MS Algebra I/II Recitation Notes

Ethan Lu

Last Updated: October 12, 2021

Contents

1 Recitation 1: Preliminaries (8/31/21)

EXERCISE 1.1 **Associativity**

Show that, if $\circ$ is an associative operation, then any valid parenthesization of $g_1 \circ g_2 \circ \cdots \circ g_n$ is equal to

$$g_1 \circ (g_2 \circ \cdots (g_{n-1} \circ g_n))).$$

Proof. We proceed by induction on n. The base case $n = 2$ is clear.
Now fix $n \geq 3$ and assume that the statement holds for all integers $< n$. Consider an arbitrary parenthesization of $g_1 \circ \cdots \circ g_n$ as above, and decompose it as

$$e_1 \circ e_2 := \underbrace{(g_1 \circ \cdots \circ g_k)}_{\text{parenthesized somehow}} \circ \underbrace{(g_{k+1} \circ \cdots \circ g_n)}_{\text{parenthesized somehow}}$$

for $k < n$. Then by hypothesis, we have

$$e_1 = g_1 \circ (g_2 \circ \cdots \circ (g_{k-1} \circ g_k)))$$

and hence

$$e_1 \circ e_2 = (g_1 \circ (\cdots \circ (g_{k-1} \circ g_k))) \circ e_2 = g_1 \circ (\cdots \circ (g_{k-1} \circ g_k)) \circ e_2)$$

by associativity. Applying the hypothesis again, we get the desired conclusion. ■

As just a quick reminder, some definitions discussed in class:

Definition 1. $(G, \cdot)$ is a **semigroup** if $\cdot : G \times G \to G$ is an associative operation.

Definition 2. $(G, \cdot)$ is a **monoid** if it's a semigroup and there exists $e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$.

Definition 3. $(G, \cdot)$ is a **group** if it's a monoid and for all $g \in G$, there exists $h \in G$ such that $gh = hg = e$.

EXAMPLE 1.2 **Semigroups, Monoids, and Groups**

Classify the following.

1. $(\{0, 1, \cdots, n-1\}, +)$.
2. $(\{1, \cdots, n-1\}, \times)$.
3. $(\mathbb{R}^{3\times 3}, \times)$ (i.e. the set of 3×3 matrices).
4. $\{M \in \mathbb{R}^{3\times 3} \mid \det(M) = 1\}$.
5. $\{M \in \mathbb{Z}^{3\times 3} \mid \det(M) = 1\}$.
6. (Strings, +).

2 Recitation 2: Permutation Groups (9/7/21)

Below, X will be a fixed (possibly infinite) set and $\sigma : X \to X$ an arbitrary permutation.

Let $\sim$ be the binary relation on X such that $x \sim y \iff \exists k \in \mathbb{Z} \mid y = \sigma^k(x)$.

EXERCISE 2.1

Show that $\sim$ is an equivalence relation.

Let's call the equivalence classes "cycles."

EXERCISE 2.2

Show that for each $x \in X$ that its cycle $[x]$ is either a finite loop or an infinite "line."

Now let's say that X is finite, i.e. that up to relabeling, $X = \{1, 2, ..., n\}$.
The result we've proved above gives us a much more compact way of specifying σ: rather than writing out something like this:

x	0	1	2	3	4	5	6	7	8	9
$\sigma(x)$	0	2	9	5	4	7	6	3	8	1

we can just write $\sigma := (1,2,9)(3,5,7)$.

EXERCISE 2.3

Show any disjoint cycles commute.

EXERCISE 2.4

Show that the representation above is unique up to commuting cycles.

EXERCISE 2.5

Let $X = \{1, \cdots, 9\}$, $\sigma := (1,2,9)(3,5,7)$, and $\tau := (1,3,2)(4,9)$. Compute $\sigma\tau$.

This next exercise has some connections to the **Orbit-Stabilizer** theorem, which we'll probably be talking about next week:

EXERCISE 2.6

Let $x \in X$. Show that $G := \{k \in \mathbb{Z} : \sigma^k(x) = x\}$ is a subgroup of $\mathbb{Z}$. By homework, this implies G is either trivial or $n\mathbb{Z}$ for $n \in \mathbb{N}$. What do these cases correspond to?

EXERCISE 2.7

Suppose $|X| < \infty$, and $\sigma, \tau \in S_X$. Show that σ, τ are conjugate to each other iff they have the same cycle decomposition.

