Algebraic Theory I

Thomas Fleming

November 19, 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 $|H| \mid |G|$ (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 $\operatorname{ord}(g)$ and we define $g^0 := 1$ 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 $\mathrm{Aut}\,(G)$ 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 $f \in \mathrm{Aut}\,(G)$ is called an **automorphism** of G. The group operation is usually denoted, for $f, g \in \mathrm{Aut}\,(G)$, $x \in G$, 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 $\alpha, \beta, \alpha\beta \in \mathrm{Aut}\,(G)$.

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

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

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

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 $\alpha : G \to \operatorname{Perm}(\Omega)$. 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,

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

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

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

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. $\diamond$

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 $\alpha : G \to \text{Perm}\,(G)\,,\ x \mapsto (\alpha(g))\,(x) \coloneqq x^g$, 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 $G_{x^g} = gG_xg^{-1}$ for all $x \in \Omega$, $g \in G$.

Proof.

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

□

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

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

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 $\operatorname{Im}(f) = \mathscr{O}_x$. Now, if we prove the map is injective, we have a bijection from the $[G : G_x] \to \mathscr{O}_x$. Now, suppose $f\left(gG_x\right) = f\left(hG_x\right)$, 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
$G_x = \{g \in G : gxg^{-1} = x^g = x\} = Z_G\left(\langle x \rangle\right)$.
Hence,

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

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 $Z\left(x\right) = Z\left(G\right)$. ◇

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 $\alpha : G \to \text{Perm}(G) \simeq S_2$. 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 $H \trianglelefteq G$. $\square$

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. $\square$

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 $H \trianglelefteq G$. $\square$

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 $\operatorname{ord}(g) = p$ 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 $\operatorname{ord}(x) = p$ as $\operatorname{ord}(x) \mid |G|$ 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 $|H| = \operatorname{ord}(x)$. So, $\{H = x, x^2, \ldots, x^{\operatorname{ord}(x)}\}$. If $p \mid |H|$, then $\operatorname{ord}\left(x^{|H|/p}\right) = p$, so such an element exists. In the other case $(p \nmid |H|)$. Then, $p|\,|G/H|$ as $p|\,|G| = |G/H| \cdot |H|$. 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 $p|\,|G/H|$ so the inductive hypothesis implies there is a $y \in G$ such that $\operatorname{ord}(\varphi_H(y)) = p$. Let $m = \operatorname{ord}(y)$. Then, $y^m = 1$, so $\varphi(y^m) = \varphi(y)^m = 1$, so $\operatorname{ord}(\varphi(y)) = p \mid m$ (and $m = \alpha p$). Hence, $\operatorname{ord}(y^\alpha) = p$. 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. $\square$

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. $\lightning$. □

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. ◇

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 $\operatorname{ord}(x) = p$. 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 $|H/\langle x \rangle| = \frac{|H|}{p} = p^{n-1} \Rightarrow |H| = p^n$. □

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 $n \equiv |\Omega| \pmod p$

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

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

□

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. $n_p \equiv 1 \pmod p$.
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 $m0 \pmod p$.
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

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

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. $\square$

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 $xy = yx$. $\square$

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 $n_{p| \frac{|G|}{p}}$. 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 $p \pmod{p}$ and if $n_q \equiv p \equiv 1 \pmod{q} = 1$, 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 $xy = yx$. $\square$

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 $(x_1, h_1)(x_2, h_2) = (x_1 x_2, h_1 h_2)$.

Definition 5.2 (Semidirect Product)**.** Let H, N be groups and let $\alpha : H \to \mathrm{Aut}(N)$. 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 $(x_1, h_1)(x_2, h_2) = \left(x_1, x_2^{h_1}, h_1 h_2\right)$

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,

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

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 $N \triangleleft H$ 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 $\alpha : H \to \operatorname{Aut}(N)$ 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 $\alpha : H \to \operatorname{Aut}(N)$ 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. $\square$

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 $\alpha : H \to \mathrm{Aut}(N), h(x) \mapsto \alpha(h)(x) = hxh^{-1}$. 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

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

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

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

We know G can act on itself by conjugation with

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

So, $\alpha : H \to \operatorname{Aut}(G)$ 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 $\alpha : H \to \operatorname{Aut}(N)$ 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. ◇

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 $g \in h_1Hh_2^{-1} = H$. 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 $n_7 = 1 \pmod 7$. 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 $n_3 = 1 \pmod 3$ implying that n_3 could be 7, hence only 1 direction worked. $\square$

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. $\diamond$

Lecture 12: Classification of Finite Groups

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 $\alpha : C_2 \to \mathrm{Aut}\,(C_{15})$.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 $\mathrm{ord}\,(\alpha\,(t)) \mid 2$.
Now note that

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

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. ◇

Lecture 13

Fri 24 Sep 2021 11:30

I originally missed this lecture so it is transcribed from a classmates notes.

6 Nilpotent Groups

Lecture 14: Nilpotent Groups

Fri 24 Sep 2021 11:30

Let G be a group, and $Z_0(G) = \{1\}$ with $Z_1(G) = Z(G)$. Thus, $G/Z_1(G)$ is a group which has $Z(G/Z_1(G)) = \frac{Z_2(G)}{Z_1(G)}$ where $Z_2(G)$ is the preimage of $Z(G/Z_1(G))$, that being the subgroup of G containing $Z_1(G)$. We see we may continue

$$\begin{aligned} Z_2(G)/Z_1(G) &= Z(G/Z_1(G)) \\ \text{then, } (G/Z_1(G))/(Z_2(G)/Z_1(G)) &\simeq G/Z_2(G) \\ \text{which has a center } Z(G/Z_2(G)) &= Z_3(G)/Z_2(G). \end{aligned}$$

Definition 6.1 (Nilpotence)**.** We recursively define $Z_i(G)$ to be the subgroup such that $Z(G/Z_i(G)) = Z_i(G)/Z_{i-1}(G)$. This yields a growing sequence $Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \ldots$. We say a group G is **nilpotent** if $G = Z_n(G)$ for some $n \geq 0$. The minimal $n \geq 0$ for which this is the case is called the **nilpotent class** of G.

Example. The trivial group $\{1\}$ is nilpotent with class $c = 0$.
A nontrivial abelian group is nilpotent with class $c = 1$.
◇

Theorem 6.1. Every finite p-group is nilpotent.

Proof. We know the center of a nontrivial p-group to be nontrivial and its subgroups and quotient groups will also be p-groups. Hence $Z_1(G)$ is nontrivial except in the case G is trivial. Hence we have that $Z_2(G)/Z_1(G)$ is nontrivial unless $Z_2(G) = G$. Hence either $Z_1 < Z_2$ or $Z_2 = G$. Now, denote $|G| = n$. Then either $1 = |Z_0| < |Z_1| < \ldots < |Z_n|$ hence $Z_n = G$ or $Z_i = G$ for some $i < n$, so $Z_n = G$. Hence, G is nilpotent. ☐

Definition 6.2. A subgroup $H \leq G$ is **characteristic** if for every automorphism of G, we have $\alpha(H) = H$. This is equivalent to $\alpha(H) \leq H$ for all automorphisms as $\alpha^{-1} : G \to G$ is also an automorphism, hence $H \leq \alpha(H)$, so equality holds. Since conjugation is always an automorphism, being characteristic implies normality.

Proving vs. Using Characteristicness

This means that in order to show that something is characteristic we need only show $\alpha(H) \leq H$, but when we use that something is characteristic we will often use the full equality.

Lemma 6.1. As we know $K \trianglelefteq H$ and $H \trianglelefteq G$ does not imply $K \trianglelefteq G$. On the other hand, K being characteristic in H and $H \trianglelefteq G$ does yield $K \trianglelefteq G$.

Proof. Let $\alpha_x : G \to G$ be the conjugation by x map. We know this to be an automorphism of G, hence as H is normal, we have $\alpha_x|_H : H \to H$ is an automorphism of H, and since K is characteristic in H, we see an automorphism of H fixed K, hence $\alpha_x(K) = xKx^{-1} = K$ for all $x \in G$, hence $K \trianglelefteq G$. ☐

Lemma 6.2. Let G be a finite group with p being prime and P being a sylow p-group in G. Then, the following are equivalent

1. P is the unique sylow p-group in G.
2. $P \trianglelefteq G$.
3. P is characteristic in G.
4. Any subgroup generated by elements whose orders are each powers of p is itself a p-group.

Proof.
1. We have already shown $1 \Leftrightarrow 2$.
2. As conjugation is always an automorphism, we see $2 \Leftarrow 3$ is trivial.
3. We show $1 \Rightarrow 3$. Let $\alpha : G \to G$ be an arbitrary automorphism of G. Then, $\alpha(P) \leq G$ and $|P| = |\alpha(P)|$. As P is the unique sylow p-group, we see there is no distinct group of cardinality $|P|$, hence $\alpha(P) = P$.
4. Now we show $1 \Rightarrow 4$. Let X be a set satisfying $\text{ord}(x) = p^n$ for each $x \in X$. Then each $\langle x \rangle$ is contained in a p-group, and as there is a unique maximal p-group, we have that $\langle x \rangle \subseteq P$ for each $x \in X$. Hence, $\langle X \rangle \subseteq P$ and as X is a p-group we have that $X = P$.
5. $4 \Rightarrow 1$. Let X to be the union of all sylow p-groups in G. By hypothesis, $\langle X \rangle$ is a p-group and thus it is contained in some sylow p-group so WLOG, we have $\langle X \rangle \subseteq P$. But if there were distinct p-groups, $P' \neq P$ then $P' \subseteq X$ and $P \subset \langle P' \cup P \rangle \subseteq X \subseteq P$. ↯. Hence P is the unique sylow p-group.

□

Lecture 15: Nilpotent Groups (2)

Tue 28 Sep 2021 17:46

Lemma 6.3. If H, K are groups, then $Z(H \times K) = Z(H) \times Z(K)$.

Proof. Let $(x, y) \in H \times K$. If $(x, y) \in Z(H \times K)$ then

$$\underbrace{(a,1)(x,y)(a,1)^{-1}}_{=(axa^{-1},1)} = (x,y).$$

Hence, $x \in Z(H)$ and similarly, $y \in Z(K)$. Hence, $Z(H \times K) \subseteq Z(H) \times Z(K)$. The other direction of inclusion is trivial and left as an exercise. □

Lemma 6.4. Let $\varphi : G \to G'$ be a homomorphism with $\ker(\varphi) = K$ and $H \leq G$ such that $K \leq H$. Then, $N_G(H) = f^{-1}(N_{G'}(\varphi(H)))$.

Proof. Let $x \in N_G(H)$, so $xHx^{-1} = H$. Hence,

$$\varphi(H) = \varphi\left(xHx^{-1}\right) = \varphi(x)\varphi(H)\varphi(x)^{-1}.$$

Thus,

$$\begin{aligned}
\varphi(x) &\in N_{G'}(\varphi(H)) \\
\Rightarrow x &\in \varphi^{-1}(N_{G'}(\varphi(H))) \\
\Rightarrow N_G(H) &\subseteq \varphi^{-1}(N_{G'}(\varphi(H))).
\end{aligned}$$

Conversely, let $x \in \varphi^{-1}(N_{G'}(\varphi(H)))$, hence $\varphi(x) \in N_{G'}(\varphi(H))$.
Then, we see

$$\begin{aligned}
\varphi(H) &= \varphi(x)\varphi(H)\varphi\left(x^{-1}\right) \\
&= \varphi\left(xHx^{-1}\right) \\
\Rightarrow xHx^{-1} &\subseteq \varphi^{-1}(\varphi(H)) \\
&= \langle H, \ker(\varphi)\rangle \\
&= H \text{ as } \ker(\varphi) \subseteq H.
\end{aligned}$$

Hence, $xHx^{-1} \subseteq H$, so $x \in N_G(H)$. This concludes the proof. □

Now, recall that if G is a finite group with P being a sylow p-group, then TFAE

1. P is unique.
2. $P \trianglelefteq G$.
3. P is characteristic.
4. Any subgroup generated by elements whose orders are powers of p is itself a p-group.

Theorem 6.2. If G is a finite group, then the following are equivalent:

1. G is nilpotent.
2. $H < G \Rightarrow H < N_G(H)$.
3. All sylow p-groups are normal.
4. G is the direct product of its sylow p-groups.

Proof.

- $(2 \Rightarrow 3)$. Let P be a sylow p-group of G. Assume P is not normal, then denote $N = N_G(P) \subset G$. Hence, by the preceding lemma, P is characteristic in N. Then, as $N \trianglelefteq N_G(N)$, we see $P \trianglelefteq N_G(N)$. But $N = N_G(P)$ was the largest subgroup in which P was normal, hence $N_G(P) = N_G(N)$. So, by contrapositive of the assumption, (2), we have $N = N_G(N)$, so $N = G$, hence $P \trianglelefteq G$.
- $(3 \Rightarrow 4)$.
- $(1 \Rightarrow 2)$. Let G be nilpotent. If G is abelian, then $N_G(A) = G$ for all $A \leq G$, hence any proper subgroup $H < G$ has $H < N_G(H) = G$. Hence, assume G is non-abelian and proceed by induction on $|G|$ with base case $|G| = p$ being already completed p-prime. Suppose indirectly that there is an $H < G$ such that $H = N_G(H)$.
  Now, we note that $Z(G) \leq N_G(H) = H$ by definition of $Z(G)$. That is, $Z(G) \leq H$. Let $\varphi : G \to G/Z(G)\,,\ x \mapsto \varphi(x) = xZ(G)$. Since G is nilpotent, $Z(G) = 1 \Leftrightarrow G = 1$, but we assumed G to be nonabelian, so this is not the case. Hence, we can assume $Z(G) = \{1\}$, hence $|G/Z(G)| < |G|$.
  As we know, G being nilpotent implies $G/Z(G)$ is nilpotent. Lastly, we note that $Z(G) \leq H < G$, so by the lattice theorem, we have $H/Z(G) < G/Z(G)$. Applying the induction hypothesis yields $H/Z(G) < N_{G/Z(G)}(H/Z(G))$.
  Recalling the lemma from last class, $\varphi^{-1}\left(N_{G/Z(G)}(H/Z(G))\right) = N_G(H)$.
  Then, we note
  $$\varphi^{-1}(\varphi(H)) < \varphi^{-1}\left(N_{\varphi(G)}(\varphi(H))\right) = N_G(H).$$
  And as $\ker(\varphi) = Z(G) \leq H$, we have $H < N_G(H)$.

