Lecture Notes by Jonathan Alcaraz (UCR)

Algebra

Math 201A
Fall 2016

Based on Lectures by

Dr. David Rush
University of California, Riverside

last updated August 25, 2017

Lecture 1 23 Sep 2016

Definition 1.1 A *monoid* is a set together with a binary operation that is associative and has an identity (usually denoted e).

Example The collection of maps from a set to itself is a monoid with respect to composition.

Definition 1.2 An element x of a monoid G is said to be *invertible* if there exists some $y \in G$ such that $xy = yx = e$. It follows that such an element is unique. We call such an element the *inverse* of x and usually denote it by x^{-1}.

Definition 1.3 A monoid in which every element is invertible is called a *group*.

Example The collection of bijections from a set to itself is a group with respect to compostition.

Definition 1.4 A map $f : G_1 \to G_2$ of monoids is a *homomorphism* is $f(g_1g_2) = f(g_1)f(g_2)$ and $f(e_1) = e_2$. If G_1, G_2 are groups, it suffices to say that $f(xy) = f(x)f(y)$.

Definition 1.5 A bijective homomorphism is called an *isomorphism*. An isomorphism from a group to itself is called an *automorphsim*.

Theorem 1.6 For any group G, there is a set S and an injective homomorphism from G to the group of permutations of S.

Let $P(G)$ be the group of permuations of G and define $f : G \to P(G)$ by $f(g) = L_g$ where $L_g(x) = gx$. Note that L_g has an inverse, $L_{g^{-1}}$, and hence is a permutation. Moreover, note that

$$L_{g_1g_2}(x) = g_1g_2x = g_1L_{g_2}(x) = L_{g_1}(L_{g_2}(x))$$

so f is in fact a homomorphism. To show f is injective, we intend to show it has trivial kernel. Let $f(g) = id_G$. That is $L_g(x) = gx = x$ for any $x \in G$. In particular, if $x = e$, we see $g = e$. ■

Definition 1.7 Given a subgroup H of G, a *left coset* of H is a subset of G of the form

$$aH = \{ah : h \in H\}$$

for some $a \in G$. One can similarly define a *right coset*.

Note Any 2 left cosets of H have the same cardinality.

Exercise 1 The set of left cosets of H in G partition G.

> Note the cosets cover G since $e \in H$, so for any $a \in G$, $a \in aH$. Note that if $b \in aH$, then $bH = aH$. So, by the contrapositive of this statement, the cosets are pairwise disjoint.

Definition 1.8 The number of cosets of H in G is called the *index* of G over H and is denoted by $[G : H]$.

Theorem 1.9 If H is a subgroup of G, then

$$[G : 1] = [H : 1][G : H]$$

where 1 denotes the trivial subgroup of G.

Theorem 1.10 If H is a subgroup of G, the following properties are equivalent:

(i) $xHx^{-1} = H$ for any $x \in G$;

(ii) $xH = Hx$ for any $x \in G$;

(iii) The elementwise product of two right cosets is a right coset.

(iv) H is the kernel of some group homomorphism $f : G \to G'$ for some G'.

Definition 1.11 A subgroup with any of the above properties is said to be *normal*.

Lecture 2 26 Sep 2016

Let us now prove the above theorem.

(i) $\Rightarrow$ (ii) This implication follows directly from the definition of these sets. (ii) $\Rightarrow$ (iii) We have

$$(Hx)(Hy) = H(xH)y = H(Hx)y = (HH)xy = Hxy$$

(iii) $\Rightarrow$ (iv) By (iii), $HxHy = Hz$ for some $z \in G$. So the cosets Hxy and Hz have an element $xy = hz$ in common. So $Hxy = Hz$.
(iv) $\Rightarrow$ (i) Let f be the homomorphism given by (iv). Notice that for $h \in H$, $f(xhx^{-1}) = e$, so $xHx^{-1} \subseteq \ker(f) = H$. Similarly, $H \subseteq xHx^{-1}$.

Definition 2.1 Let H be a subgroup of G. The *normalizer* of H is

$$N_H = \{x \in G : xHx^{-1} = H\}$$

The *centralizer* of a subset S of G is

$$\{x \in G : xhx^{-1} = h \, \forall h \in H\}$$

The centralizer of G itself is said to be the *center* of G, usually denoted by $Z(G)$.

Theorem 2.2 Let H, K be subgroups of G with $H \subseteq N_K$. Then

(a) $HK = KH$;

(b) HK is a subgroup of G;

(c) K is normal in HK, $H \cap K$ is normal in H, and $H/H \cap K \cong HK/K$.

