $n_3 = 10$.
Now, trying with n_5 yields $n_5 = 1$ or $n_5 = 6$. Again, we know if $n_5 = 1$, then G is not simple so let us assume $n_5 = 6$.
Let P_1, P_2 be 2 sylow 3-groups. Then, either $P_1 = P_2$ or $P_1 \cap P_2 = \varnothing$, as $|P_1| = |P_2| = 3$ is prime. Thus, the 3-groups may only intersect trivially as they are of prime order. Hence, there are at least $n_3 \cdot (3 - 1)$ elements of order 3 in G. Hence, there are at least 20 elements of order 3 in G.
Similairly, we see there must be atleast $n_5 \cdot (5 - 1)$ elements of order 5 in G hence there are 24 elements of order 5, but as no element can have order 3 and 5, and we have $|G| = 30 < 24 + 20 + 1$ (the 1 being the identity which we did not count yet), we see either n_3 or $n_5 = 1$. Hence, G cannot be simple as it must have either a normal 3-group or a normal 5-group. ◇

Lecture 12

Mon 20 Sep 2021 11:13

Recall. We showed that for a finite group G we could exploit the number of sylow p-groups, n_p to set up a congruence system with the only solution being $n_p = 1$ for some p, hence G was not simple (as $n_p = 1$ guarantees the corersponding p-group to be normal). Failing this, we found we could assume a sylow p-group of order p had only trivial intersection to attain a lower bound on the size of the group which was larger than $|G|$, implying once again that $n_p = 1$ for a particular p, so G was not normal.

We wish to continue this example to classify all possible groups of $|G| = 30$.
We had that either a sylow 3-group, denoted P, or a sylow 5-group, denoted Q, must be normal, hence either $P \trianglelefteq G$ or $N \trianglelefteq G$ (with $Q_G(P) = G$ or $P \leq N_G(Q) = G$). Hence PQ is a group by the 2nd homomorphism theorem. Hence as $P, Q \leq PQ$, we have $|P| = 3 \mid |PQ|$ and $|Q| = 5 \mid |PQ|$, so $15 \mid |PQ|$. Furthermore, as $P \cap Q = \{1\}$ (all nonidentity elements of P have order 3, and all or Q have order 5). As $3 \mid 5 - 1$, then we know by an earlier theorem (a group of order pq with $p \not| q - 1$ is abelian) we have an abelian group. Hence $PQ \simeq C_{15}$. Using cauchy's theorem yields an element t or order 2, then we have $t \notin PQ$ as PQ had no elements of even order. Hence, $\langle PQ, t\rangle = G$.
Let $H = \langle t\rangle \simeq C_2$ and let $N = PQ \simeq C_{15}$. Clearly, $N \trianglelefteq G$ and $H \cap N = \{1\}$. By another theorem from class, we have that $G = HN \simeq N \rtimes_\alpha H$ by some automorphism $\alpha : C_2 \to (C_{15})$.It remains only to determine what automorphisms α are possible in this case. As $C_2 = \{1, x\}$ for some x of order 2, then we see α is completely characterized by the value of $\alpha(x)$ and as

$$\underbrace{\alpha\left(t^2\right)}_{=\alpha(1)=1} = (\alpha(t))^2$$

we see $(\alpha(t)) \mid 2$.
Now note that

$$\begin{aligned}(C_{15}) &= (C_3 \times C_5)\\ &\simeq (C_3) \times (C_5)\\ &= C_2 \times C_4\end{aligned}$$

and as there are 4 elements in $C_2 \times C_4$ of order 1 or 2, we have at most 4 possible automorphisms α (though some could give rise to isomorphic groups). It turns out that there are 4 such automorphisms, yielding nonisomorphic groups $C_{30}, D_{30}, C_3 \times D_{10}, C_5 \times S_3$.
We now introduce a second trick for inducing normal subgroups by exploiting low-index subgroups.

Proof. Assume G is finite and $H \leq G$ with $|G : H| = k$, k being sufficiently small. Let G act on the left H-cosets by left multiplications. This is of course transitive as $aH \mapsto bH$ by ba^{-1}.
Let $\alpha : G \to S_k$ be the associated homomorphism. If $\ker(\alpha) = G$, then there is a $g \in G$ such that $x^g = 1$ hence $k = 1$ by transitivity, hence $\ker(\alpha) = G \Leftrightarrow H = G$. Similairly, if $\ker(\alpha) = \{1\}$, then α is an injection. Thus, $G \leq S_k$ up to isomorphism. Hence, knowledge of the subgroups of S_k may yield that $G \trianglelefteq S_k$, hence

a contradiction. If we have a contradiction, then $\{1\} < \ker(\alpha) < G$, so we have a nontrivial normal subgroup.
One easy way to exploit this is to compare $|G|$ and $|S_k| = k!$. Clearly, $|G| \mid k!$ or $G \not\leq S_k$. So, if $|G| \mid k!$ we have the kernel is nontrivial so there is a proper nontrivial subgroup $K = \ker(\alpha) \trianglelefteq G$. □

Example. Recall that $n_p = |G : N_G(P)|$ where P is a sylow p-group. Hence, if n_p is small (but larger than 1), we can use $N_G(P)$ to be our group of small index. ◇