$\square$

Lecture 16: Nilpotent Groups (3)

Wed 29 Sep 2021 11:25

Corollary 2. A finite abelian group is the direct product of its sylow groups.

This follows directly from the theorem from last class.

Corollary 3. If G is a finite group such that for all $n \mid |G|$ such that there are at most n elements $x \in G$ with $x^n = 1$, then G is cyclic.

Proof. Let p be an arbitrary prime with $p \mid |G|$. Let P be a sylow p-group with $|P| = p^\alpha$. We know for any $x \in P$, we have $x^{|P|} = 1$, hence there are $|P| = p^\alpha$ elements $x \in P$ such that $x^{p^\alpha} = 1$. By hypothesis there is infact equality. If

there was another distinct sylow p-group we would have elements $y \notin P$ such that $y^{p^{\alpha}} = 1$. Hence, P is unique. Hence, as every p-group is unique, so normal, we see G is the product of its P-groups.
Denote $G = P_1 \times P_2 \times \dots P_t$ with the P_is being the distinct sylow p_i
$) - groupsofG$. Also, if $|P_1| = p_1^{\alpha_1}$, then all $x \in P_1$ have $\operatorname{ord}(x) \mid p_1^{\alpha_1}$ and there are at most $p_1^{\alpha_1 - 1} < p_1^{\alpha_1}$ such x with $\operatorname{ord}(x) \mid p_1^{\alpha_1 - 1}$. Since $|P| < p_1^{\alpha_1 - 1}$ we see there is an $x \in P_1$ with $\operatorname{ord}(x) = p_1^{\alpha_1} = |P|$, hence $\langle x \rangle = P_1$. So, P_1 is cyclic. Likewise, all other P_i are shown cyclic by the same argument, with $P_i = \langle x_i \rangle$. Then, the element $x = \prod_{i=1}^{t} x_i$ is a generator of G, so G is cyclic. □

Theorem 6.3 (Frattini's Argument)**.** Let G be a finite group , $H \trianglelefteq G$, $P \leq H$ being a sylow p-group in H. Then,

$$G = HN_G(P) \text{ and } |G : H| \mid |N_G(P)|.$$

Proof. Let $g \in G$, we wish to show $g \in HN_G(P)$. We know this to be a subgroup as $H \trianglelefteq G$. Let G act by conjugation on its sets. Now

$$\begin{aligned} P^g &= gPg^{-1} \\ &\leq H^g \\ &= gHg^{-1} \\ &= H \text{ by normality.} \end{aligned}$$

Then, we see as $|P^g| = |P|$, then P^g is another sylow p-group in H. And, as we know all sylow p-groups are conjugate. Hence, there is an $h \in H$ such that $P^h = P^g$. Hence, $P = P^{h^{-1}g}$, hence $h^{-1}g \in N_G(P)$. Then, we see $g \in hN_G(P) \subseteq HN_G(P)$. So, we see $G = HN_G(P)$
Now, we show the other result. Note that by the second isomorphism theorem, we have

$$G/H = (HN_G(P))/H \simeq \frac{N_G(P)}{H \cap N_G(P)}.$$

Thus, $|G : H| = |N_G(P) : H \cap N_G(P)|$. As we know this divides $|N_G(P)|$, hence $|G : H| \mid |N_G(P)|$. □

Theorem 6.4. if G is a finite group, then G is nilpotent if and only if every maximal subgroup in G is normal in G.

Lecture 17: Nilpotent Groups (4) and Solvable Groups

Fri 01 Oct 2021 11:28

Recall. We had a theorem that, for a finite group G, implied G was nilpotent if and only if all maximal subgroups are normal.

Proof.
1. ($\Rightarrow$). Let $M < G$ be a maximal subgroup, so $M < N \leq G$ implies $N = G$. Let $N_g(M)$ be the normalizer of $M<$ then $M < G$, hence $M < N_G(P)$ by the earlier characterization of finite nilpotent groups. Hence, $N_G(M) = G$. But $M < N_G(M)$ and M ix maximal, hence $N_G(M)$ if and only if M is normal.

2. ($\Leftarrow$). Assume every maximal subgroup is normal. Note that it suffies to show that all sylow groups are normal in G by the earlier characterization. Let $P \leq G$ be an arbitrary sylow p-group and let $N = N_G(P)$. Let M be a maximal subgroup containing $N_G(P)$. We know such a group exists because if we assume indirectly that P is not normal, this implies $N_G(P) < G$ as every proper subgroup of a finite group is contained in a maximal subgroup.
We now have $P \leq N_G(P) \leq M < G$ and by hypothesis, we know $M \trianglelefteq G$. Since $P \leq M$with P being a sylow group of G implies $P \leq M$ is a sylow group for M. But now we can applying the frattini argument. We see $G = N_G(P)M$ but $N_G(P) \leq M$, hence $G \subseteq MM = M < G$. $\lightning$.

$\square$

Remark. If G is nilpotent, then recall $Z_0(G) < Z_1(G) < Z_2(G) < \ldots < Z_i(G)$ is the upper central series where $Z_0(G) = \{1\}$, $Z_1(G) = Z(G)$ and $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$.
There is an alternative characterization, let $G^0 = G$, $G^1 = [G, G] = \langle x^{-1}y^{-1}xy : x, y \in G \rangle$ and define recursively $G^i = \left[G, G^{i-1}\right] = \langle x^{-1}y^{-1}xy : x \in G, y \in G^{i-1} \rangle$ to be the lower central series. Then, G is nilpotent if and only if there is $c \geq 0$ such that $G^c = \{1\}$. Furthermore, we find $G^{c-i} \leq Z_i(G)$ for all $0 \leq i \leq c$, with the minimal constant c being the same in the upper and lower central series.

7 Solvable Groups

Definition 7.1 (Solvable Groups)**.** A group G is **solvable** if there's a chain of subgroups

$$H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_n = G$$

such that H_i/H_{i-1} are abelian for $1 \leq i \leq n$.

As it turns out there is an equivalent chain condition for solvability closed to our characterizations of nilpotence. Define $G^{(0)} = G$, $G^{(1)} = [G, G] = G^1$, Now, define $G^{(i)} = \left[G^{(i-1)}, G^{(i-1)}\right] = \langle x^{-1}y^{-1}xy : x, y \in G^{(i-1)} \rangle$. So, $G^{(n)}$ is essentially the n-th iterated commutator of G. Then, we obtain a chain

$$G^{(0)} \geq G^{(1)} \geq \ldots \geq G^{(c)} \geq \ldots.$$

If $G^{(c)} = 1$ for some $c \geq 1$, then G is solvable. We show these two conditions are equivalent. The proof will involve multiple invocations of the basic result that G/H is abelian if and only if $[G, G] \leq H$.

Proof. Assume G is solvable, and the 1st characterization is true with $1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$ with H_i/H_{i-1} being abelian for all $1 \leq i \leq n$. We will show by induction that $G^{(i)} \leq H_{n-i}$ for all $1 \leq i \leq n$. For $i = 0$ we have $H_n = G$, hence $G^{(0)=G}$ and $G \leq G$, so the claim holds for $i = 0$. Now, note that

$$\begin{aligned} G^{(i)} &= \left[G^{(i-1)}, G^{(i-1)}\right] \\ &\leq \left[H_{n-(i-1)}, H_{n-(i-1)}\right] \text{ by inductive hypothesis} \\ &= \left[H_{n-i+1}, H_{n-i+1}\right] \\ &. \end{aligned}$$

We also know that H_{n-i+1}/H_{n-i} is abelian, hence we have $G^{(i)} \leq [H_{n-i+1}, H_{n-i+1}] \leq H_{n-i}$ by the preceding lemma. This completes the induction. But, we have $G^{(n)} \leq H_{n-n} = H_0 = \{1\}$, so $G^{(n)}$ is trivial. □

Lecture 18: Solvable Groups (2) and Free Groups

Mon 04 Oct 2021 11:28

Recall. A group is solvable if there exists a chain of subgroups

$$\{1\} \trianglelefteq H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$$

such that H_i/H_{i-1} is abelian.
We had that this is equivalent to the condition that $G^{(n)} = \{1\}$ where $G^{(0)} = G$ and $G^{(i)} = \left[G^{i-1}, G^{i-1}\right]$ for some $n \geq 0$. We showed the forward implication, so now we show the reverse implication.

Proof. Suppose $G^{(n)} = 1$ for some $n \geq 0$. Then, we have a chain

$$G = G^{(0)} \trianglelefteq G^{(1)} \trianglelefteq \ldots \trianglelefteq G^{(n)} = \{1\}.$$

So, we have

$$\{1\} = G^{(n)} \trianglerighteq G^{(n-1)} \trianglerighteq \ldots \trianglerighteq G^{(0)} = G.$$

Furthermore, we know the commutator of $G^{(i)}$is a characteristic subgroup, hence it is normal.
Then, define $H_i = G^{(n-i)}$ for $0 \leq i \leq n$. We need only show the quotients to be abelian. We see $H_i/H_{i-1} = G^{(n-i)}/G^{(n-i+1)}$. But, $G^{(n-i+1)} = \left[G^{(n-i)}, G^{(n-i)}\right]$ by definition. Hence, $G^{(n-i)}/G^{(n-i+1)}$ is abelian by the lemma from last class. So, the chain condition holds and G is solvable. □

Theorem 7.1. Let G be a solvable group with H being a subgroup. Then, H is solvable.

Proof. We simply show $H^{(n)} \leq G^{(n)}$ for all n by induction. For the base case we know $H = H^{(0)} \leq G^{(0)} = G$. Then, we note $H^{(n)} = \left[H^{(n-1)}, H^{(n-1)}\right] \subseteq \left[G^{(n-1)}, G^{(n-1)}\right] = G^{(n)}$ by inductive hypothesis. Since G is solvable, we find a $n \geq 0$ such that $G^{(n)} = \{1\}$. Then, $H^{(n)} \leq G^{(n)} = \{1\}$, so $H^{(n)} = \{1\}$ hence H is solvable. □

Theorem 7.2. If G is solvable and $\varphi : G \to G'$ is a homomorphism, then $\varphi(G)$ is also solvable.

Proof. We see $\varphi\left(G^{(0)}\right) = \varphi\left(G\right)^{(0)}$. So, $\varphi\left(G^{(0)}\right) = \varphi\left(G\right)^{(0)}$. We induce on n. We see

$$\begin{aligned}
\varphi\left(G^{(n)}\right) &= \varphi\left(\left[G^{(n-1)}, G^{(n-1)}\right]\right) \\
&= \varphi\left(\left\langle x^{-1}y^{-1}xy : x, y \in G^{(n-1)}\right\rangle\right) \\
&= \left\langle \varphi\left(x^{-1}y^{-1}xy : x, y \in G^{(n-1)}\right)\right\rangle \\
&= \left\langle \varphi\left(x\right)^{-1}\varphi\left(y\right)^{-1}\varphi\left(x\right)\varphi\left(y\right) : x, y \in G^{(n-1)}\right\rangle \\
&= \left\langle \overline{x}^{-1}\overline{y}^{-1}\overline{xy} : \overline{x}, \overline{y} \in \varphi\left(G^{(n-1)}\right)\right\rangle \\
&= \left\langle \overline{x}^{-1}\overline{y}^{-1}\overline{xy} : \overline{x}, \overline{y} \in \varphi\left(G\right)^{(n-1)}\right\rangle \text{ by the inductive hypothesis.} \\
&= \left[\varphi\left(G\right)^{(n-1)}, \varphi\left(G\right)^{(n-1)}\right] \\
&= \varphi\left(G\right)^{(n)}.
\end{aligned}$$

Since G is solvable, we find an $n \geq 0$ such that $G^{(n)} = \{1\}$. Hence, $\varphi\left(G^{(n)}\right) = \varphi\left(\{1\}\right) = \{1\} = \varphi\left(G\right)^{(n)}$, so $\varphi\left(G\right)$ is solvable. □

Theorem 7.3. If G is a group with $H \trianglelefteq G$, then G is solvable if and only if H and G/H are solvable.

Proof. ($\Rightarrow$). We know all subgroups and homomorphic images to be solvable, hence this direction is already proven.
($\Leftarrow$). Assume H and G/H are solvable. As H is solvable it has a normal chain

$$H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = H$$

with H_i/H_{i-1} is abelian for all $1 \leq i \leq n$. Similarly, since G/H is solvable there is a normal chain

$$\{1\} = K_{n+0} \trianglelefteq K_{n+1} \trianglelefteq \ldots K_{n+s} = G/H$$

With K_{n+i}/K_{n+i-1} being abelian for all $i \geq 1$. We know by the lattice theorem that there are groups H_{n+i} such that $K_{n+i} = H_{n+i}/H$ for some $H_{n+i} \leq G$ and $H \leq H_{n+i}$. Then, we have

$$\{1\} = H/H \trianglelefteq H_{n+1}/H \trianglelefteq \ldots \trianglelefteq H_{n+s}/H = G/H.$$

Then, we have $H_n = H$ and $H_{n+s} = G$ and, as each contains the kernel, this correspondance preserves normality, hence we have

$$H_n = H \trianglelefteq H_{n+1} \trianglelefteq H_{n+2} \trianglelefteq \ldots H_{n+s} = G.$$

Then, note that $H_{n+i}/H_{n+i-1} = \left(H_{n+i}/H\right)/\left(H_{n+i-1}/H\right) = K_{n+i}/K_{n+i-1}$ which we know to be abelian. Hence all successive quotients are abelian. So,

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n \trianglelefteq H_{n+1} \trianglelefteq H_{n+2} \trianglelefteq \ldots H_{n+s} = G.$$

with H_i/H_{i-1} being abelian, so G is solvable. □

Remark. Subgroups and quotients of nilpotent groups are nilpotent, but this converse does not hold in general for nilpotent groups.

8 Free Groups

Recall. $\langle \alpha, \tau : \alpha^n = 1, \tau^2 = 1, \tau\alpha\tau = \alpha^{-1} \rangle = D_{2n}$ is the dihedral group of order $2n$. This is technically ill defined. In general, we have generators α, τ and a set of relations that allow us to say when products of generators are equal. Similairly, we find $\langle \alpha : \alpha^n = 1, \alpha^{n+1} = 1 \rangle = \{1\}$. We have not, however, ensured that these form groups. This problem motivates the definition of free groups.