(a) Since $H \subseteq N_K$, $hKh^{-1} = K$ for $h \in H$. Thus $hK = Kh$ for any $h \in H$. So for $hk \in HK$, $hk = hK = Kh \subseteq KH$. Thus $HK \subseteq KH$. Similarly, $kh \in Kh = hK \subseteq HK$.

(b) Clearly HK contains the identity since H and K do. Moreover, for some $hk \in HK$, $k^{-1}h^{-1} \in KH = HK$ and $k^{-1}h^{-1}hk = hkk^{-1}h^{-1} = e$. It remains to show that HK is closed under its operation. Note that a product of elements of HK would, a priori, be in $HKHK$. By (a),

$$HKHK = HHKK = HK$$

(c) Note that N_K is a group containing H and K *(the fact that N_K is a group can be proven with a simple check of the group axioms)*. Hence $HK \subseteq N_K$ and thus K is normal in HK.

Let $\varphi : H \to HK/K$ be the composition of the inclusion $H \to HK$ and the projection $HK \to HK/K$. Then φ is a surjective homomorphism. Indeed, each element of HK/K is of the form $hkK = hK$. Moreover, the kernel of φ is $H \cap K$. So $H \cap K$ is normal in H and $H/H \cap K \cong HK/K$.

Lemma 2.3 If $K \subseteq H$ are subgroups of the finite group G, then

$$[G : K] = [G : H][H : K]$$

Let $\{h_i\}$ be a set of representatives of left cosets of K in H and $\{g_j\}$ be a set of representatives of the left cosets of H in G. We claim that $\{g_i h_j\}$ is a set of representatives of K in G. These cover G since

$$G = \cup g_i H = \cup g_i h_j K$$

Suppose $g_i h_j K = g_r h_s K$. Then in particular, $g_i h_j H = g_r h_s H$ and thus $g_i = g_r$, so $i = r$. Therefore, $g_i h_j K = g_i h_s K$ and thus $h_j K = h_s K$, so $j = s$. Hence, these cosets are disjoint.

Lecture 3 28 Sep 2016

Definition 3.1 Let A be a finite set. Denote the *set of permutations* of A by S_A or $P(A)$. Given $\sigma \in S_A$ we can define an equivalence relation $\sim_\sigma$ such that $a \sim_\sigma b$ if $\sigma^n(a) = b$. The equivalence classes, say $B_1, \ldots, B_k$, of this relation are called the *orbits* of σ. For $1 \leq i \leq k$, define $\sigma_i : A \to A$ by

$$\sigma_i(x) = \begin{cases} \sigma(x) & ;\ x \in B_i \\ x & ;\ \text{otherwise} \end{cases}$$

Notice $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$ and these σ_i commute with one another.

Definition 3.2 A permutation $\sigma \in S_A$ is called a *cycle* if it has at most one orbit of cardinality greater than one. If said orbit has k elements, σ is said to be a *k-cycle*.

Definition 3.3 Two cycles are said to be *disjoint* if their orbits are disjoint.

Definition 3.4 A *transposition* is a 2-cycle.

Theorem 3.5 Every permutation can be written as a product (composition) of transpositions.

> We start by introducing cycle notation. Let $(a_1\, a_2\, \ldots\, a_k)$ denote the k-cycle that takes $a_i \mapsto a_{i+1}$ and $a_k \mapsto a_1$. This notation makes it clear that
> $$(a_1\, a_2\, \ldots\, a_k) = (a_1\, a_k) \cdots (a_1\, a_3)(a_1\, a_2)$$
> And any permutation is the product of k-cycles, we are done.

Note Let $\sigma_1 = (a_1\, \ldots\, a_k)$, $\sigma_2 = (b_1\, \ldots\, b_m)$ and $\tau = (a_i\, b_j)$. Without losing generality, suppose $i = j = 1$. Compute:

$$\begin{aligned}\tau\sigma_1\sigma_2 &= (a_1\, b_1)(a_1\, \ldots\, a_k)(b_1\, \ldots\, b_m)\\ &= (b_1\, \ldots\, b_m\, a_1\, \ldots\, a_k)\end{aligned}$$

Consider $\sigma = (a_1\, a_j)(a_1\, \ldots\, a_k$ Then $\sigma = (a_1\, \ldots\, a_{j-1})(a_j\, a_{j+1}\, \ldots\, a_k)$. So if i and j are in the same orbit of σ, then the cycles of σ are the same except that the cycle containing i and j is broken into two cycles.