Proof. $\implies$: I kinda messed this up in recitation so I'll actually write up something that works here. Suppose that $\sigma = \pi\tau\pi^{-1}$, i.e. that π witnesses conjugacy of the two. Then for any $x \in X$,

$$[x]_\sigma = \bigcup_{k\in\mathbb{N}} \sigma^k(x) = \bigcup_{k\in\mathbb{N}} \pi\tau^k(\pi^{-1}x) = \pi[\pi^{-1}x]_\tau$$

where we write $[x]_\sigma, [x]_\tau$, to denote the cycle of x according to the respective permutations. Note then that applying π to any subset of X preserves it's cardinality, and hence we can identify any equivalence class according to τ with a corresponding equivalence class of π that has the same cardinality, so we're done!
$\impliedby$: Exercise!

■

3 Recitation 3: Group Actions (9/14/21)

As just a quick reminder, some definitions discussed in class:

Definition 4. A **group action** of the group G on the set X (denoted by $G \curvearrowright X$), is either (or equivalently)

- A homomorphism $G \to S_X$.
- A function $\cdot : G \times X \to X$ such that
  1. $e \cdot x = x \quad \forall x \in X$
  2. $g_1 g_2 \cdot x = g_1 \cdot (g_2 \cdot x) \forall g_1, g_2 \in G, x \in X$

THEOREM 3.1

Suppose that G is a group and $H \leq G$ with $[G : H] = n$. Then $\exists N \leq H$ normal in G with $[G : N]$ dividing $n!$ Hint: consider the action $G \curvearrowright G/H$ by left multiplication.

The next several exercises will build up to the following result.

THEOREM 3.2

Suppose G is a group such that $|G| = p^2$. Then either $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ or $G \cong \mathbb{Z}_{p^2}$.

Now we'll show some quick auxiliary results needed for the next result.

Definition 5. The **center** $Z(G)$ of a group G is the set

$$Z(G) := \{g \in G \mid gh = hg \quad \forall h \in G\}.$$

EXERCISE 3.3

Show that $Z(G)$ is a normal subgroup.

EXERCISE 3.4

Show if $G/Z(G)$ is cyclic, than it's trivial.

EXERCISE 3.5

Show that if G is a nontrivial p-group, then $Z(G) \neq \{e\}$.

EXERCISE 3.6

Use the previous 3 results to prove the theorem.

Recall for any two groups G, H, we can equip their Cartesian product $G \times H$ with the group structure of their **direct product** (i.e. the coordinate-wise product).

EXERCISE 3.7

Show that the direct product $G \times H$:

1. has subgroups isomorphic to G and H.
2. has quotients isomorphic to G and H.

Proposition 1. *The 5 subgroups of order 8 are:*

1. $\mathbb{Z}_8$.
2. $\mathbb{Z}_4 \times \mathbb{Z}_2$.
3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
4. D_8.
5. *The quaternions.*

Back to group action stuff:

EXERCISE 3.8

Show that if $H \leq G$, then $gHg^{-1} \leq G$ for all $g \in G$, and hence that we have a natural action $G \curvearrowright \{H \mid H \leq G\}$.

Recall the following:

Definition 6. The sign $\operatorname{sgn}(\sigma)$ of a permutation σ is $(-1)^{T(\sigma)}$, where $T(\sigma)$ is the number of 2-cycles in any valid decomposition of σ into two-cycles.

Definition 7. The **alternating group** A_n is the set

$$A_n := \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$$

EXERCISE 3.9

Show that:

1. $\sigma \mapsto (1 + \operatorname{sgn}(\sigma))/2$ is a homomorphism from S_X to $\mathbb{Z}_2$, and hence that $A_n \leq S_n$.
2. 3-Cycles are always even.
3. Whenever $n > 4$ any two 3-cycles are conjugate in A_n.

4 Recitation 4: Sylow's Theorems and Friends (9/21/21)

Today we'll be reviewing Sylow's theorems with some applications. A quick reminder of what those are:

Definition 8. $H \leq G$ is a **Sylow p-subgroup** if it's a maximal p-subgroup.

THEOREM 4.1 **(Sylow's theorems)**

---

1. Sylow p-subgroups exist; that is, for all groups G, with $|G| = p^k m$, $\exists H \leq G$ with $|H| = p^k$.
2. Any two Sylow p-subgroups are conjugate to each other.
3. The number of Sylow p-groups $n_p(G)$ satisfies:
   - $n_p(G) = [G : N_G(H)]$ (in particular, $n_p(G)$ divides m).
   - $n_p(G) \equiv 1 \pmod{p}$.