If S is a set, then we let S^{-1} be a disjoint set of formal symbols with $x \mapsto x^{-1}$, so $S = \{a, b, c\}$ and $S^{-1} = \{a^{-1}, b^{-1}, c^{-1}\}$. Then, let $F(S)$ to be the set of all formal products of elements from $S \cup S^{-1} \cup \{1\}$. Next class we will define an equivalence relation which takes these products into a group.

Lecture 19: Free Groups (2)

Wed 06 Oct 2021 11:33

Recall we had a set of letters $X = \{a, b, c, \ldots, a^{-1}, b^{-1}, c^{-1}, \ldots, 1\}$. Then, we define a word on the alphabet X to be a string $\omega = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots, x_s^{\varepsilon_s}$ where $x_1, x_2, \ldots, x_s \in X$ and $\varepsilon_i = \pm 1$. For example with $X = \{x_1, x_2, x_3\}$ we have a word $x_1 x_1 x_2 x_1^{-1} x_1 x_3$ for example. Then, define 1 to be the empty product, that being a string with no symbols. Now, we define an equivalence relation on the words to induce a group.
We say two words $\omega_1 \sim \omega_2$ if we can transform ω_1 into ω_2 with a finite sequence of the following operations

- Remove a sequential pair xx^{-1} or $x^{-1}x$ from the string.
- Insert a substring xx^{-1} or $x^{-1}x$ into the string.

So, we see $x_1 x_2 x_3^{-1} x_4 \sim x_1 x_2 x_3^{-1} x_2 x_2^{-1} x_1^{-1} x_1 x_4$ and so on. It is trivial to verify this to be an equivalence relation, so we omit the proof. Henceforth, we will denote the equivalence class of a word ω by $[\omega]$. So, we see if $\omega_1 \sim \omega_2$, we have $[\omega_1] = [\omega_2]$.
Now, let $F(X)$ be the set of all equivalence classes on X and define $[\omega_1][\omega_2] \coloneqq [\omega_1\omega_2]$ with $\omega_1\omega_2$ simply being the concatenation of the two words. First, we verify this to be well-defined. Suppose $w' \sim w$ and $v' \sim v$ are 4 words. Hence, there is a simple sequence taking $v \mapsto v'$ and $w \mapsto w'$. It is easy to see then, that the same operations applied to their respective parts will take $vw \mapsto v'w'$ and $wv \mapsto w'v'$, hence $[vw] = [v'w']$.
Next, we show this forms a group. We see $[w][1] = [w \cdot 1] = [w]$ and likewise $[1][w] = [w]$, so 1 is the identity.
Next,

$$\begin{aligned}
[w]([u][v]) &= [w][uv] \\
&= [w(uv)] \\
&= [(wu)v] \\
&= [wu][v] \\
&= ([w][u])[v]
\end{aligned}$$

.

Hence, $F(X)$ is associative. Lastly, we show inverses exist. Let $w = x_1^{\varepsilon_1} \dots x_s^{\varepsilon_s}$, then let $w^{-1} = x_s^{-\varepsilon_s} \dots x_1^{-\varepsilon_1}$ and we see $ww^{-1} \sim 1$, so $F(X)$ has inverses.

Definition 8.1 (Free Group)**.** For an alphabet X, we define $F(X)$ to be the **Free Group on** X. More generally, the free group F on X is a group F together with an injection $\sigma : X \hookrightarrow F$ such that any $\alpha : X \to G$, with G being an arbitrary group, extends to a unique homomorphism $\beta : F \to G$ such that $\beta \circ \sigma = \alpha$.

$$\begin{tikzcd} & F(X) \arrow[dr, dotted, "\beta"] & \\ X \arrow[ur, "{\sigma, x \mapsto [x]}"] \arrow[rr, "\alpha"] & & G \end{tikzcd}$$

Figure 1: In this commutative diagram solid lines represent given maps and dotted lines represent maps that must then exist

Next, recall a homomprhism $\varphi : H \to G$ is determined by the images of generators of H. Let $H = \langle X \rangle$. Then for an arbitrary $h \in H$ with $h = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ we find $\varphi(h) = \varphi(x_1)^{\varepsilon_1} \dots \varphi(x_n)^{\varepsilon_n}$ with $x_i \in X$ and $\varepsilon_i = \pm 1$.
Now, let G be a group with $\alpha : X \to G$ being a map and $\sigma : X \hookrightarrow F$ be the inclusion map. Let $w = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}$ and let $(w) = \alpha(x_1)^{\varepsilon_1} \dots \alpha(x_n)^{\varepsilon_n}$ with $x_i \in X$ and $\varepsilon_i = \pm 1$. Then, we define $\beta([w]) = [\beta(w)]$. It is simple to check this is well defined as we may always insert or delete substrings of the form $\alpha(x_i)^{\varepsilon_i} \alpha(x_i)^{-\varepsilon_i}$ in order to induce an equivalence. We see β is also a homomoprhism as

$$\begin{aligned} \beta([w][v]) &= \beta([wv]) \\ &= \beta(wv) \\ &= \beta(w)\beta(v) \\ &= \beta([w])\beta([v]). \end{aligned}$$

Lastly, we see the map β is unique as a homomoprhism is completely characterized by where it sends the generators.

Lecture 20: Free Groups (3)

Fri 08 Oct 2021 11:26

Recall. F is a free group on the set X when there is an injection $\sigma : X \overset{F}{\hookrightarrow}$ such that for all maps $\alpha : X \to G$, there is a homomorphism $\beta : F \to G$ such that $\beta \circ \sigma = \alpha$.

Remark. F is also a free group on $\sigma(X) \subseteq F$, using a similair inclusion map, so often we will assume $X \subseteq F$.

Theorem 8.1. If F_1 is free on X_1 and F_2 is free on X_2 and $|X_1| = |X_2|$, then $F_1 \simeq F_2$.

Proof. Since $|X_1| = |X_2|$ we find a bijection $\alpha : X_1 \to X_2$ and we can assume WLOG that $X_1 \subseteq F_1$ and $X_2 \subseteq F_2$. Then, the free property of F_1 implies there is a unique homomorphism $\beta : F_1 \to F_2$ such that $\beta(x) = \alpha(x)$ for all $x \in X_1$. Similairly, thee is a unique map $\gamma : F_2 \to F_1$ extending $\alpha^{-1} : X_2 \to X_1$ such that $\gamma(y) = \alpha^{-1}(y)$ for all $y \in X_2$. So, we see

$$\begin{aligned} \beta\,|_{X_1} : X_1 &\longrightarrow X_2 \\ x &\longmapsto \beta(x) = \alpha(x) \end{aligned}$$

and

$$\begin{aligned} \gamma\,|_{X_2} : X_2 &\longrightarrow X_1 \\ y &\longmapsto \gamma(y) = \alpha^{-1}(y) \end{aligned}$$

are inverses.
Hence, we have β and γ are a pair of inverse homomorphisms as X_1 generates F_1 and likewise X_2 generates F_2 .
Then, for an arbitrary element in F of the form $x = x_1^{\varepsilon_1} \dots x_\ell^{\varepsilon_\ell}$ with $\varepsilon_i \in \mathbb{Z}$ and $x_i \in X_1$, then we see $\gamma(\beta(x)) = x$, hence this completes the proof. $\square$

Theorem 8.2. Let F be a free group with H, G being groups. Suppose $\alpha : F \to H$ is a homomorphism and $\beta : G \to H$ is a surjective homomorphism. Then, there is a $\gamma : F \to G$ such that $\beta\gamma = \alpha$.

Proof. Let F be free on $X \subseteq F$. Then, each $x \in X$ has $\alpha(x) \in H = \operatorname{Im}(\beta)$. Then, there is some $g_x \in G$ such that $\beta(g_x) = \alpha(x)$. By the universal mapping property of F , we have the map $X \to G, x \mapsto g_x$ extends to a homomorphism

$$\begin{aligned} \gamma : F &\longrightarrow G \\ x &\longmapsto \gamma(x) = g_x. \end{aligned}$$

Then, for $x \in X$ we see $\beta(\gamma(x)) = \beta(g_x) = \alpha(x)$, so $\beta \circ \gamma = \alpha$ on X which generates F , so $\beta \circ \gamma = \alpha$ on F as $\beta \circ \gamma, \alpha$ are homomorphisms. $\square$

Definition 8.2 (Group Presentations)**.** Any group G is a homomorphic image of a free group F. An explicit homomorphism $\alpha : F \to G$ with F is called a **presentation** of G. Its kernel $N = \ker(\alpha) \trianglelefteq F$ has $F/N \simeq G$. So, we may write $\langle X : Y \rangle = G$ where F is a free group on X and $Y \subseteq F$ has normal closure, $\bigcap_{H \trianglelefteq G, Y \leq H} H = N$.

Example. $D_{2n} = \left\langle \alpha, \tau : \alpha^n, \tau^2, \tau\alpha\tau\alpha \right\rangle$. Here, we see F is free on the set $\{\alpha, \tau\}$ and N is the normal closure of $\left\langle \alpha^n, \tau^2, \tau\alpha\tau\alpha \right\rangle$, that being the smallest normal subgroup of F containing these three elements.
In general if $H \leq G$, then $\bigcap_{N \trianglelefteq G, H \leq N} N \trianglelefteq G$ is the normal closure of H. $\diamond$

Remark. In general, a group of relations can generate other relations that we may not account for, so it is good to know what elements in the normal closure look like. If $X \subseteq G$, we find elements in the normal closure N of $\langle X\rangle$ in G include inverses and products of elements from X. Furthermore, arbitrary conjugates and their products/inverses will be in N. We see this yields

$$N \supseteq \{\prod_{i=1}^{\ell} \left(g_i x_i g_i^{-1}\right) : \ell \geq 0, g_i \in G, x_i \in X \cup X^{-1}\}.$$

Furthermore, we see this set is in fact a normal subgroup itself, so equality holds.

Lecture 21: Homework and Free Groups (4)

Wed 13 Oct 2021 11:23

Homework II

We spent the majority of class reviewing homework problems.

Theorem 8.3. Let $G = \langle X : R\rangle$ and $H = \langle X : R'\rangle$ be groups generated by X following relations R and R' . Suppose all generators for H satisfy all defining relations for G. That is, R is a subset of R'. Then, we find H is a homomorphic image of G.

Proof. Recall $G = F(X)/N$ where N is the normal closure of R in $F(X)$ and $H = F(X)/N'$ where N' is the normal closure of R' in $F(X)$. But, since all relations on R are satisfied by H , we have $N \leq N'$. Then, since $F(X)/N' = (F(X)/N)/(N'/N) = G/(N'/N)$, hence H is a homomorphic image of G. □

Lecture 22: Free Groups (5)

Fri 15 Oct 2021 11:21

Recall. Let G, H be groups with presentations $\varepsilon : F \to G$ and $\delta : F \to H$ for some free group F, If every relator of G is also a relator for H, then there is a surjective homomorphism $\varphi : G \to H,\ \varepsilon(x) \mapsto \delta(x)$.

Definition 8.3 (Reduced Word)**.** We define a word w to be **reduced** if no string xx^{-1} or $x^{-1}x$ occurs within w for any $x \in X$. We find any word is equivalent to some reduced word by applying our relations.

Theorem 8.4. Every word is equivalent to a unique reduced word.

Proof. We proceed fancily (he really said this). Let R be the set of reduced words on the alphabet X. For each $m \in X$, define a map

$$m' : R \to R,\ x_1^{\varepsilon_1} \dots x_\ell^{\varepsilon_\ell} \mapsto \begin{cases} m x_1^{\varepsilon_1} \dots x_\ell^{\varepsilon_\ell}, & m \neq x_1^{-\varepsilon_1} \\ x_2^{\varepsilon_2} \dots x_\ell^{\varepsilon_\ell}, & m = x_1^{-\varepsilon_1} \end{cases}$$

We see m' is a bijection as $\left(m^{-1}\right)' = m'^{-1}$. Hence, m' is simply a permutation of the set R.
Now, using the universal mapping property on $F(X)$, we define a homomorphism

$$\begin{aligned} \theta : F(X) &\longrightarrow \mathrm{Sym}(R) \\ [m] &\longmapsto m' \end{aligned}$$

where $\mathrm{Sym}(R)$ is simply the set of all permutations of R. Now, suppose $w = x_1^{\varepsilon_1} \dots x_\ell^{\varepsilon_\ell}$ and $w' = y_1^{\delta_1} \dots y_s^{\delta_s}$ are two reduced words that are equivalent, that is $[w] = [w']$. Then, we have $\theta([w]) = (x_1')^{\varepsilon_1} \dots (x_\ell')^{\varepsilon_\ell}$.Then, we see $\theta([w])(1) = w$. Hence, $\theta([w']) = \theta([w]) = y_1^{\delta_1} \dots y_s^{\delta_s}$. Hence, we see $x_1^{\varepsilon_1} \dots x_\ell^{\varepsilon_\ell} = y_1^{\delta_1} \dots y_s^{\delta_s}$ as words. Hence, there is at most one distinct reduced word in $[w]$. And, as there is always atleast 1 reduced word, we see this completes the proof.

□

Remark. We define $x^n = \underbrace{x \dots x}_{n \text{ times}}$ and $x^{-n} = \underbrace{x^{-1}x^{-1} \dots x^{-1}}_{n \text{ times}}$. Then, we see any reduced word has the form $x_1^{\ell_1} \dots x_s^{\ell_s}$ with $\ell_i \in \mathbb{Z} \setminus \{0\}$ and $x_i \neq x_{i-1}$ for all $1 \leq i \leq s$. This is called the normal form of a word.

Definition 8.4. With the normal form of a word, we define a **multiplicity function**. For $x \in X$ and a word $w = x_1^{\ell_1} \dots x_s^{\ell_s}$ we define $V_x(w) = \sum_{x_j = x} \ell_j$.

We note that if $w \sim w'$, we have $V_x(w) = V_x(w')$ for all $x \in X$. Furthermore, $V_x(w) = V_x\left(v^{-1}wv\right)$ for all $x \in X$ and words v, w. Moreover, $V_x(wv) = V_x(w) + V_x(v)$, so its a homormophism from $F(X) \to \mathbb{Z}$.