Lecture 4 30 Sep 2016

Definition 4.1 We say a permutation is *even* (resp. *odd*) if it can be written as a product of an even (resp. odd) number of transpositions.

Theorem 4.2 No permutation is both even and odd.

Definition 4.3 The group of even permutations of $\{1, \ldots, n\}$ is called the *alternating group* denoted A_n.

Lemma 4.4 A_n is generated by 3-cycles.

> We will consider the case where there are two 2-cycles and this can be

extended to any even permutation. If the 2 cycles are disjoint,

$$(a\,b)(c\,d) = (a\,c\,b)(a\,c\,d)$$

otherwise,

$$(a\,b)(a\,c) = (a\,c\,d)$$

So any even permutation can be written as a product of pairs of transpositions and each pair can be written as a product of 3-cycles, as desired.

Lemma 4.5 If $n \geq 5$, then any two 3-cycles in S_n are conjugate by an element of A_n.

Let $\sigma_1 = (a\,b\,c)$ and $\sigma_2 = (a\,b\,c)$. Let $\gamma \in S_n$ map $a \mapsto e$, $b \mapsto f$, $c \mapsto g$. Note,

$$\gamma\sigma_1\gamma^{-1} = \gamma(a\,b\,c)\gamma^{-1} = (e\,f\,g) = \sigma_2$$

If γ is even, we are done. Otherwise, choose distinct $r, s \in \{1, 2, \ldots, n\} \backslash \{a, b, c\}$. Such r, s exist since $n \geq 5$. Let $\tau = (r\,s)$. Since τ and σ are disjoint, they commute, hence

$$\begin{aligned} (\gamma\tau)\sigma_1(\gamma\tau)^{-1} &= (\gamma\tau)\sigma_1(\tau^{-1}\gamma^{-1}) \\ &= \gamma(\tau\sigma_1)\tau^{-1}\gamma^{-1} \\ &= \gamma(\sigma_1\tau)\tau^{-1}\gamma^{-1} \\ &= \gamma\sigma_1\gamma^{-1} = \sigma_2 \end{aligned}$$

and $\gamma\tau$ is even as desired.

Corollary 4.6 If a normal subgroup N of A_n contains a 3-cycle, then N contains all 3-cycles of S_n.

Theorem 4.7 A_n is simple if and only if $n \geq 5$.

The forward direction can be done ad hoc for $n < 5$.
Let N be a normal subgroup of A_n.

Case 1: N contains a 3-cycle. By the above corollary, it contains all 3-cycles, so since A_n is genereated by 3-cycles, $N = A_n$. We now wish to reduce the nontrivial cases to this case. That is, we wish to show that N contains a 3-cycle in each of the following cases.
Case 2: N contains an element $\sigma = (a_1\ a_2\ \ldots\ a_r)\tau$ where $r \geq 4$ and τ is a product of cycles which are disjoint from $(a_1\ \ldots\ a_r)$. Let $\delta = (a_1\ a_2\ a_3)$. Then $\delta^{-1} = (a_1\ a_2\ a_3)$. Then $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$. But

$$\begin{aligned}\sigma^{-1}(\delta\sigma\delta^{-1}) &= [\tau^{-1}(a_r\ \ldots\ a_1)](a_1\ a_2\ a_3)[(a_1\ \ldots\ a_r)\tau](a_1\ a_2\ a_3)\\ &= (a_1\ a_2\ a_3)\end{aligned}$$

as desired.

Lecture 5 3 Oct 2016

Case 3: N contains $\sigma = (a_1\ a_2\ a_3)(a_4\ a_5\ a_6)\tau$ where τ is a product of disjoint cycles which are disjoint from $(a_1\ a_2\ a_3)$ and $(a_4\ a_5\ a_6)$. Let $\delta = (a_1\ a_2\ a_4)$, so $\delta^{-1} = (a_1\ a_4\ a_2)$. Then, $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$. However, $\sigma^{-1}(\delta\sigma\delta^{-1}) = (a_1\ a_4\ a_2\ a_6\ a_3)$, so we are done by case 2.
Case 4: N contains $\sigma = (a_1\ a_2\ a_3)$ where τ is product of disjoint 2-cycles which are disjoint from $(a_1\ a_2\ a_3)$. Then $\sigma^2 \in N$. However, since τ is a product of disjoint 2-cycles, $\tau^2 = ()$, so