Now we'll show some auxiliary results that will be useful in showing simplicity of A_5.

EXERCISE 4.2

Any group with order 15 is cyclic.

EXERCISE 4.3

Any group with order 30 has a subgroup of order 15.

The counting type argument used above is pretty cool, and will be useful in the next result, but make sure that you're careful when using it! In particular, we're exploiting cyclicity to conclude that $H \cap K = \{e\}$ for any H, K both p-groups, but this doesn't necessarily work when $|H|, |K|$ are higher powers of p.

EXERCISE 4.4

Any group with order 60 and $n_5(G) > 1$ is simple. Hint: first show that $5 \nmid |H|$ for any proper $H \trianglelefteq G$, then do some quotient trickery.

COROLLARY 4.5

A_5 is simple. Hint: consider $\langle (1,2,3,4,5) \rangle$ and $\langle (1,3,2,4,5) \rangle$.

THEOREM 4.6

A_n is simple.

Proof. We didn't actually get to this in recitation, so see section 4.6 in Dummit and Foote. ■

COROLLARY 4.7

A_n is generated by 3-cycles. Hint: Use the results from last week to show that the group generated by 3-cycles is normal in A_n.

5 Recitation 5: Nilpotence and Solvability (9/28/21)

Recall the following definitions from class:

Definition 9. Given a group G, the **commutator** $[g, h]$ of any two elements $g, h \in G$ is defined via

$$[g, h] := g^{-1}h^{-1}gh$$

and is extended to sets $A, B \subseteq G$ via

$$[A, B] := \langle \{[a, b] \mid a \in A, b \in B\} \rangle.$$

Definition 10. The **derived series** of a group G is the sequence of subgroups $\{G^{(i)}\}_{i \in \mathbb{N}}$ defined recursively via $G^{(0)} = G, G^{(i+1)} = [G^i, G^i]$. The **lower central series** of a group G is the sequence of subgroups $\{G^i\}_{i \in \mathbb{N}}$ defined recursively via $G^0 = G, G^{i+1} = [G, G^i]$.

Definition 11. A group is **solvable** if $G^{(i)} = \{e\}$ for some $i \in \mathbb{N}$. The smallest such i for which this happens is the solvable length of the group. A group is **nilpotent** if $G^i = \{e\}$ for some $i \in \mathbb{N}$. The smallest such i for which this happens is the nilpotency class of the group.

EXERCISE 5.1

Recall that D_{2n} is the dihedral group on n elements. Show that D_{2n} is generated by the elements $r := x \mapsto x + 1 \pmod{n}$, $s := x \mapsto -x \pmod{n}$ and further that we have the identities:

- $s^2 = r$.
- $sr = r^{-1}s$.
- $sr^k = r^{-k}s$.

EXERCISE 5.2

Show that D_{2n} is always solvable, and that it's nilpotent iff $n = 2^k$ for $k \in \mathbb{N}$.

EXERCISE 5.3

Let $D_{2\mathbb{N}}$ be the automorphism group of the bi-infinite graph on $\mathbb{Z}$; that is, the graph with edges between k and $k + 1$ for all $k \in Z$. Show that this group is generated by r, s as above and that the same identities hold. Classify the nilpotence and solvability of this group.

Definition 12. Recall that given two groups G, H where $G \curvearrowright H$ by automorphisms, we can define the **semidirect** product $H \rtimes G$ on $H \times G$ via

$$(g_0, h_0)(g_1, h_1) = (h_0(g_0 \cdot h_1), g_0 g_1)$$

EXERCISE 5.4

Suppose that $A \in \mathbb{Z}^{2\times 2}$ with determinant ± 1. Show that $\mathbf{x} \mapsto A\mathbf{x}$ is an automorphism on $(\mathbb{Z}^2, +)$. Conclude that this naturally induces an action $\mathbb{Z} \curvearrowright \mathbb{Z}^2$ via $n \cdot \mathbf{x} = A^n \mathbf{x}$.

EXERCISE 5.5

Show that the semi-direct product above is always solvable. Show also that when $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ this group is nilpotent but when $A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ it's not.

6 Recitation 6: Midterm Review (10/5/21)

Not much to say here :)

7 Recitation 7: Rings and Category Stuff (10/12/21)

As per usual, let's start by recalling some definitions from class.