Definition 8.5 (Rank)**.** Recall that if $|X| = |Y|$, we had $F(X) \simeq F(Y)$. We define $\mathrm{Rank}(F(X)) = |X|$. We have yet to show this is well defined, but the next theorem will take care of this.

Theorem 8.5. If X and Y are sets with $F(X) \simeq F(Y)$, then $|X| = |Y|$.

We will prove this claim next class.

Lecture 23: Free Groups (6)

Mon 18 Oct 2021 11:26

Recall, we defined the rank of a free group to be the size of its underlying alphabet. In order to ensure this was well defined, we needed to prove the following claim

Proposition 8.1. If $F(X) \simeq F(Y)$ via the isomoprhism φ, then $|X| = |Y|$.

Proof. Denote $G = F(X)$ and $G' = F(Y)$ and let $H = \left\langle g^2 : g \in F(X) \right\rangle$. We know this to be a characteristic subgroup by the homework problem. Hence, we have $H \trianglelefteq F(X)$. Consider G/H and note that $\varphi(H) = H' = \{h^2 : h \in F(Y)\}$.

Since, $\varphi(H) = \{\varphi(g^2) = \varphi(g)^2 : g \in F(X)\} = \{h^2 : h \in \varphi(F(X)) = F(Y)\}$. Hence, $G/H \simeq \varphi(G)/\varphi(H) \simeq G'/H'$ as φ is an isomorphism. We show that $G/H \simeq \underbrace{\mathbb{Z}/2\mathbb{Z} + \ldots + \mathbb{Z}/2\mathbb{Z}}_{|X| \text{ times}} \simeq (\mathbb{Z}/2\mathbb{Z})^{|X|}$.

First, note $xyxy = (xy)^2 = 1$ in G/H for all $x, y \in G/H$ by definition. Hence, $xyx^{-1}y^{-1} = xyxy$ as $x^2 = y^2 = 1$ for every $x, y \in G/H$. Hence, $xyx^{-1} = y$, so G/H is an abelian 2-group. Now, note that $\langle xH : x \in X\rangle = G/H$ and denote $xH = \overline{x}$ for each $x \in G$. Then $G/H = \{\overline{x} : x \in X\}$. Note that an element $g \in G/H$ has

$$\overline{x_1}\overline{x_2}\ldots\overline{x_\ell}$$

with all $\overline{x_1}, \ldots, \overline{x_\ell}$ being distinct.
Suppose $\overline{x_1}\ldots\overline{x_\ell} = \overline{y_1}\ldots\overline{y_s}$. We claim that $\ell = s$ and there is a permutation such that $x_i = y_i$ for all i. Suppose the contrary, so WLOG $x_1 \notin \{y_1, \ldots, y_\ell\}$. Hence, $w = \overline{x_1}\ldots\overline{x_\ell}\overline{y_s}\ldots\overline{y_1} = 1$, so $w \in H$. Furthermore, we find $V_{x_1}(w) = 1$. But, for any generator $g^2 \in H$, we have $V_{x_1}(g^2) = 2n$ for some $n \geq 0$. So, we must have $V_{x_1}(w) = \sum_{i=1}^m V_{x_1}(g_i^2) = 2\hat{n}$ for generators g_i and some $\hat{n} \geq 0$. $\lightning$.
Hence there is a unique representation in G/H.
This shows that

$$\begin{aligned} G/H &= \langle \overline{x} : x \in X\rangle \\ &= \bigoplus_{x \in X} \langle x \rangle \end{aligned}$$

with each $\langle \overline{x}\rangle \in \mathbb{Z}/2\mathbb{Z}$ as $\operatorname{ord}(\overline{x}) = 2$. Hence,

$$G/H = \sum_{i=1}^{|X|} \mathbb{Z}/2\mathbb{Z}.$$

We know this to be a vector space over a 2 element field, $\mathbb{F}_2$, consisting of elements $(\varepsilon_x)_{x\in X} \mapsto \prod_{x\in X} \overline{x}^{\varepsilon_x}$ with almost all (finitely many) $\varepsilon_x = 0$ and $\dim_{\mathbb{F}_2}(G/H) = |X|$ as $\overline{X}$ is a basis for G/H. As $G/H \simeq G'/H'$, we see $\dim_{\mathbb{F}_2}(G'/H') = |X|$. But by the same argument, we see $\dim_{\mathbb{F}_2}(G'/H') = |Y|$ as well. Hence, $|X| = |Y|$. $\square$

Remark. If $F \simeq F(X)$ is free and $H \leq F$, then H is free. Similairly, if $|F : H| = m < \infty$ then $\operatorname{Rank}(H) = \operatorname{Rank}(F) \cdot m + (1 - m)$ for some $m \geq 0$.

Midterm

The test Wednesday will be proofs of ~ 4 (choose 2 out of 4) theorems, propositions, lemmas we proved in class. There will be a second part consisting of short answers consisting of applying theorems, lemmas, … from class to prove simple or concrete results.

Lecture 24: Summary of Group Theory

Mon 18 Oct 2021 18:06

9 Summary of Group Theory

This is a study guide for the midterm and not an actual lecture.

9.1 Basic Group Theory

Theorem 9.1 (Isomorphism Theorems)**.** The isomorphism theorems go roughly as follows:

- Kernel's of surjective homomorphisms are normal subgroups.
- Quotients behave like division: $\frac{G}{H} = \frac{\frac{G}{K}}{\frac{H}{K}}$ (if $K \leq H$).
- Quotients "cancel" into simpler quotients: $\frac{HK}{K} = \frac{H}{H \cap K}$.
- Quotients perserve group structure: Bijecetion between $H \trianglelefteq G$ and $\frac{H}{K} \trianglelefteq \frac{G}{K}$ if $\ker(\varphi) \trianglelefteq H$.

Definition 9.1. We denote the following sets

$$\begin{aligned} G_x &= \{g \in G : x^g = x\} \\ G_X &= \{g \in G : x^g = x \forall x \in X\} \\ N_G(X) &= \{y \in G : yXy^{-1} = X\} \\ Z_G(X) &= \{y \in G : yxy^{-1} = x \forall\ x \in X\} \\ [X, Y] &= \{xyx^{-1}y^{-1} : x \in X, y \in Y\} \end{aligned}$$

$\mathscr{O}_X = \{x^g : x \in X, g \in G\}$.

Definition 9.2 (Group Action)**.** A group G acts on Ω by permuting its elements. Formally $\alpha : G \to \mathrm{Perm}(\Omega)$ such that each g permutes Ω. A special group action is the conjugation map $x \mapsto yxy^{-1}$.

Remark. We need only check $(x^g)^h = x^{hg}$ and $x^1 = 1$.

Definition 9.3. A group action is faithful if it has trivial kernel.

Theorem 9.2. $G_{x^g} = gG_xg^{-1}$.

Proof. Allude to definitions and take a change of variables to the conjugation. □

Theorem 9.3. $x^g = x^h$ if and only if x, y are in a common left G_x-coset.

Proof. Show $g \in hG_x$ by definitions. □

Theorem 9.4 (Orbit-Stabilizer)**.** $|\mathcal{O}_x| = |G : G_x|$.
$|\Omega| = |Z_G(G)| + \sum_{x \in C'} |G : Z_G(x)|$.

Proof. Take the map $f : \{gG_x : g \in G\} \to \Omega,\ x \mapsto f(gG_x) = x^g$ and show its a bijection. For the second equation let the orbit be the whole set and peel of the first term of the summation. □

9.2 P-groups

Definition 9.4. H and K are conjugate if $K = gHg^{-1}$ for some g. Note that the number of subgroups conjugate to H is $|G : N_G(H)|$ by appealing to definitions.

Theorem 9.5. A subgroup of index 2 is normal.

Proof. Let G act on all conjugate subgroups by conjugation. It is trivial that $N_G(H) = H$ or G. G is proof and if it is H we see there are two conjugate subgroups $\Omega = \{H, K\}$ so there is a homomorphism into S_2 and its kernel is H. □

Remark. A subgroup of index of the smallest prime divisor of G is normal by the same argument.

Definition 9.5. A group is a p-group if the order of every element is p^n. A subgroup is a sylow p-group if its order is the highest prime power of p in $|G|$.

Theorem 9.6 (Cauchy's Theorem)**.** If $p \mid |G|$ then there is a $\operatorname{ord}(g) = p$ (hence a subgroup of order p).

Proof. There are two cases, the abelian and nonabelian.

- For the abelian case we proceed as follows:
- Let $H = \langle x \rangle$ and note that if $p \mid H$, then $\operatorname{ord}\left(x^{|H|/p}\right) = p$, so such an element exists.
- If $p \nmid |H|$, then appeal to the quotient group so $p \mid |G/H|$ and define a homomorphism to the quotient where the IH guaranteed an element of order p which we can pullback.
- For the nonabelian case we cite the class equation. If $p \mid |Z(G)|$, then appeal to the abelian case. Else, we find atleast one $p \nmid |G : Z_G(x)|$ by appealing to the class equation mod p. Then, we see $p \mid |Z_G(x)|$. If $Z_G(x)$ is smaller than G we apply IH else we see if a point centralizer is G this implies that element is in $Z(G)$, a contradiction.

□

Theorem 9.7. A p group acting on a finite set has a number of fixed points congruent to $|\Omega|$ mod p.

Proof. Seperate out all orbits of index ≥ 2 and note that $|G : G_x| = p^m$, and the congruency follows. □

Theorem 9.8. A sylow p-group has $H \leq N_G(P) \Rightarrow H \leq P$.

Proof. Appeal to the 3rd isomorphism theorem to see $|HP| / |P| = |H| / |H \cap P|$. Then, we sandwich $|HP|$ between $|P|$ to induce the result. □

Theorem 9.9 (Sylow's Theorem)**.**
- $n_p \geq 1$.
- A p-group is contained in a sylow p-group.
- p-groups are conjugate.
- $n_p \equiv 1 \mod p$
- $n_p = |G : N_G(P)|$ hence $n_p \mid \frac{|G|}{n^p}$

Proof.
- 1 is already shown
- Let Ω be the set of subgroups conjugate to P and G act by conjugation. G acts transitively, hence $|\Omega| = |G : G_P|$ Then, $p \nmid |G : N_G(P)|$. THen, restricting the action to H yields by an earlier lemma the number of fixed points a multiple of p. Hence, there is some fixed point P' which is conjugate to P and $H \leq P'$.
- We find a P' conjugate to P and we see $P' \leq P$ but $|P| = |P'|$, so equality holds and we see the claim holds.
- As all $p$groups are conjuagte applying orbit stabilizer yields $n_p = |\Omega| = |G : G_P| = N_G(P)$ hence $n_p \equiv |\Omega| \mod p$. Letting P' be another P group which is fixed we see $P' = P$ and $P \subseteq N_G(P')$ and $P' = P$ is the only fixed point so $n_p \equiv 1 \mod p$.

□

Theorem 9.10. A group of order p^2 is abelian.

Theorem 9.11. A nontrivial p-group admits a nontrivial $Z(G)$.

Proof. Appeal to the class equation to see $p \mid |Z(G)|$. As the center is nontrivial wee it has order p or p^2. If $|Z(G)| = p$ hence cylic hence $G = Z(G) \cup G/Z(G)$. Then, we see generators $x, Z(G)$ which commute, so G is abelian. □

Theorem 9.12. If $|G| = pq$ $p < q$ and $p \nmid q - 1$, then G is abelian.

Proof. We see $n_p = 1 = n_q$ by sylow's theorem, Hence every $g \in G$ fixes P, Q by conjugation. Then, we see $pq|| |PQ|$, so $|PQ| = G$ THen appealing to the size of the subgroups and normality yields $xy = yx' = x'y' = xy \Rightarrow xy = yx$. □

9.3 Semidirect products

Definition 9.6. $(x, y)(a, b) = (xa^y, b)$

Remark. $(x, y)^{-1} = \left(\left(x^{-1}\right)^{h^{-1}}, h^{-1}\right)$

Theorem 9.13. If $H \trianglelefteq N \rtimes_\alpha H$, then $\alpha = 1$

Proof. Examine $(x, 1)(1, h)\left(x^{-1}, 1\right)$ and we find $\left(x^{-1}\right)^h = x^{-1}$ □

Theorem 9.14. $NH \simeq N \rtimes_\alpha H$ if $\alpha : h \mapsto hxh^{-1}$.

Proof. Appeal to 2nd isomorphism theorem and we see $\frac{NH}{N} \simeq H$. So, we see there are $|H|$ N-cosets in NH. So every Nh is distinct. So, $\alpha : xh \mapsto (x, h)$ is a bijective homomorphism. So they are isomorphic. □

9.4 Simple Groups

Definition 9.7 (Simple Groups)**.** G is simple if it has no nontrivial proper normal subgroups.

Remark. Methods for Determining if a group is simple

- Counting elements of p-groups of power 1.
- Permutation representations.
- Small index subgroups.
- Playing p-groups off each other.

Remark. Counting elements of p-groups of order 1 consists of finding sylow p-groups of order p^1 and then it is clear all elements of the sylow p-groups must be distinct (except identity). Adding these up for all p yields a contradiction.

Remark. For small index subgroups we know a subgroup of index k implies $G \simeq H \leq S_k$. Hence, $|G| \mid |S_k|$. Then, we know if k is the smallest integer such that $|G| \mid k!$, then k is also the minimal index over all proper subgroups. From here we can induce a contradiction by appealing to sylows theorem.

Remark. For Permutation Representations we appeal to one of the following facts. If G has an element of order of k , then so does S_k and if P is a sylow p-group of G, then $|N_G(P)| \mid |N_{S_k}(P)|$. Then, we see the number of p-groups in S_k is $\frac{\prod_{i=k-p+1}^{k} i}{p(p-1)}$. Hence $|N_{S_k}(p)| = p(p-1)$, so $|N_G(P)| \mid p(p-1)$.

Remark. For playing p-groups off of each other. Take a p-group in a p-group, for example $P \leq Q$ and force it to be normal. Then, it is eithere a P-group in G or its contained in one, P^* (which is contained in $N_G(P)$). Hence, we find $\langle N_G(Q), P^* \rangle \leq N_G(P)$, so $|N_G(Q)||P^*| \mid |N_G(P)|$. We can induce a contradiction from here.