$$\sigma^2 = (a_1\ a_2\ a_3)^2\tau^2 = (a_1\ a_2\ a_3)^2 = (a_1\ a_3\ a_2)$$

as desired.
Case 5: Every $\sigma \in N$ is a product of an even number of disjoint 2-cycles. Say $\sigma = (a_1\ a_2)(a_3\ a_4)\tau$ where τ is a product of an even number of 2-cycles which are disjoint from $(a_1\ a_2)$ and $(a_3\ a_4)$. If $\delta = (a_1\ a_2\ a_3)$, then $\sigma^{-1}(\delta\sigma\delta^{-1}) = (a_1\ a_3)(a_2\ a_4)$. Since $n \geq 5$, we can choose $b \in \{1, \ldots, n\}\backslash\{a_1, a_2, a_3, a_4\}$. Then $\xi = (a_1\ a_3\ b) \in A_n$ and $\gamma = (a_1\ a_3)(a_2\ a_3) \in N$. Further, $\gamma(\xi\gamma\xi^{-1}) \in N$ and $\gamma(\xi\gamma\xi^{-1}) = (a_1\ a_3\ b)$.

* * *

Definition 5.1 A *category* $\mathscr{C}$ is a class of objects, denoted $\mathrm{Ob}(\mathscr{C})$, and for each $A, B \in \mathrm{Ob}(\mathscr{C})$ a set $\mathrm{Hom}_{\mathscr{C}}(A, B)$ of morphisms. For each $A, B, C \in$

$\mathrm{Ob}(\mathscr{C})$, there is a binary operation $\mathrm{Hom}_{\mathscr{C}}(A,B)\times\mathrm{Hom}_{\mathscr{C}}(B,C) \to \mathrm{Hom}_{\mathscr{C}}(A,C)$ (where we write the image of (f,g) by $g \circ f$) such that

(1) If $A \neq A'$ or $B \neq B'$, then $\mathrm{Hom}_{\mathscr{C}}(A,B) \cap \mathrm{Hom}_{\mathscr{C}}(A',B') = \emptyset$

(2) The binary operation $\circ$ is associative.

(3) For each $A \in \mathrm{Ob}(\mathscr{C})$, there is and element $1_A \in \mathrm{Hom}_{\mathscr{C}}(A,A)$ such that $1_A \circ g = g$ and $f \circ 1_A = f$ for $g \in \mathrm{Hom}_{\mathscr{C}}(B,A)$ and $f \in \mathrm{Hom}_{\mathscr{C}}(A,B)$.

Lecture 6 5 Oct 2016

Example Some common examples of categories.

- `Set` is the category of sets where the morphisms are maps.
- `Grp` is the category of groups with homomorphisms.
- `Ab` is the category of abelian groups with homomorphisms.
- `Rng` is category of rings category of rings with ring homomorphisms.
- `Top` is the category of topological spaces with continuous maps.
- `HTop` is the category of topoligical spaces whose morphisms are homotopy classes of continuous maps.

Definition 6.1 If $\mathscr{C}$ and $\mathscr{D}$ are categories, a *covariant functor* $F : \mathscr{C} \to \mathscr{D}$ is a map $F : \mathrm{Ob}(\mathscr{C}) \to \mathrm{Ob}(\mathscr{D})$ and for each $A, B \in \mathrm{Ob}(\mathscr{C})$, we have a map $F_{AB} : \mathrm{Hom}_{\mathscr{C}}(A,B) \to \mathrm{Hom}_{\mathscr{D}}(F(A),F(B))$ such that

(1) If $f \in \mathrm{Hom}_{\mathscr{C}}(A,B)$ and $g \in \mathrm{Hom}_{\mathscr{C}}(B,C)$ then $F(g \circ f) = F(g) \circ F(f)$.

(2) $F(1_A) = 1_{F(A)}$.

Definition 6.2 A *contravariant functor* from $\mathscr{C}$ to $\mathscr{D}$ is a map $F : \mathrm{Ob}(\mathscr{C}) \to \mathrm{Ob}(\mathscr{D})$ and for each $A, B \in \mathrm{Ob}(\mathscr{C})$, we have a map $F_{AB} : \mathrm{Hom}_{\mathscr{C}}(A,B) \to \mathrm{Hom}_{\mathscr{D}}(F(B),F(A))$ such that

(1) If $f \in \mathrm{Hom}_{\mathscr{C}}(A,B)$ and $g \in \mathrm{Hom}_{\mathscr{C}}(B,C)$ then $F(g \circ f) = F(f) \circ F(g)$.