Definition 13. A ring is a structure $(R, +, \times)$ where $+, \times$ are binary operations on R such that $(R, +)$ is an abelian group, $(R, \times)$ is a semigroup, and for all $a, b, c \in R$:

$$a \times (b + c) = a \times b + a \times c \quad \text{and} \quad (a + b) \times c = a \times c + b \times c$$

Definition 14. A **ring homomorphism** between rings R, S is a function $\varphi : R \to S$ such that $\varphi(r + s) = \varphi(r) + \varphi(s)$ and $\varphi(rs) = \varphi(r)\varphi(s)$ for all $r, s \in R$. In the case R, S have 1, it's called **unital** if $\varphi(1_R) = 1_S$.

EXERCISE 7.1

Suppose R is a ring with 1. Show that there exists a unique unital ring hom $\varphi : \mathbb{Z} \to R$.

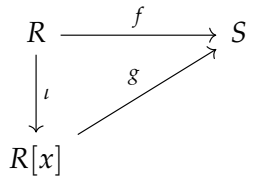
Recall also that given any commutative ring with 1 R, we can form the polynomial ring $R[x]$ by "adding in x" and having it commute with everything. (Technically the assumptions of commutativity and the existence of a unit aren't necessary, but they make things slightly nicer so for the purposes of this handout we'll assume it).

EXERCISE 7.2

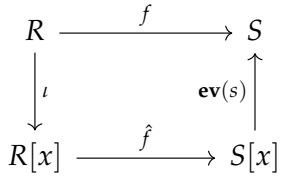
Show that $\iota : R \to R[x]$ via $\iota(r) = r$ is an injective ring homomorphism.

EXERCISE 7.3

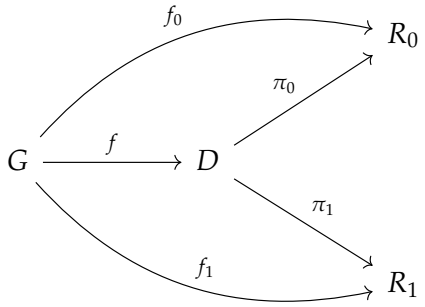
Let R, S be commutative rings with 1, $f : R \to S$ be a homomorphism, and $s \in S$. Show that there exists a unique ring hom $g : R[x] \to S$ such that $g \circ \iota = f$ and $g(x) = s$. (e.g. that the following diagram commutes).



Remark. This is **the universal property of polynomial rings**, and can actually be used as a defining property for $R[x]$. What's really going on in our construction is the following.



Definition 15. Suppose R_0, R_1 are algebraic structures. We call D a **direct product** of R_0, R_1 if D is also a structure (of the same type) and there exists $\pi_i : D \to R_i$ homomorphisms such that for any other structure G and homomorphisms $f_i : G \to R_i$, there exists a unique $f : G \to D$ such that the following diagram commutes.



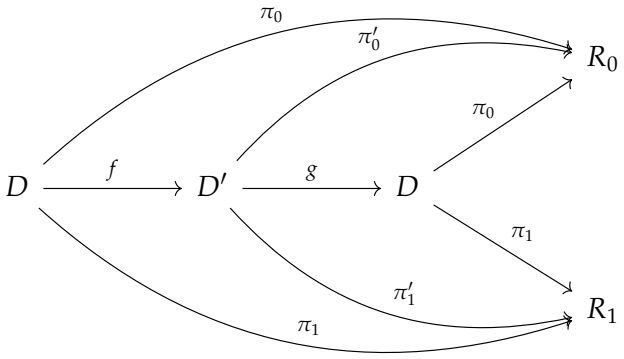
EXERCISE 7.4 **The direct product is a direct product**

Show that $R_0 \otimes R_1$ as defined in class is a direct product.

EXERCISE 7.5

Show that the direct product is unique up to isomorphism.

Proof. Let D, D' be any two direct products with associated homomorphisms π_i, π_i'. Take a moment to reflect on the following diagram:



where f, g are the (unique!) homomorphisms guaranteed by the universal property. By the universal property of D on itself, we see that we must have $f \circ g = \mathbf{Id}_D$, and hence by symmetric logic, $g \circ f = \mathbf{Id}_{D'} \implies f$ is an isomorphism.

■

Remark. The same construction above generalizes to direct products of arbitrarily many algebraic structures, though the exact numerology gets a bit more subtle when you're dealing with infinite products.