9.5 Nilpotent Groups

Definition 9.8. The upper central series is $Z_1(G) = Z(G)$, and $Z_n(G)/Z_{n-1}(G) = Z(G/Z_n(G))$. If this is G eventually, then G is nilpotent.
Equivalently the lower central series is $G^1 = [G, G]$, $G^n = \{G, G^{n-1}\}$. If this is trivial eventually, then G is nilpotent.

Theorem 9.15. Every finite p-group is nilpotent.

Proof. We know the center of a p-grop is nontrivial. From here we show $Z_1 < Z_2$ and induce up to the size of the group. □

Definition 9.9. A subgroup H is characteristic if every automorphism has $\alpha(H) \leq H$.

Remark. $K \trianglelefteq H$ and H characteristic is G yields $K \trianglelefteq G$.

Theorem 9.16. TFAE

- P is the unique sylow p-group in G.
- $P \trianglelefteq G$
- P characteristic in G.
- A subgroup generated by elements of order p^i is a p-group.

Proof.
- $1 \Leftrightarrow 2$ is already shown and $1 \Rightarrow 3$ follows as $\alpha(P)$ is also a sylwo p-group.
- $1 \Rightarrow 4$ If X is such a group $\langle x \rangle \subseteq P$ for all x so $X \subseteq p$ is a p-group.
- $4 \Rightarrow 1$ if they were not unique we have that such a group X would be $P \subseteq \langle P \cup P' \rangle \subseteq X \subseteq P$ so contradiction.

□

Remark. If H, K are groups then $Z(H \times K) = Z(H) \times Z(K)$

Proof. Appeal to definitions. □

Theorem 9.17. For a homomorphism with $\ker(\alpha) = K \leq H$, then $N_G(H) = f^{-1}(N_{G'}(\varphi(H)))$.

Proof. Appeal to homomorphism properties in both directions with $x \in N_G(H)$ xHx^{-1} □

Theorem 9.18. TFAE

- G is nilpotent
- Proper subgroups are proper in their normalizers
- All p-groups are normal
- G is the direct product of its sylow p-groups.

Proof.
- $2 \Rightarrow 3$ G must be abelian with a P not normal. Then as P is

characteristic in $N_G(P)$, we see its normal in $N_G(N_G(P))$ so by definition the normalizers are equal. Hence we have a non normal P-group implies there is a subgroup not in its normalizer contradiction.

□

Theorem 9.19. If G has $n \mid |G|$ with at most n x , $x^n = 1$, then G is cyclic.

Proof. First, we see there are at most $|P| = p^\alpha$ elements with $x^{p^\alpha} = 1$, so P must be distinct. So, all P-groups are normal G is the product of the P-groups. Then, we can show each P_i group is cyclic and the product of their generators is a generator of G as the primes are distinct. □

Theorem 9.20 (Frattini Argument)**.** If $H \trianglelefteq G$ and $P \leq H$ is a sylow group of H , then $G = HN_G(P)$.

Proof. $HN_G(P) \leq G$ by an earlier lemma so letting G act by conjugation yields $P^g \leq H$ so P^g is a sylow p-group which is conjugate to P, so there is a $P^h = P^g$ and we find $h^{-1}g \in N_G(P)$, so $g \in hN_G(P)$. Appealing to third isomorphismtheorem yields $|G : H| \mid |N_G(P)|$. □

Theorem 9.21. G is nilpotent iff every maximal subgroup is normal.

Proof. $\Rightarrow$ If M is maximal then $M = N_G(M)$ or M is normal. If $M = N_G(M)$ this is contradiction as nilpotent groups do not admit proper subgroups equal to their normalizer. $\Leftarrow$ We need only show all sylow groups are normal. Take a maximal subgroup containing $N_G(P)$. Applying frattini argument yields $G = N_G(P)M$, so $G \subseteq MM = M < G$ contradiction. □

9.6 Solvable Groups

Definition 9.10. A group is solvable if it admite a normal chain $H_0 \trianglelefteq H_1 \ldots \trianglelefteq H_n = G$ with the quotient of consecutive H_i being abelian.
An equivalent characterization is the iterated commutator $G^{(1)} = [G, G]$ and $G^{(n)} = \left[G^{(n-1)}, G^{(n-1)}\right]$. If this is trivial at some point then G is solvable.

Proof. $\Rightarrow$ We show each $G^{(i)} \leq H_i$. Induce $G^{(i)} \leq H_{n-i}$ on i and the base case is trivial. For the i case note $G^{(i)} \leq \left[H_{n-(i-1)}, H_{n-(i-1)}\right]$ and we get $G^{(n)} \leq H_{n-n} = \{1\}$.
$\Leftarrow$. Let $H_i = G^{(n-i)}$ and induce on i to show the quotient H_i/H_{i-1} is abelian as it is the quotient of a commutator.. □

Theorem 9.22. A subgroup of a solvable group is solvable.

Proof. Induce to show $H^{(n)} \leq G^{(n)}$. □

Theorem 9.23. Homomorphisms preserve solvability.

Proof. Induce on $G^{(i)}$ to show $\varphi\left(G^{(i)}\right) = \varphi(G)^{(i)}$ $\square$

Theorem 9.24. Let G and $H \trianglelefteq G$ then G solvable iff H and G/H are solvable.

Proof. $\Rightarrow$ Already shown. $\Leftarrow$. Take normal chains of H and G/H and append then to each other. $\square$

9.7 Free Groups

Definition 9.11. X is an alphabet, then $F(X)$ is the free group on X.

Theorem 9.25 (Universal Mapping Property)**.** $F(X)$ is a group F with an injection $\sigma : X \overset{F}{\hookrightarrow}$ so that for any $\alpha : X \to G$ there is a $\beta : F \to G$ such that $\beta(\sigma) = \alpha$.

Theorem 9.26. Use universal mapping property to induce bijective homomorphisms from $F_1 \to F_2$ which is an extension of the assymed bijection $\alpha : X_1 \to X_2$.

Theorem 9.27. For $\alpha : F \to H$ and $\beta : G \to H$, we find a $\gamma : F \to G$ so that $\beta\gamma = \alpha$.

Proof. Let $\beta(g_x) = \alpha(x)$ for some g_x , then we find a homomorphism $x \mapsto g_x$. $\square$

Definition 9.12 (Group Presentations)**.** A group presentation is a set X and a set of relators Y such that $\bigcap_{H \trianglelefteq G, H \geq Y} H = N$ yields a group $F(X)/N$ following the relations.

Remark. $\{\prod_{i=1}^{\ell}\left(g_i x_i g_i^{-1}\right) : g_i \in G, g\times \in X \cup X^{-1}\}$

Theorem 9.28. If $G = \langle X : R\rangle$ and $H = \langle X : R'\rangle$ with all relations in R being relations in R' , then $\alpha(G) = H$ for some α homomorphism.

Proof. $N \leq N'$ so appealing to isomorphism theorems yields $F(X)/N' = G/(N'/N)$. $\square$

Theorem 9.29. Every word is equivalent to a uniqe reduced word.

Proof. For each letter define a map multiplying elements by m on the left. It is a permutation on the set of redued words hence each letter corresponds to a symmetry of R via a homormophism. Then for any two reduced words which are equivalent we find their representation in the symmetry group is the same, hence the words are the same. $\square$

Definition 9.13. $V_X(w)$ = the sum of total powers of a letter in a word.

Definition 9.14. $\text{Rank}\,(F\,(X)) = |X|$.

Theorem 9.30. If $F\,(X) \simeq F\,(Y)$, then $|X| = |Y|$

Proof. Take a subgroup generated by squares and remark that it is characteristic hence normal. Then, we see $G/H \simeq \varphi\,(G)\,/\varphi\,(F\,(X)) \simeq G'/H'$. Then as every elements square is 1 in G/H , so it is an abelian 2-group. Then, we see all products of cosets are unique by multiplying any two and noting the multiplicity of elements versus the multiplicity of their generators.
Hence, we find $G/H = \bigoplus_{x \in X} \langle x \rangle = (\mathbb{Z}/2\mathbb{Z})^{|X|}$. This is a vector space over $\mathbb{F}_2$ with elements corresponding to the power 1 or 0 of some $\overline{x} \in X$. Then, we find the dimensions of G/H and G'/H' are equal and as the dimensions are simply $|X|$, $|X'|$ this completes the proof. □

Theorem 9.31. Subgroups of free groups are free. A subgroup of finite index, m, has $\text{Rank}\,(H) = \text{Rank}\,(F)\,m + 1 - m$.

Lecture 25: Review of Test and Intro to Ring Theory

Fri 22 Oct 2021 11:31

Proof of question 6. Let $C_{105} \rtimes_\alpha C_5$ and define $\alpha : C_5 \to \text{Aut}\,(C_{105})$. Recall, we need only show α is the trivial homomorphism. Recall $\text{Aut}\,(C_{105}) = C_2 \times C_4 \times C_6$. Hence, $|\text{Aut}\,(C_{105})| = 2 \cdot 4 \cdot 6$ and as $5 \nmid 2 \cdot 4 \cdot 6$, we see every element must map to 1. □

10 Intro to Ring Theory

Definition 10.1 (Ring)**.** A **ring** R is a set equipped with two closed operations $+$ and $\times$ obeying the following properties

1. $(R, +)$ forms an abelian group with additive identity, 0 .
2. There is a multiplicative identity, 1 .
3. $0 \neq 1$. (This would guarantee the ring is trivial)
4. The multiplicative operation is associative : $(xy)\,z = x\,(yz)$ for all $x, y, z \in R$.
5. The distributive properties hold: $x\,(y + z) = xy + xz$ and $(x + y)\,z = xz + yz$ for all $x, y, z \in R$.

A ring for which the multiplication operation is also commutative: $xy = yx$, will be called a **commutative ring**.
In general not every element $x \in R$ has a multiplicative inverse. We define the special class of elements with inverses the **units** of R and we denote x^{-1} to denote the unique inverse of a unit x.
A (not necessarily commutative) ring in which every nonzero element is a unit is a **division ring**. A commutative ring for which every nonzero element is a unit is a **field**.

Remark. Technically, a ring need not have a multiplicative identity, but almost all of them will be equipped with one. Sometimes we denote a ring without identity to be a rng (no i).

Example. $\diamond$

Lecture 26: Ring Theory

Mon 25 Oct 2021 11:31

Recall. A ring is a set, an abelian addition and an associative multiplication with identity.

Definition 10.2 (Subring)**.** A **subring**, R' of R is a subset $R' \subseteq R$ such that R' is closed under its operations and $1 \in R'$.

This object turns out to be mostly uninteresting, so we introduce the following concept.

Definition 10.3 (Ideal)**.** A **left ideal** of the ring R is a nonempty subset $I \subseteq R$ so that $I \leq R$ under addition and $rI \subseteq I$ for all $r \in R$. This second condition is equivalent to for all $x \in I$, $r \in R \Rightarrow rx \in I$.
Right ideals follow the same first condition and for the second condition we have $Ir \subseteq I$ for all $r \in R$. A **(two-sided) ideal** is a set I which is both a left and a right ideal.

Example. $I = p\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

$\diamond$

Ideals will play a similar role as that of normal subgroups.

Definition 10.4 (Ring Homomorphisms)**.** If R, R' are rings and $\psi : R \to R'$ is a map. ψ is a **ring homomorphism** if

- $\psi(x+y) = \psi(x) + \psi(y)$ for all $x, y \in R$,
- $\psi(xy) = \psi(x)\psi(y)$ for all $x, y \in R$,
- $\psi(1_R) = 1_{R'}$ (if R, R' are rings with identities).

A ring homomorphism which is a bijection is a **ring isomorphism**.

Example. If $R = \mathbb{Z}/6\mathbb{Z}$. Consider the map $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, $x \mapsto 3x$. We see the first two conditions hold under standard modular arithmetic, but the identity condition clearly fails, so we would consider this a ring homomorphism of rings without identity, but it is not a homomorphism of rings with identity. $\diamond$

Definition 10.5. If R is a ring and $I \subseteq R$ is an ideal.
Then, we define $R/I = \{x + I : x \in R\}$, with $(x+I)+(y+I) \coloneqq (x+y)+I$ and $(x+I)(y+I) \coloneqq xy + I$, to be the **quotient ring** of $R \mod I$.

We see this operation to be well defined as $x' + I = x + I$ and $y' + I = x + I$ implies $x' + a = x$ and $y' + b = y$ for some $a, b \in I$, so we find $xy + I =$

$(x' + a)(y' + b) + I = x'y' + x'b + ay' + ab + I = x'y' + I$ by the absorption property.

Theorem 10.1 (1st Isomorphism Theorem for Rings)**.** If $\psi : R \to R'$ is a surjective ring homomorphism, then $\ker(\psi)$ is a two-sided ideal in R and $R/\ker(\psi) \simeq R'$.

Proof. First, we verify $\ker(\psi)$ is an ideal. It is clearly an additive subgroup as ψ is an additive group homomorphism. Also, if $x \in \ker(\psi)$ and $r \in R$, we see $\psi(x) = 0$, hence

$$\begin{aligned} \psi(rx) &= \psi(r)\psi(x) = 0 \\ \psi(xr) &= \psi(x)\psi(r) = 0 \\ &\Rightarrow rx, xr \in \ker(\psi). \end{aligned}$$

Hence, we find $\ker(\psi) = I$ is an ideal. Now, take the map We wish to show this is well-defined, so we must show that $\psi(x) = \psi(x')$ produces the same coset. As it turns out, this is in fact well defined, so we need only show there is a bijective homomorphism. Clearly the map is surjective and

$$\begin{aligned} xy &\mapsto xy + I \\ x &\mapsto x + I \\ y &\mapsto y + I \\ \text{and } (x + I)(y + I) = xy + I &\mapsto xy + I. \end{aligned}$$

Hence it is a homomorphism. Lastly, as this is an injective map at the group theory level, it is trivial to show injection holds. Hence $R' \simeq R/\ker(\psi)$. □

Remark. It has yet to be formally stated, but $0 \cdot x = 0$ for all $x \in R$ as $ax = ax$, hence $(a - a)x = 0$, so $0 \cdot x = 0$ (and $x \cdot 0 = 0$).