(2) $F(1_A) = 1_{F(A)}$.

Definition 6.3 In a category $\mathscr{C}$, $A \in \mathrm{Ob}(\mathscr{C})$ is said to be an *initial object* in $\mathscr{C}$ if for each $B \in \mathrm{Ob}(\mathscr{C})$, there is a unique morphism $f \in \mathrm{Hom}_{\mathscr{C}}(A,B)$.

Lecture 7 7 Oct 2016

Definition 7.1 $A \in \mathrm{Ob}(\mathscr{C})$ is a *terminal object* in $\mathscr{C}$ if for each $B \in \mathrm{Ob}(\mathscr{C})$ there is a unique morphism $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$.

Definition 7.2 Let $\{A_i\}_{i\in I}$ be a family of objects in the category $\mathscr{C}$. Then a product for $\{A_i\}_{i\in I}$ is an object P together with a family of morphisms $\{\pi_i \in \mathrm{Hom}(P, A_i)\}$ such that if $\{g_i \in \mathrm{Hom}_{\mathscr{C}}(H, A_i)\}$ is any family of morphisms, then there exists a unique $g \in \mathrm{Hom}_{\mathscr{C}}(H, P)$ such that $\pi_i \circ g = g_i$ for every $i \in I$.

Note Given a family of objects $\{X_i\}_{i\in I}$ in $\mathscr{C}$, we can define a category $\mathscr{D}$ whose objects are pairs $(A, \{a_i \in \mathrm{Hom}_{\mathscr{C}}(A, X_i)\}_{i\in I})$. Say A with $\{a_i\}$ and B with $\{b_i\}$ are objects in this category, a morphism from the former to the latter would be completely determined by a morphism $f : A \to B$ such that $a_i = b_i \circ f$ for all i. The product of $\{X_i\}$ can be equivalently defined as the terminal object of $\mathscr{D}$.

Theorem 7.3 Products exists in *Grp*.

> Let $\{A_i\}_{i\in I}$ be a family of groups and P be their Cartesian product. More precisely, an element of P is and I-tuple whose ith coordinate is an element of A_i. Denote the ith coordinate of $x \in P$ by x_i. Notice P is a group with coordinate-wise operation, that is, the ith coordinate of xy is $x_i y_i$. Let $\{\pi_i\}_{i\in I}$ be the projection maps on P, i.e $\pi_i(x) = x_i$. We claim that P with $\{\pi_i\}$ is a product of *Grp*. Let G be some group and $\{g_i : G \to A_i\}$ be a family of morphisms in *Grp*. Define $g : G \to P$ by $g(x)_i = g_i(x)$. Indeed, $\pi_i \circ g = g_i$ by definition. Moreover, g is unique since any other morphism would not have this property.

Lecture 8 10 Oct 2016

Definition 8.1 If S is a subset of a group (respectively monoid) G, then the *subgroup* (respectively *submonoid*) of G *generated by* S is the intersection of all subgroups (respectively submonoids) of G containing S.

Note The submonoid of a monoid G generated by $S \subseteq G$ consists of the set of all finite products of elements of S where the empty product is the identity. Further, if G is a group, then the subgroup of G generated by S is the submonoid of G generated by $S \bigcup S^{-1}$ where S^{-1} is the set of inverses of S.

Note If S is a subset of a group (or monoid) G which generates G and $f : S \to H$ is a map into a group (or monoid) H, then there exists at most one homomorphism $\overline{f} : G \to H$ such that $\overline{f}|_S = f$. In short, a group (or monoid) homomorphism is completely determined by where it sends the set of generators.

Definition 8.2 Let S be a set . A *free group* on S is a group G together with a map $\lambda : S \to G$ such that if g is a map on S into a group H, then there is a unique homomorphism $\overline{g} : G \to H$ such that $\overline{g} \circ \lambda = g$.

Note We can generalize this notion to any concrete category (that is, a category whose objects are sets). A free group is simply a free object in *Grp*.

Definition 8.3 Let $\mathscr{C}$ be a concrete category, X be a set, A an object in $\mathscr{C}$, and $i : X \to A$ a map between sets. We say A together with i is a *free object* in $\mathscr{C}$ if for any object B in $\mathscr{C}$ and map $f : X \to B$ between sets, there is a unique morphism $g \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ such that $g \circ i = f$.

