Lecture Notes by Jonathan Alcaraz (UCR)

Algebra

Math 201A Fall 2016

Based on Lectures by

Dr. David Rush University of California, Riverside

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 composition.

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 *automorphism*.

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

$$L_{q_1q_2}(x) = g_1g_2x = g_1L_{q_2}(x) = L_{q_1}(L_{q_2}(x))$$

so f is in fact a homomorphism. To show f is injective, we intend to show it has trivial kernal. 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 kernal 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 kernal 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 $\{g_ih_j\}$ is a set of representatives of K in G. These cover G since

$$G = \bigcup g_i H = \bigcup g_i h_i K$$

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_{σ} 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 $1 \le i \le k$, 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 $(a_1 \ a_2 \dots a_k)$ denote the k-cycle that takes $a_i \mapsto a_{i+1}$ and $a_k \mapsto a_1$. This notation makes it clear that

$$(a_1 \ a_2 \ \dots \ a_k) = (a_1 \ a_k) \cdots (a_1 \ a_3)(a_1 \ a_2)$$

And any permutation is the product of k-cycles, we are done.

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

$$\tau \sigma_1 \sigma_2 = (a_1 \ b_1)(a_1 \dots a_k)(b_1 \dots b_m)$$
$$= (b_1 \dots b_m \ a_1 \dots a_k)$$

Consider $\sigma = (a_1 \ a_j)(a_1 \dots a_k$ Then $\sigma = (a_1 \dots a_{j-1})(a_j \ a_{j+1} \dots a_k)$. 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 $\{1, ..., n\}$ 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 $r, s \in \{1, 2, ..., n\} \setminus \{a, b, c\}$. Such r, s exist since $n \geq 5$. Let $\tau = (r s)$. Since τ and σ are disjoint, they commute, hence

$$(\gamma \tau)\sigma_1(\gamma \tau)^{-1} = (\gamma \tau)\sigma_1(\tau^{-1}\gamma^{-1})$$
$$= \gamma(\tau \sigma_1)\tau^{-1}\gamma^{-1}$$
$$= \gamma(\sigma_1 \tau)\tau^{-1}\gamma^{-1}$$
$$= \gamma \sigma_1 \gamma^{-1} = \sigma_2$$

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 generated 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 $\sigma = (a_1 \ a_2 \dots a_r)\tau$ where $r \geq 4$ and τ is a product of cycles which are disjoint from $(a_1 \dots a_r)$. 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

$$\sigma^{-1}(\delta\sigma\delta^{-1}) = [\tau^{-1}(a_r \dots a_1)](a_1 \ a_2 \ a_3)[(a_1 \dots a_r)\tau](a_1 \ a_2 \ a_3)$$
$$= (a_1 \ a_2 \ a_3)$$

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 $b \in \{1, \ldots, n\} \setminus \{a_1, a_2, a_3, a_4\}$. 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 $\operatorname{Hom}_{\mathscr{C}}(A,B) \cap \operatorname{Hom}_{\mathscr{C}}(A',B') = \emptyset$
- (2) The binary operation \circ is associative.
- (3) For each $A \in \text{Ob}(\mathscr{C})$, there is and element $1_A \in \text{Hom}_{\mathscr{C}}(A, A)$ such that $1_A \circ g = g$ and $f \circ 1_A = f$ for $g \in \text{Hom}_{\mathscr{C}}(B, A)$ and $f \in \text{Hom}_{\mathscr{C}}(A, B)$.

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.
- \bullet 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 $f \in \text{Hom}_{\mathscr{C}}(A, B)$ and $g \in \text{Hom}_{\mathscr{C}}(B, C)$ 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 $f \in \text{Hom}_{\mathscr{C}}(A, B)$ and $g \in \text{Hom}_{\mathscr{C}}(B, C)$ 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 $A \in \text{Ob}(\mathscr{C})$ is a *terminal object* in \mathscr{C} if for each $B \in \text{Ob}(\mathscr{C})$ there is a unique morphism $f \in \text{Hom}_{\mathscr{C}}(A, B)$.

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 $\{\pi_i \in \operatorname{Hom}(P, A_i)\}$ such that if $\{g_i \in \operatorname{Hom}_{\mathscr{C}}(H, A_i)\}$ is any family of morphisms, then there exists a unique $g \in \operatorname{Hom}_{\mathscr{C}}(H, P)$ 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 $(A, \{a_i \in \operatorname{Hom}_{\mathscr{C}}(A, X_i)\}_{i\in I})$. 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_iy_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 $g\in \operatorname{Hom}_{\mathscr C}(A,B)$ such that $g\circ i=f$.

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



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 $\overline{f}(s_1, \ldots, s_n) = f(s_1) \cdots f(s_n)$. 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

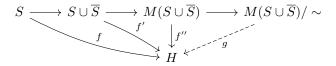
$$w' = s_1^{\varepsilon_1} \dots s_{i-1}^{\varepsilon_{i-1}} s_{i+2}^{\varepsilon_{i+2}} \dots s_k^{\varepsilon_k}$$

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 $w_1w_2 \sim w_1'w_2'$. 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:



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 set of permutations of S.