Definition 10.6. If R is a ring with $X \subseteq R$, then (X) is the smallest ideal containing X. In other words,

$$(X) = \bigcap_{\substack{X \subseteq I \subseteq R \\ I \text{ is an ideal}}} I.$$

General elements of (X) (in a commutative ring R) have the form $\sum_{i=1}^{n} r_i \prod_{j=1}^{m_i} x_{j_i}$ for $x_i \in X, r_i \in R$. That is, linear combinations of monomials with terms from X.

Remark. The intersection of (right/left/two-sided) ideals is itself a (right/left/two-sided) ideal.

Lecture 27: Ring Theory (2)

Fri 29 Oct 2021 11:31

Lecture 28: Ring Theory (3)

Fri 29 Oct 2021 11:31

Recall R will be a commutative ring unless otherwise noted.

Definition 10.7 (Prime Ideal)**.** Recall an ideal $P \subseteq R$ is a **prime ideal** when $xy \in P$ implies one of $x \in P$ or $y \in P$. This is equivalent to the statement that R/P is an integral domain.

Definition 10.8 (Maximal Ideals)**.** A proper ideal $M \subseteq R$ is maximal if it is not strictly contained in any other proper ideal. That is, the only ideals containing M are M and R. Equivalently, an ideal I is maximal if and only if R/I is a field.

We prove these two definitions to be equivalent.

Proof. First, assume I maximal. Then, note that an ideal in R/I has the form J/I with $I \subseteq J \subseteq R$ and J being an ideal in R. Hence, as I is maximal, we find $J = I$ or $J = R$. Hence, R/I is a field by prior characterization.
Now assume R/I is a field for some ideal I. Then, the only ideals of R/I are $\{0\}$ and R/I. Suppose I nonmaximal, then we find a $I \subset J \subset R$ corresponding to a proper nontrivial ideal $J/I \subseteq R/I$, $\lightning$ as R/I is a field. □

Proposition 10.1. In a commutative ring R any maximal ideal is prime.

Proof. Since $M \subset R$ and R/M is a field (hence integral domain), we find M to be a prime ideal by the quotient characterization. □

Example. If $R = \mathbb{Z}$, then (0) is a prime ideal, but it is obviously not maximal. ◇

In order to prove some theorems concerning maximal ideals, we need to state some results from basic set theory.

Definition 10.9. If $(X, \preceq)$ is a poset (partially ordered set), with a totally ordered subset $Y \subseteq X$, then an **upper bound** of Y is an element $x \in X$ so that $y \leq x$ for all $y \in Y$. A **maximal element** of X is a $x \in X$ so that for all $y \in X$, $x \leq y$ implies $x = y$.

Law 1 (Zorn's Lemma)**.** If $(X, \preceq)$ is a nonempty poset, with every totally ordered subset having an upper bound, then we find a maximal element $x \in X$.

Of course, this is equivalent to axiom of choice, so we must take it as an axiom. Using Zorn's lemma, we find that every ideal is contained in a maximal ideal (as with subgroups).

Theorem 10.2. If R is a commutative ring with $I \subset R$ being a proper ideal. Then there is a maximal ideal $M \subset R$ with $I \subseteq M$.

Proof. Let $(X, \subseteq)$ be the set of all proper ideals of R which contain I partially ordered by inclusion. As I is proper, we see $I \subseteq I$ hence $I \in X$, so $X \neq \varnothing$. Any maximal element $m \in X$ will be a maximal ideal of R containing I. Hence, we need only show the existence of a maximal element.
Let $(I_\alpha)_{\alpha \in \Omega}$ by a nonempty totally ordered subset of X. Hence, each I_α is a proper ideal containing I with either $I \subseteq I_\alpha \subseteq I_\beta$ or $I \subseteq I_\beta \subseteq I_\alpha$ for all

$\alpha, \beta \in \Omega$. Let $J = \bigcup_{\alpha\in\Omega} I_\alpha$, clearly, $I_\alpha \subseteq J$ for all $\alpha \in \Omega$, so we need only show $J \in X$. Clearly, $I \subseteq I_\alpha \subseteq J$, so J is nonempty and contains I. Now, let $x, y \in J$ with $x \in I_\alpha$, $y \in I_\beta$. By total ordering WLOG, let $I_\alpha \subseteq I_\beta$. Hence, $x, y \in I_\beta$. Hence, $x - y \in I_\beta \subseteq J$ as this is an ideal and $rx \in I_\beta \subseteq J$ for all $r \in R$, hence J is an ideal. Finally, suppose $J = R$, then $1 \in J$, so $1 \in I_\alpha$ for some $\alpha \in \Omega$ $\lightning$, as I_α is assumed proper. Hence, $J \in X$ is an upper bound of $(I_\alpha)_{\alpha\in\Omega}$, so there is a maximal element $M \in X$ which is clearly a maximal ideal. □

Lecture 29: Ring Theory (4)

Mon 01 Nov 2021 11:31

We will again denote all rings R to be commutative.

Recall. An ideal I is principal if $I = (x)$, that is I is generated by one element, so $I = Rx$.

Notation. We say $x \mid y$ if $y = rx$ for some $r \in R$, hence $y \in (x)$.

Proposition 10.2. If $x \mid y$ and $y \mid x$, then $(x) = (y)$.

Proof. $x \mid y$ implies $y \in (x)$, so $(y) \subseteq (x)$.
Similarly, $y \mid x$ implies $x \in (y)$, so $(x) \subseteq (y)$.
Conversely, if $(x) = (y)$, then $x = ry$ and $y = sx$ for some $r, s \in R$, hence $x \mid y$ and $y \mid x$. □

Proposition 10.3. If R is an integral domain with $x \neq 0$, then $x \mid y$ and $y \mid x$ if and only if $y = mx$ for a unit $m \in R$.

Proof. If $(x) = (y)$, then $y = rx$ and $x = sy$ for some $r, s \in R$ hence $x = sy = srx$, so $sr = 1$, hence s and r are units. The other direction is immediately clear, if $x = my$, then $x \in (y)$ so $m^{-1}x = y \in (x)$, hence $(x) = (y)$. □

Remark. If $x = my$ for a unit m, then we say x and y are associated if x and y are equal up to multiplication by a unit.

Definition 10.10 (Principal Ideal Domain)**.** A commutative integral domain R in which every ideal is principal is called a **principal ideal domain** (or PID).

Definition 10.11 (Euclidean Domain)**.** Suppose R is an integral domain and there is a size function (sometimes called a norm) $f : \mathbb{R} \setminus \{0\} \to \mathbb{N}_0$ such that for all $a, b \in R$ with $b \neq 0$, there is $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $f(r) < f(b)$, then R is a **euclidean domain** or ED.

Example. $\mathbb{Z}$ is a PID. $\mathbb{Z}$ is also a euclidean domain under norm $|x|$. ◇

Proposition 10.4. A euclidean domain is a principal ideal domain.

Proof. Let I be a proper nontrivial ideal and let $x \in I$ be a nonzero element with $f(x)$ being minimal (where f is the norm from the definition). We know such an x to exist by the well ordering of $\mathbb{N}_0$. Now, let $y \in I$ and we find by the division algorithm that $y = qx + r$ for some $q, r \in R$ with $f(r) < f(x)$ and $r = 0$. Hence, we find $r = y - qx \in I$ as $x \in I$, $y \in I$. Suppose $f(r) < f(x)$, then $\lightning$ as x is the minimal element of I, hence, we find $r = 0$, so $y = qx$. Hence, we find $y \in (x)$, so $I = (x)$. ☐

Definition 10.12 (Primality/Irreducibility)**.** Let R be a commutative ring

- A non-zero, non-unit $p \in R$ so that for all $x, y \in R$, we have $p \mid xy$ implies $p \mid x$ or $p \mid y$ is called a **prime element**.
- A non-zero, non-unit such that $x = yz$ with $y, z \in R$ implies either y or z is a unit is called an **irreducible** or an **atom**.

Proposition 10.5. $p \in R$ is prime implies (p) is prime.

Proof. Suppose $xy \in (p)$, so $p \mid xy$. Hence, $p \mid x$ or $p \mid y$ as p is prime. Hence, $x \in (p)$ or $y \in (p)$. As p is not a unit, we see $(p) \neq R$, so (p) is prime. ☐

Proposition 10.6. If $p \in R$ is irreducible, then (p) is maximal by inclusion among all proper principal ideals of R.

Proof. Suppose $(p) \subset (x) \subset R$, that is x is not a unit. Then, $p \in (p) \subset (x)$, so $p = rx$ for some $r \in R$, but p is irreducible, so either r or x is a unit, but we know x to be a non-unit, so r must be a unit. So, $(p) = (rx) = (x)$, $\lightning$, as the unit will not change the ideal generated and (p) must be properly contained in (x) . ☐

Corollary 4. If R is a PID, then $p \in R$ being irreducible implies (p) is maximal.

Proposition 10.7. If R is an integral domain with $p \neq 0$ and (p) being maximal among all proper principal ideals, then p is irreducible.

Proof. Suppose $p = xy$, hence $p \in (x)$ and $p \in (y)$. Hence, $(p) \subseteq (y)$ and as (p) is maximal, we have $(y) = (p)$ or $(y) = R$. If $(y) = (p)$, then $p = uy$ for some unit y. But, $p = xy = uy$, hence $x = u$ as we're in an integral domain (with $x, y \neq 0$), so x is a unit. If $(y) = R$, then y is a unit, hence p is irreducible by an earlier lemma. ☐

Lecture 30: Ring Theory (5)

Wed 03 Nov 2021 11:32

Again, we suppose R to be commutative unless otherwise stated.

Proposition 10.8. If R is an integral domain with $p \in R$ being prime, then p is irreducible.

Proof. We know p is nonzero and a non-unit. Then, suppose $p = xy$ $x, y \in R$. Since p prime, we see $p \mid xy$ implies $p \mid x$ or $p \mid y$. WLOG, suppose $p \mid x$, then

$x \in (p)$, so $x = rp$ for an $r \in R$. Then, we see

$$p = xy = (rp)\,y = (ry)\,p.$$

Canceling p yields $1 = ry$, so y is a unit. Hence, p is irreducible. $\square$

Remark. Here are a few basic facts about principal ideals, prime ideals, etc. we have shown, compiled together:

- $x \mid y \Leftrightarrow y \in (x) = Rx$.
- $x \mid y$ and $y \mid x \Leftrightarrow (x) = (y)$.
- If R is an integral domain with $x \neq 0$ then $(x) = (y) \Leftrightarrow ux = y$ for a unit u.
- $(x) = R \Leftrightarrow x$ is a unit.
- $p \in R$ is prime implies (p) is a prime ideal.
- (p) is a prime ideal and $p \neq 0$ implies $p \in R$ is prime.
- $p \in R$ irreducible implies (p) is maximal among all proper principal ideals.
- If R is an integral domain and $p \neq 0$, then $(p) \subset R$ is maximal among principal ideals $\Leftrightarrow p \in R$ is irreducible.
- If R is an integral domain with $p \in R$ being prime then p is also irreducible.

Definition 10.13 (Factorization)**.** If R is a commutative ring, a **factorization** of an element $x \in R$ is an expression

$$x = u\prod_{i=1}^{n} y_i$$

where u is a unit and $y_1, \ldots, y_n$ are irreducibles.
The factorization is a **unique factorization** if for a second factorization

$$x = u'\prod_{i=1}^{n'} y_i'$$

we find $n = n'$ and there exists a permutation π of $\{1, \ldots, n\}$ such that $y_{\pi(i)} = y_i'$ up to units for all $1 \leq y \leq n$.

Definition 10.14 (Unique Factorization Domain)**.** A commutative ring R that is an integral domain in which every nonzero $x \in R$ has a unique factorization is called a **Unique Factorization Domain (UFD)**.

Theorem 10.3. If R is a UFD, then $p \in R$ is prime if and only if p is irreducible.

Proof. Since R is a UFD, it is an integral domain, hence a prime is irreducible. Now, let p be irreducible, so $p \neq 0$ and p is a non-unit. Suppose $p \mid xy$ for some

$x, y \in R$. Then, we see $xy = rp$ for some $r \in R$, hence letting

$$x = u_1 \prod_{i=1}^{n} x_i$$
$$y = u_2 \prod_{i=1}^{m} y_i$$

be the unique factorizations for x and y respectively yields a factorization

$$xy = u_3 \prod_{i=1}^{n} x_i \prod_{i=1}^{m} y_i.$$

Hence,

$$rp = rxy = u_3 \prod_{i=1}^{n} x_i \prod_{i=1}^{m} y_i \cdot r.$$

Hence, we find

$$u_3 \prod_{i=1}^{n} x_i \prod_{i=1}^{m} y_i \cdot r = r \cdot p.$$

Hence, cancelling r, we must have $p = x_j$ or y_k for some $1 \leq j \leq n$ or $1 \leq k \leq m$ as it is irreducible. So, $p \mid x$ or $p \mid y$, hence p is prime. $\square$

It is of note that a factorization can contain multiple copies of a particular irreducible. Hence, we can also represent a factorization as a multi-set. That is, if $x = up_1^{\alpha_1} \dots p_n^{\alpha_n}$, we can represent this as the multi-set

$$\mathrm{Fac}\,(x) = \{\underbrace{p_1, \dots, p_1}_{\alpha_1 \text{times}}, \underbrace{p_2, \dots, p_2}_{\alpha_2 \text{times}}, \dots, \underbrace{p_n, \dots, p_n}_{\alpha_n \text{times}}\}.$$

Then, we can view the factorization of a product xy as the union of their respective factorization multisets, $\mathrm{Fac}\,(x) \cup \mathrm{Fac}\,(y) = \mathrm{Fac}\,(xy)$.

Definition 10.15 (Finitely Generated)**.** An ideal I is finitely generated if $I = (x_1, x_2, \dots, x_n)$ for a finite set $\{x_1, x_2, \dots, x_n\}$.

Definition 10.16 (Noetherian Ring)**.** A commutative ring is **Noetherian** if it satisfies the **ascending chain condition (a.c.c.)** on ideals. That is, if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ is an ascending chain for some ideals $I_1, I_2, \dots$, then there exists a $m \geq 1$ such that $I_i = I_m$ for all $i \geq m$.
More simply, a ring is Noetherian if all properly ascending chains of ideals are finite in lengths.