Note This property of free objects is sometimes abbreviated by simply drawing the following diagram:

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "f"'] & A \arrow[d, dashed, "g"] \\ & B \end{tikzcd}$$

and saying it *commutes* which in general means that all paths between two objects are equivalent.

Theorem 8.4 Free monoids exist.

> Let S be a set. Define $M(S) := \{(s_1, \ldots, s_n) | n \geq 0, s_i \in S\}$. $M(S)$ is a monoid with concatenation and identity $(\,)$. We have the canonical injection $\varphi : S \to M(S)$ defined by $\varphi(s) = (s)$. Given a map f

from S to some monoid H, define $\overline{f} : M(S) \to H$ by $\overline{f}(s_1, \dots, s_n) = f(s_1)\cdots f(s_n)$. One can check that the respective diagram commutes.

Theorem 8.5 Free groups exist.

Let S be a set and $\overline{S}$ be a set disjoint from S such that there is a bijection from S to $\overline{S}$. Given $s \in S$, denote its image via this bijection by s^{-1}. We say an element $w \in M(S \cup \overline{S})$ is of the form

$$w = s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k}$$

where $s_i \in S$ and $\varepsilon_i = \pm 1$ and we say $w' \in M(S \cup \overline{S})$ is *obtained* from w if $s_i = s_{i+1}$ and $\varepsilon_i = -\varepsilon_{i+1}$ and

$$w' = s_1^{\varepsilon_1} \dots s_{i-1}^{\varepsilon_{i-1}}\, s_{i+2}^{\varepsilon_{i+2}} \dots s_k^{\varepsilon_k}$$

We call this process elementary reduction and we say w is a *reduced word* if $s_i = s_{i+1}$ implies $\varepsilon_i = \varepsilon_{i+1}$ for all i.
Define an equivalence relation $\sim$ by $w \sim w'$ meaning there is a sequence of words in $M(S \cup \overline{S})$ $w = w_1, w_2, \dots w_{n-1}, w_n = w'$ such that either w_i is obtained from w_{i+1} for all i or w_{i+1} is obtained from w_i for all i. This is indeed an equivalence relation on $M(S \cup \overline{S})$. Moreover, if $w_1 \sim w_1'$ and $w_2 \sim w_2'$, then $w_1 w_2 \sim w_1' w_2'$. Hence the multiplication (concatenation) on $M(S \cup \overline{S})$ induces multiplication on $M(S \cup \overline{S})/\sim$ and $M(S \cup \overline{S})/\sim$ is a group. So far, we have the following sequence of maps:

$$S \longrightarrow S \cup \overline{S} \longrightarrow M(S \cup \overline{S}) \longrightarrow M(S \cup \overline{S})/\sim$$

Suppose we are given a map $f : S \to H$ for some group H. Define $f' : S \cup \overline{S} \to H$ by $f'(s^{\pm 1}) = f(s)^{\pm 1}$. Let $f'' : M(S \cup \overline{S}) \to H$ be the unique map given by $M(S \cup \overline{S})$ being the free monoid on $S \cup \overline{S}$ and let g be the map induced by f'' on $M(S \cup \overline{S})/\sim$. One can check that the following diagram commutes:

$$\begin{tikzcd} S \arrow[r] \arrow[drr, bend right, "f"'] & S \cup \overline{S} \arrow[r] \arrow[dr, "f'"] & M(S \cup \overline{S}) \arrow[r] \arrow[d, "f''"] & M(S \cup \overline{S})/\sim \arrow[dl, dashed, "g"] \\ & & H & \end{tikzcd}$$

Lecture 9 12 Oct 2016

Note We've shown that a free group is a set equivalence classes $M(S \cup \overline{S})/\sim$

Theorem 9.1 Each equivalence class of $M(X \cup \overline{X})/\sim$ contains a unique reduced word.

Let S be the set of reduced words in $M(S \cup \overline{S})$ and $P(S)$ be the group of permutations of S. For each $x \in X$, define $f_x \in P(S)$ defined by

$$f_x(x_1^{\varepsilon_1}, \ldots, x_n^{\varepsilon_n}) = \begin{cases} (x, x_1^{\varepsilon_1}, \ldots, x_n^{\varepsilon_n}) & \text{if } x_1^{\varepsilon_1} \neq x^{-1} \\ (x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n}) & \text{if } x_1^{\varepsilon_1} = x^{-1} \end{cases}$$

Note $f_{-x} \circ f_x = id$. So define the map of sets $g : X \to P(S)$ by $g(x) = f_x$ and let $F(X)$ be the free group on X. By definition, we have the following commutative diagram:

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[dr, "g"'] & F(X) \arrow[d, dashed, "\overline{g}"] \\ & P(S) \end{tikzcd}$$

where $\overline{g}$ is the induced homomorphism of groups. Note that if $w \sim w'$ are reduced words in $M(X \cup \overline{X})$, then $\overline{g}(w) = \overline{g}(w')$. In particular, $\overline{g}(w)() = \overline{g}(w')()$, so $w = w'$.