This definition is rather clunky, so the following characterization is the more standard use case:

Theorem 10.4. *R is a noetherian ring if and only if all ideals in R are finitely generated.*

Remark. A Noetherian ring which is also an integral domain is sometimes called a **Noetherian Domain**.

Noetherian domains are a weaker class of rings than principal ideal domains, but they are more "resiliant" to algebraic operations. That is, most algebraic operations preserve Noetherian-ness even if they do not preserve the PID property.

Lecture 31: Noetherian Rings

Fri 05 Nov 2021 11:34

11 Noetherian Rings

Recall. A commutative ring is noetherian if it satisfies the ascending chain condition on ideals. We claimed this to be equivalent to the property that all ideals are finitely generated.

Proof. First, we assume R to be noetherian. Suppose there is an ideal I which is not finitely generated. Then, let $x_1 \in I$ be a nonzero element of I. Hence, we have $(0) \subset (x_1)$ with $(x_1) \neq I$ by assumption. Moreover, there is an $x_2 \neq x_1$ which is also nonzero such that $(0) \subset (x_1) \subset (x_1, x_2)$ and $(x_1, x_2) \neq I$ by assumption. Recursing, we see there are $x_1, x_2, \ldots \in I$ such that $(x_1, x_2, \ldots, x_n) \subset (x_1, x_2, \ldots, x_n, x_{n+1}) \subset I$ for all n. Hence, letting $I_n = (x_1, \ldots, x_n)$ we obtain an infinite strictly ascending chain of ideals $\lightning$. Hence, $I_n = I$ for some n, so I is finitely generated.
Now, assume all ideals are finitely generated. Suppose there is an infinite proper chain of ideals

$$I_0 \subset I_1 \subset \ldots$$

with each containment being proper. Then, we see $\bigcup_{k \in N_0} I_k = I$ is an ideal. Moreover since I is finitely generated there are $y_1, y_2, \ldots, y_n \in I$ such that $I = (x_1, x_2, \ldots, x_n)$. Then, since $y_1, y_2, \ldots, y_n \in \bigcup_{k \in N_0} I_k$, we see each one is in I_k for some k. Since each $I_k \subset I_{k+1}$, let I_m be an ideal containing all $y_1, y_2, \ldots, y_n$. Then, we see $I \subset I_m$, but this is a contradiction as $I \neq I_m$ by the proper containment assumption and $I \not\subseteq I_m$ as I_m is within the union. $\lightning$. Hence, the chain cannot be strictly ascending. $\square$

Proposition 11.1. Let R be a commutative ring. If R satisfies the ascending chain condition on all principal ideals, then every nonzero element in R has a factorization.

Proof. Let $x \in R$ be a nonzero, nonunit. If x is irreducible, $x = x$ is a factorization. Hence, we can assume $x = x_1 x_2$ with x_1, x_2 being nonzero, nonunits. Similarly, we see x_1, x_2 cannot both be irreducible else this would be a factorization. Hence define $x_1 = x_{11} x_{12}$ and $x_2 = x_{21} x_{22}$ with atleast 3 of $x_{11} x_{12} x_{21} x_{22}$ being non-units. Hence, $x_1 = x_{11} x_{12} x_{21} x_{22}$. Recursing n times yields

$$x = \prod_{i=1}^{2^n} x_i$$

with atleast 2^{n-1} elements being nonunits. If for some n, we find all x_i, $1 \leq i \leq 2^n$ to be irreducible (or units), then x has been factored. Hence, we may assume atleast one x_i to be not an irreducible for all n. Then, we see there must be a sequence k_i such that $(x) \subset (x_1) \subset (x_{k_1}) \subset (x_{k_2}) \subset \dots$ as each x_{k_i} splits into a product of elements which are not both irreducble or units. Moreover, each containment must be proper, so letting n grow yields $\lightning$, as such a chain will continue indefinitely unless all x_i are irreducble or units at some step. Hence we must have at some point all x_i to be irreducibles, hence x is factorable. □

Theorem 11.1. If R is a noetherian domain then R is a unique factorization domain if and only if all irreducible elements are prime.

Proof. Note, we have already shown all primes to be irreducible in an integral domain (hence noetherian domain) and we know UFD implies primes are irreducibles. Hence, only one implication remains to be shown, that all irreducible being prime implies UFD.
Since R is a noetherian domain, factorizations exist. Hence, we need only show these factorizations are unique. Suppose

$$\begin{aligned} x &= ux_1x_2\dots x_n \\ &= u'y_1y_2\dots y \end{aligned}$$

with u, u' being units and x_i, y_i being irreducibles for each i. We proceed by induction on $|\text{Fac}(x)|$. If $|\text{Fac}(x)| = 1$, then x is irreducible and the claim is obviously true. Of course the case $|\text{Fac}(x)| = 0$ implies x a unit, hence not factorable, so the claim is vacuously true in this case.
Now, assuming the case $n-1$, if $|\text{Fac}(x)| = n$ (as is the case in the original x), we see $x_1 \mid x$ with x_1 being irreducible, hence prime. Supposing the claim false, we see $x_1 \mid u'y_1y_2\dots y_t$, so WLOG, $x_1 \mid y_1$ up to units. As y_1 is irreducible and divided by x_1 , we see $y_1 = x_1r_1$ with r_1 being a unit, hence $x_1 = y_1$ up to units. Repeating yields for each $1 \leq i \leq n$, $x_i = y_j$ for some $1 \leq j \leq t$ (up to permutation of the y_i's) up to units, hence

$$\begin{aligned} x &= ux_1x_2\dots x_n \\ &= \hat{u}x_1x_2\dots x_ny_s\dots y_t \text{ for a unit } \hat{u} \text{ and some } s \leq t \ . \end{aligned}$$

This yields, $y_1y_2\dots y_t = 1$ up to units, $\lightning$ as the y_i's were assumed nonunits. □

«««< HEAD

Lecture 32

Sun 14 Nov 2021 15:09

=======

Lecture 32

Wed 10 Nov 2021 17:32

»»»> fbddf3e930553556ea514c68e105d294dc597cc6

12 Ring Localization

Lecture 33: Localization of Rings

Wed 10 Nov 2021 17:33

Recall. Recall R denotes a commutative ing. If $S \subseteq R$ is a multiplicative subset, we see $x, y \in S$ implies $xy \in S$ and $0 \notin S$ but $1 \in S$.
Then, we define $S^{-1}R = \{X/s : x \in R, s \in S\}$. Then, we see $\frac{x_1}{s_1} = \frac{x_2}{s_2}$ if and only if there is an $s \in S$ so that $s\left(s_2 x_1 - s_1 x_2\right) = 0$. Of course, if R is an integral domain we see this iplies $s_2 x_1 - s_1 x_2 = 0$, the normal definition of fraction equality.

Now, we turn this set into a ring. We define $\frac{x_1}{s_1} \cdot \frac{x_2}{s_2} := \frac{x_1 x_2}{s_1 s_2}$ and $\frac{x_1}{s_2} + \frac{x_2}{s_2} = \frac{s_2 x_1}{s_1 s_2} + \frac{s_1 x_2}{s_1 s_2} = \frac{s_2 x_1 + s_1 x_2}{s_1 s_2}$. Now, we need to show that $+, \cdot$ are well defined (meaining they do not vary for different representatives of a given equivalence class). This fact is easily checked by symbolic manipulation so we omit the proof. For the addition case suppose $\frac{x_1}{s_1} = \frac{x_1'}{s_1'}$ and similairly for $\frac{x_2}{s_2}$ then take the multiplicative representation of the fraction and multiply the $\frac{x_1}{s_1}$ representation by $-s_2 s_2' ts$ and the $\frac{x_2}{s_2}$ representation by $-s_1 s_1' st$ and by adding together these representations we see terms cancel and we obtain that addition is in fact well defined. Moreover, it is trivial to check that the ring axioms hold.

Definition 12.1 (Ring Localization)**.** We denote this new fraction ring $S^{-1}R$ to be the **localization of** R with additive identity $\frac{0}{1}$, multiplicative identity $\frac{1}{1}$ and $\frac{tx}{ts} = \frac{x}{s}$ for all $t \in S$.

Note that $s \in S$ is nonzero by definition, so $\frac{1}{s} \cdot \frac{s}{1} = \frac{1}{1} = 1_{S^{-1}R}$, so every element has an inverse.

Proposition 12.1. If R is a commutative ring with $S \subseteq R$ being a mult-plicative subset. Then the map

$$\begin{aligned} \pi : R &\longrightarrow S^{-1}R \\ x &\longmapsto \pi(x) = \frac{x}{1} \end{aligned}$$

is a ring homomorphism. Moreover, if S has no zero-divisors, then π is an injection.

Proof. If $x, y \in R$ then $\pi\left(x \pm y\right) = \frac{x \pm y}{1} = \frac{x}{1} \pm \frac{y}{1} = \pi\left(x\right) \pm \pi\left(y\right)$. Furthermore $\pi\left(1\right) = \frac{1}{1} = 1$.
Lastly, $\pi\left(xy\right) = \frac{xy}{1} = \frac{x}{1}\frac{y}{1} = \pi\left(x\right)\pi\left(y\right)$. Hence, π is a ring homomorphism. Now consider $\ker\left(\pi\right) = \left\{x \in R : \frac{x}{1} = \frac{0}{1}\right\}$. We see this implies an $s \in S$ so that $s\left(1x - 1 \cdot 0\right) = sx = 0$, hence s is a zero divisor if $x \neq 0$ $\lightning$. So, the kernel is trivial. $\square$

Example. If R is a commutative ring and $P \subseteq R$ is a prime ideal, then $S \coloneqq R \setminus P$ is a multiplicative set. Moreover, $0 \in P$ so $0 \notin S$ and $P \subset R$ is proper, so $1 \in S$.
If $x, y \in S$ with $xy \notin S$, then $xy \in P$ so $x \in P$ or $y \in P$ $\lightning$. So, S is closed under multiplication. Then the localization $S^{-1}R$ is often denoted R_P. This is

the canonical example of localization which we will study more next class. $\diamond$

The use of this construction is that it allows us to embed an integral domain R in a field $R_{(0)}$ called the **field of fractions**.

13 Chinese Remainder Theorem

Lecture 34: Chinese Remainder Theorem

Fri 12 Nov 2021 17:29

Theorem 13.1 (Classical Chinese Remainder Theorem)**.** If $m_1, \ldots, m_r$ are relatively prime integers, then for $a_1, \ldots, a_r$ we find an $x \in \mathbb{Z}$ so that $x \equiv a_i \mod m_i$ for each $1 \leq i \leq r$.

Theorem 13.2 (Generalized Chinese Remainder Theorem)**.** Let R be a commutative ring with $I_1, \ldots, I_n \subseteq R$ being ideals so that $I_i + I_j = R$ for all $i \neq j$. That is, the I_is are pairwise co-maximal. Then for any $x_1, \ldots, x_n \in R$ we find an $x \in R$ so that $x \equiv x_i \mod I_i$ for all $1 \leq i \leq n$.

Recall. $x \equiv x_i \mod I_i$ if $x - x_i \in I_i$.

Proof. If $n = 1$ this is trivial. Of course, $x = x$.
For the case $n = 2$ we have $I_1 + I_2 = R$, hence $1 \in R = I_1 + I_2$. Hence, $1 = a_1 + a_2$ with $a_1 \in I_1, a_2 \in I_2$. Then, let $x = x_1a_1 + x_2a_2$, and we see $a_1 + a_2 = 1$ but $a_1 \equiv 0 \mod I_1$ and likewise $a_2 \equiv 0 \mod I_2$, hence $a_1 \equiv 1 \mod I_2$ and $a_2 \equiv 1 \mod I_1$. Hence,

$$\begin{aligned} x &= x_1a_2 + x_2a_1 \\ &\equiv x_1a_2 \mod I_1 \\ &\equiv x_1 \mod I_1 \\ \text{and } x &\equiv x_2a_1 \\ &\equiv x_2 \mod I_2. \end{aligned}$$

Hence, the claim holds for $n = 2$. Now, we induce on n.
Let $n \geq 3$ and suppose the case $n - 1$ to be true. Then, we find Then, we see $I_1 + I_i = R$ for all $i \geq 2$ by hypothesis. Hence, $1 = a_i + b_i$ with $a_i \in I_1$, $b_i \in I_i$. Then, we find

$$1 = \underbrace{1 \cdot \ldots \cdot 1}_{n \text{ times}} = \prod_{i=1}^{n}(a_i + b_i) \in \prod_{i=1}^{n}(I_1 + I_i) \subseteq I_1 + \prod_{i=2}^{n} I_i.$$

Moreover, we know $I_1 + \prod_{i=2}^{n} I_i$ to be an ideal as the product and sum of ideals are still ideals.
Then applying the case $n = 2$, we find a $y \in R$ so that $y_1 \equiv 1 \mod I_1$ and $y_1 \equiv 0 \mod \prod_{i=2}^{n} I_i$. Repeating for each $1 \leq i \leq n$ yields a $y_j \in R$ so that $y_j \equiv 1 \mod I_j$ and $y_j \equiv 0 \mod \prod_{1 \leq i \leq n; i \neq j} I_i$. Now, define $x = \prod_{i=1}^{n} x_iy_i$. We see $y_j \in I_i$ for all $i \neq j$, hence $y_jx_j \equiv 0 \mod I_i$ for all $i \neq j$. Hence $x \equiv x_iy_i \equiv x_i \mod I_i$. $\square$

Note that in the preceding proof $\prod I_i$ denotes the ideal product as defined in the homework. In the next theorem we will use this symbol for the cartesian product, so ideal products will be written without product notation when the context is not necessarily clear.