Theorem 9.2 Let X be a subset of a group G. The following are equivalent:

(i) The inclusion $X \to G$ is a free group on X.

(ii) X generates G.

(iii) X generates G and if w is a non-trivial reduced word in G, then $w \neq 1$.

(iv) Each element of G can be written uniquely as $x_1^{n_1} \cdots x_k^{n_k}$, $n_i \in \mathbb{Z} \backslash \{0\}$ such that $x_i \neq x_{i+1}$ for each i.

Corollary 9.3 If F is a free group on the set X and $Y \subseteq X$ and G is the subgroup of F generated by Y, the G is free on Y.

Corollary 9.4 Let F by the free group on $\{a, b\}$. For each $i \in \mathbb{Z}$, let $c_i = a^{-i}ba^i \in F$. Let G be the subgroup of F generated by $\{c_i \mid i \in \mathbb{Z}\}$. Then G is the free group on $\{c_i\}$.

Since

$$a^{-i_1} b^{r_1} a^{i_1 - i_2} \cdots a^{i_{n-1} - i_n} b^{r_n} a^{i_n} \neq 1$$

when $r_j \neq 0$ for any j, the desired statement follows from the above theorem.

Theorem 9.5 Let $F(X)$ be the free group on X. Then $F(X) \cong F(Y)$ iff $|X| = |Y|$.

($\Leftarrow$) This implication is clear from the construction of the free group.

($\Rightarrow$) If X is infinite, we are done. Otherwise, $\mathrm{Hom}_{\texttt{Grp}}(F(X), \mathbb{Z}_2) \cong \mathrm{Hom}_{\texttt{Grp}}(F(Y), \mathbb{Z}_2)$. But, $|\mathrm{Hom}_{\texttt{Grp}}(F(X), \mathbb{Z}_2)| = |\mathrm{Hom}_{\texttt{Set}}(X, \mathbb{Z}_2)| = 2^{|X|}$, so $2^{|X|} = 2^{|Y|}$ and thus $|X| = |Y|$.

Lecture 10 14 Oct 2016

Definition 10.1 A *coproduct* of a family $\{G_i\}$ of objects (ie groups) is a family of morphisms (ie group homomorphisms) $\{\lambda_i : G_i \to G\}$ into an object (ie group) G such that if $\{f_i : G_i \to H\}$ is another family of morphisms and H another object, there exists a unique morhpsim $f : G \to H$ such that $f \circ \lambda_i(x) = f_i(x)$ for all i.

Note Just as the categorcal product can be defined as a terminal object in a category, the categorical coproduct can be defined as the initial object in a similar category.

Note Coproducts are uniquely determined up to unique homomorphism.

Exercise 2 If $\{\lambda_\alpha : G_\alpha \to G\}$ is a coproduct of $\{G_\alpha\}$, then each λ_α is injective.

Fix $\alpha \in I$. For each $\beta \in I$, define $f_\beta : G \to G_\alpha$ by

$$f_\beta = \begin{cases} 0 & \text{if } \alpha \neq \beta \\ id_{G_\beta} & \text{if } \alpha = \beta \end{cases}$$

By definition of coproduct, there exists a unique morphism f such that the following diagram commutes:

$$\begin{tikzcd} G_\beta \arrow[r, "\lambda_\beta"] \arrow[dr, "f_\beta"] & G \arrow[d, dashed, "f"] \\ & G_\alpha \end{tikzcd}$$

Taking $\alpha = \beta$, we get $f \circ \lambda_\beta = id_{G_\beta}$. In other words, λ_β has a left inverse, so λ_β is injective.

Lemma 10.2 If $\{X_i\}$ is a pairwise disjoint family of sets, then the inclusions $\{\iota_i : F(X_i) \to F(\cup X_i)\}$ are a coproduct in `Grp`.

$$\begin{tikzcd} X_i \arrow[r, "r_i"] \arrow[d, "s_i"] & \bigcup X_i \arrow[d, "s"] \\ F(X_i) \arrow[r, hook, "\iota_i"] \arrow[d, "g_i"] & F(\bigcup X_i) \\ H & \end{tikzcd}$$

Consider this diagram where r_i are the inclusions into the union and s_i and s are the respective maps given by the freeness of $F(X_i)$ and $F(\bigcup X_i)$. The maps $g_i \circ s_i$ induce a map $g' : \bigcup X_i \to H$ such that the following diagram commutes:

$$\begin{tikzcd}
X_i \arrow[r, "r_i"] \arrow[d, "s_i"] & \bigcup X_i \arrow[d, "s"] \arrow[ddl, dashed, "g'"'] \\
F(X_i) \arrow[r, hook, "\iota_i"] \arrow[d, "g_i"] & F(\bigcup X_i) \\
H &
\end{tikzcd}$$

Since $F(\bigcup X_i)$ is free on $\bigcup X_i$, g' induces a unique morphism $g : F(\bigcup X_i) \to H$ such that $g \circ s = g'$ Moreover, $g \circ \iota_i = g_i$ due again to the freeness of $F(X_i)$ and $F(\bigcup X_i$ on X_i and $\bigcup X_i$ respectively. So the desired diagram commutes:

$$\begin{tikzcd}
X_i \arrow[r, "r_i"] \arrow[d, "s_i"] & \bigcup X_i \arrow[d, "s"] \arrow[ddl, dashed, "g'"'] \\
F(X_i) \arrow[r, hook, "\iota_i"] \arrow[d, "g_i"] & F(\bigcup X_i) \arrow[dl, bend left, "g"] \\
H &
\end{tikzcd}$$

Note A special case of the above statement is that $F(X) = F\left(\bigcup\{x\}\right)$ is a coproduct of the family $\{F(\{x\})\}$. Thus the existence of free groups follows from the existence of coproducts in `Grp`.

Note Let S be a generating set of the group G. Then there is a homomorphism $g : F(S) \to G$ the following commutes:

$$\begin{tikzcd}
S \arrow[r, "\lambda"] \arrow[dr, "\iota"'] & F(S) \arrow[d, dashed, "g"] \\
& G
\end{tikzcd}$$

Moreover, g is surjective since $g(S)$ generates G. Thus $G \cong F(S)/H$ where $H = \ker(g)$. If T is a generating subset of H, then $\langle S|T\rangle$ is called a *presentation* of G.

Lecture 11 17 Oct 2017

Theorem 11.1 Any family $\{G_\alpha\}$ of groups has a coprodict in `Grp`.

Suppose G_α has a presentation $\langle X_\alpha | R_\alpha \rangle$. Recall that a presentation $\langle X|R \rangle$ consists of a set X, a surjective homomorphism $\varphi : F(X) \to G$ and a set R of relations of G (ie a generating set of $\ker(\varphi)$). We can assume without losing generality that $X_\alpha \cap X_\beta = \emptyset$ for $\alpha \neq \beta$. Let $G = \langle \cup X_\alpha | \cup R_\alpha \rangle$ where $F(\cup X_\alpha) \to G$ is the canonical map. By von Dyck's Theorem (Hungerford p67), the inclusion $X_\alpha \to \cup X_\alpha$ induces a homomorphism $\iota_\alpha : G_\alpha \to G$. We claim that $\{\iota_\alpha\}$ is a coproduct. Let $\{f_\alpha : G_\alpha \to H\}$ be a family of homomorphisms. Now, f_α induces a homomorphisms $\psi_\alpha : F(X_\alpha) \to H$ such that $\langle R_\alpha \rangle^{F(X_\alpha)} = \ker(\psi_\alpha)$. There is a homomorphism $\psi : F(\cup X_\alpha) \to H$ such that $\psi|_{X_\alpha} = \psi_{alpha}$. Since $\langle \cup R_\alpha \rangle^{F(\cup X_\alpha)} = \ker(\psi)$, then ψ induces a homomorphism $f : G \to H$ with $\psi = f \circ \varphi$.

Theorem 11.2 If $\{\lambda_\alpha : G_\alpha \to G\}$ is a coproduct of $\{G_\alpha\}$ and we identify G_α with a subgroup of a group G via λ_α, then each element of G can be written as $w = g_{\alpha_1} g_{\alpha_2} \cdot g_{\alpha_n}$ where $n \geq 0$ and we write () for the empty word, $g_{\alpha_i} \in G_{\alpha_i} \backslash \{1_{G_{\alpha_i}}\}$.