Corollary 5 (Alternative Statement of the Chinese Remainder Theorem)**.** Let R be a commutative ring with $I_1, \ldots, I_n \subseteq R$ being pairwise comaximal distinct ideals of R. Then the map

$$\begin{aligned} f : R &\longrightarrow \prod_{i=1}^{n} R/I_i \\ x &\longmapsto (x \mod I_i)_{1 \leq i \leq n} \end{aligned}$$

is a surjective ring homomorphism with kernel $\ker(f) = \bigcap_1^n I_i$. Specifically,

$$R/\left(\bigcap_{i=1}^{n} I_i\right) \simeq \prod_{i=1}^{n} (R/I_i)\,.$$

Proof. It is easily confirmed that f is a ring homomorphism with the prescribed kernel. Hence, the only claim that remains to be shown is the surjectivity. For f to be surjective, we need to take an arbitrary congruence system $\hat{x} = (x_1 \mod I_1, x_2 \mod I_2, \ldots, x_n \mod I_n)$ in the codomain of f and find a solution $x \in R$ so that $x \equiv x_i \mod I_i$ for all $1 \leq i \leq n$ (that is $f(x) = \hat{x}$). We see the generalized remainder theorem yields such an x, so f is surjective. $\square$

14 Polynomial Rings

Lecture 35: Polynomials

Mon 15 Nov 2021 11:32

Definition 14.1 (Polynomial Ring)**.** Let R be a commutative ring and we define $R[X]$ to be the ring of polynomials in the variable x with coefficients from R defined as follows.
An element $f \in R[X]$ has the form

$$f = a_0 + a_1 x + \ldots + a_n x^n$$

for some $n \geq 0$ and each $a_i \in R$. This is a formal sum in the sense that two polynomials

$$\begin{aligned} f &= a_0 + a_1 x + \ldots + a_n x^n \\ g &= b_0 + b_1 x + \ldots b_m x^m \end{aligned}$$

have $f = g$ if and only if $a_i = b_i$ for every i.
For the polynomial f, we call a_0 the **constant term** and a_n to be the **leading coefficient** and n to be the **degree**, denoted $\deg(f) = n$.
For the polynomial $f = 0$, we specifically define $\deg(f) = -1$. For all other constant polynomials g, we define $\deg(g) = 0$.

Remark. Occasionally, we will write $f = \sum_{i=0}^{\infty} a_i x^i$ with almost every $a_i = 0$. With this form we see elements of $R[X]$ are in a bijective correspondence with finite support tuples from $R^{\mathbb{N}}$.

We see $R[X]$ forms a ring with two polynomials $f, g \in R[X]$ as defined earlier having sum

$$(f+g) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

and

$$fg = \sum_{i=0}^{\infty} a_i x^i \sum_{j=0}^{\infty} b_j x^j = \sum_{n=0}^{\infty} \sum_{\substack{i,j \\ i+j=n}} a_i b_j x^n.$$

Definition 14.2 (Multivariate Polynomial Rings)**.** We define a **multivariate polynomial ring** $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$ with addition and multiplication defined similarly. It is worth noting that while degree and constants are well defined, the leading coefficient may be poorly defined without adding extra constraints.

Definition 14.3 (Projected Degree)**.** For a multivariate polynomial $f \in R[x_1, \ldots, x_n]$ we define $\deg(f)_{x_i}$ to be the degree when considered only in the variable x_i.

Remark. It is of note that polynomials are more formal objects and not necessarily functions. The distinction is mostly moot, but we can induce a function from a polynomial by defining a function

$$\begin{aligned} f : R &\longrightarrow R \\ b &\longmapsto f(b) = \sum_{i=0}^{\infty} a_i b^i. \end{aligned}$$

The point of this distinction is that polynomials over finite (or otherwise non-standard spaces) may not be distinct. For example $x \mapsto x^5 - x$ and $x \mapsto 0$ are completely equivalent in $\mathbb{F}_5$. This, of course, cannot happen over $\mathbb{R}$ unless the coefficients are precisely equal.

We can construct a function in a different way as follows:

Definition 14.4 (Evaluation Map)**.** Fixing $b \in R$ we define the **evaluation map** on $R[x]$ as

$$\begin{aligned} \mathrm{ev}_b : R[x] &\longrightarrow R \\ f &\longmapsto \mathrm{ev}_b(f) = f(b). \end{aligned}$$

We find this map to be a ring homomorphism, essentially compressing $R[x]$ down into R.

Lemma 14.1 (Gauss Lemma)**.** Let R be a UFD with K its quotient field. If $f, g \in K[x]$, then $\mathrm{Cont}(fg) = \mathrm{Cont}(f)\,\mathrm{Cont}(g)$.

Proof. Let $c_1 = \mathrm{Cont}(f)$, $c_2 = \mathrm{Cont}(g)$. Then, $f = c_1 f_1$ and $g = c_2 g_1$ for some $f_1, g_1 \in R[x]$ with $\mathrm{Cont}(f_1) = \mathrm{Cont}(g_1) = 1$. So, $fg = \mathrm{Cont}(f)\,\mathrm{Cont}(g)\, f_1 g_1$. Thus, it suffices to show $\mathrm{Cont}(f_1 g_1) = 1$. Since $f_1, g_1 \in R[x]$, we see $f_1 g_1 \in R[x]$. Hence, we need to show no p divides all the coefficients of $f_1 g_1$. Suppose by contradiction that p is a prime dividing all coefficients of $f_1 g_1$. Then, the map

$$\varphi : R[x] \longrightarrow R/(p)[x] = \overline{\mathbb{R}}[x]$$
$$.$$

Clearly (p) is a prime ideal, so $\overline{\mathbb{R}}$ is an integral domain with $0 = \varphi(f_1 g_1) = \varphi(f_1)\,\varphi(g_1)$. Hence either $\varphi(f_1) = 0$ or $\varphi(g_1) = 0$, so WLOG $p \mid a_i$ for all a_i in the representation of f_1, hence $\mathrm{Cont}(f_1) \geq p$ $\lightning$. So the claim holds. □

Lecture 36: Polynomials (2)

Mon 07 May 2018 03:55

Recall. For a commutative ring R, we define the polynomial ring $R[x_1, \ldots, x_n]$ as formal sums of powers of x_i with coefficients in R.

Moreover, if we have two commutative rings R, R' with a ring homomoprhism $\varphi : R \to \overline{\mathbb{R}}$, then there is a complementary ring homomorphism extending to the polynomial ring:

$$\overline{\varphi} : R[x] \longrightarrow \overline{\mathbb{R}}[x]$$
$$\sum_{i=0}^{\infty} \alpha_i x^i \longmapsto \sum_{i=0}^{\infty} \varphi(a_i) x^i.$$

Definition 14.5 (Map Space)**.** Now, define $\operatorname{Map}(Y \to R)$ to be the set of all maps $f : Y \to R$ with R being a commutative ring and Y being an arbitrary set. We equip $\operatorname{Map}(Y \to R)$ with pointwise operations $\times, +$ such that

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x) g(x)$$
$$.$$

These operations induce a ring over $\operatorname{Map}(Y \to R)$.

Then, we see a polynomial $f \in R[x]$ defines a corresponding map $\overline{f} \in \operatorname{Map}(R \to R)$ with $\overline{f}(a) = \operatorname{ev}_a(f)$ for all $a \in R$.

Remark. The map $f \mapsto \overline{f}$ need not be injective. See the example $f = x^5 - x$ and $g = 0$ in $\mathbb{F}_5$.

Proposition 14.1. If R is an integral domain, then $R[x]$ is also an integral domain. Moreover, for nonzero polynomials $f, g \in R[x]$ we have $\deg(fg) = \deg(f) + \deg(g)$.

This prove is completely trivial hence it is omitted.

Theorem 14.1. If F is a field, then $F[x]$ is a euclidean domain, a principal ideal domain, and a unique factorization domain.

Proof. Applying standard (euclidean) polynomial division with euclidean norm $\deg(f)$ for $f \in F[x]$ yields a euclidean domain (hence a PID and UFD). □

Theorem 14.2. If R is a commutative ring then $R[x]$ is a principal ideal domain if and only if R is a field.

Proof. One direction has already been shown.
Moreover if $R[x]$ is a PID, then R is an integral domain. Hence, if $ab = a$ with $a, b \in R$, then $a = 0$ or $b = 0$, so R is an integral domain as its a subring of $R[x]$.
Now, let $y \in R$be an arbitrary nonzero element. We wish to show y a unit. Let $I = (y, x) \subseteq R[x]$. Then, since $R[x]$ is a Principal ideal domain, we have an $f \in I$ so that $(y, x) = (f)$. Note that we must have $f \neq 0$ as $x \neq 0$ and as $y \in (f)$ we see $y = hf$ for an $h \in R[x]$ which is nonzero. Since R is an integral domain, we see $\deg(f) = \deg(h) = 0$. Hence, f is a nonzero constant $\alpha \in R$. Hence, we have $x \in I = (\alpha)$ so $x = g\alpha$ for some $g \in [x]$. But, R is an integral

domain, so $1 = \deg(x) = \deg(\alpha) + \deg(g) = \deg(g)$. So, we have $g = ax + b$ for some nonzero $a \in R \setminus \{0\}$ and $b \in R$. Thus, $x = (ax + b)\alpha = (a\alpha x + b\alpha)$, hence $a\alpha = 1$ and $b\alpha = 0$ by the coefficient property of polynomial rings. Thus,

$$(\alpha) = (f) = I = (y, x) = R[x].$$

Hence, $1 \in (y, x) = R[x](y) + R[x](x)$. So, $1 = g_1 y + g_2 x$ for some $g_1, g_2 \in R[x]$. Hence letting $g_1 = g_{11} + g_{12}x$ and similairly $g_2 = g_{21} + g_{22}x$ for some $g_{11}, g_{12}, g_{21}, g_{22} \in R$, we see $1 = yg_{11}$. So, y is a unit, hence R is a field. ☐

Corollary 6. If F is a field $F[x, y]$ is not a principal ideal domain.

Proof. $F[x, y] = (F[x])[y]$ and $F[x]$ is not a field (take $f = x$, there is no inverse), so $F[x, y]$ is not a principal ideal domain by applying the previous characterization. ☐

Theorem 14.3. If F is a field with f being a polynomial having $\deg(f) = n \geq 0$ in $F[x]$. If, $f(a) = 0$ for $a \in R$, then $(x - a) \mid f$. Moreover, f has at most n roots in F.

Proof. Since $f \neq 0$ and f has a zero, we see $\deg(f) \geq 1$. Hence, using polynomial long division yields $f = q(x - a) + r$ for some $q, r \in F[x]$ with $\deg(r) < \deg((x - a))$, hence $\deg(r) \leq 0$, that is r is a constant polynomial.
We see $f(a) = r = 0$, hence $f = q(x - a)$, so $(-a) \mid f$. Letting $a_1, \ldots, a_n$ be distinct real zeros of f, then $(x - a_1) \mid f$ implying $f = f_1(x - a_1)$ with $\deg(f_1) = \deg(f) - 1$. Inducing on the roots a_i, we see that more than n roots would imply $f = f_1 \cdot f_2 \cdot \ldots \cdot f_n \cdot f_{n+1} \cdot g$ where g is the final polynomial obtained by dividing by $x - a_{n+1}$ and is of degree $\deg(g) = \deg(f) - (n + 1) = -1$ implying g is the zero polynomial. But, we have $f = g \prod_{i=1}^{n+1} (x - a_i)$, so $f = 0$ $\lightning$. Hence there are at most n zeroes. ☐

Lecture 37: Polynomials (3)

Fri 19 Nov 2021 11:30

Theorem 14.4. Let K be a field, with U being a finite multiplicative subgroup. Then it is cyclic.

Proof. Since U is a finite additive group, we see $U = \prod_{i=1}^{n} P_i$ for some sylow p groups P_i. It suffices to show that each subgroup is cyclic as the product of their generators will generate U. Let $x \in P_i$ be an element of maximal order p^m and let $|P_i| = p^n$ for $m \leq n$. Then every $y \in P_i$ has order $\operatorname{ord}(y) \mid p^m$. Hence, they are all roots of $f = x^{p^m} - 1$ which has at most p^m roots, so $p^n = |P_i| \leq p^m$, hence $n \leq m$ so equality holds. So, x has order p^n implying x generates P_i. ☐

Corollary 7. $(\mathbb{Z}/p\mathbb{Z})^{\times} \simeq \mathbb{Z}/(p - 1)\mathbb{Z}$.

Definition 14.6 (Content of a Polynomial)**.** Let R be a UFD with its quotient field K. Let $x \in K$, then there is a unique (up to units) representation $x = \frac{a}{b}$ with $a, b \in R$ being coprime (no prime p has $p \mid a$ and $p \mid b$). Then, for a prime p, define $V_p\left(\frac{a}{b}\right) = V_p(a) - V_p(b)$ where $V_p(x)$ is the power of p in the unique factorization of x. We see one of $V_p(a)$ or $V_p(b) = 0$. Leaving results $V_p(a)$ if $p \mid a$ or $-V_p(b)$ if $p \mid b$. This is called the **p-adic** valuation of $\frac{a}{b}$. Note $V_p(0) \coloneqq \infty$.
Now, let $f \in K[x]$ with

$$f = \sum_{i=0}^{n} a_i x^i$$

for some $n \in \mathbb{N}$ and $a_i \in K$. Then, we define $V_p(f) = \inf\{V_p(a_i) : i \geq 0\}$.
With this, we define the **content** of f to be

$$\mathrm{Cont}(f) = \prod_{p \text{ prime}} p^{V_p(f)}.$$

Remark. The notion of content essentially generalizes the GCD to fraction fields.

Example. Let $R = \mathbb{Z}$ so $K = \mathbb{Q}$, then $V_2\left(\frac{2}{9}\right) = 1$ and $V_3\left(\frac{2}{9}\right) = -2$ and $V_5\left(\frac{2}{9}\right) = 0$.
Then, let $f(x) = \frac{3}{4}x^2 + 6x - 3$, then

$$\mathrm{Cont}(f) = 3 \cdot 2^{-2} = \frac{3}{4}.$$

Since $\mathrm{Cont}(f)$ will always contain all denominators, this allows us to reduce a polynomial over $\mathbb{Q}$ to a rational times a polynomial, $f_1 \in K[x]$ having content $\mathrm{Cont}(f_1) = 1$, hence $f_1 \in R[x]$. $\diamond$

Lemma 14.2. If R is a UFD, with K its quotient field, and $f \in K[x]$, then $\mathrm{Cont}(f) = 1$ implies $f \in R[x]$.

Remark. It is of note that the converse does not hold, take $2x^2 + 4$.

Definition 14.7. For a UFD R and quotient field K, we say $f \in K[x]$ is **primitive** if $\mathrm{Cont}(f) = 1$ (hence $f \in R[x]$).