Math 720 Notes - Spring 2026

0 Category Theory

Definition 0.1. A **category** C consists of:

1. a collection of **objects**, $\mathrm{ob}(\mathsf{C})$

2. for every two objects A and B of C, a collection $\mathrm{Hom}_{\mathsf{C}}(A, B)$ of **morphisms**, satisfying the following properties:

   - One can compose morphisms: two morphisms $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(B, C)$ determine a morphism $gf \in \mathrm{Hom}_{\mathsf{C}}(A, C)$. That is, for every triple of objects A, B and C, there is a function

   $$\mathrm{Hom}_{\mathsf{C}}(A, B) \times \mathrm{Hom}_{\mathsf{C}}(B, C) \to \mathrm{Hom}_{\mathsf{C}}(A, C),$$

     and the image of the pair (f, g) is denoted gf.

   - This 'composition law' is associative: if $f \in \mathrm{Hom}_{\mathsf{C}}(A, B), g \in \mathrm{Hom}_{\mathsf{C}}(B, C)$, and $h \in \mathrm{Hom}_{\mathsf{C}}(C, D)$, then

   $$(hg)f = h(gf).$$

   - For every object A of C, there exists a morphism $1_A \in \mathrm{Hom}_{\mathsf{C}}(A, A)$, the 'identity' on A, which is an identity with respect to composition: that is, for all $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(B, A)$ we have

   $$f 1_A = f, \; 1_A g = g.$$

   - The collections $\mathrm{Hom}_{\mathsf{C}}(A, B)$ are disjoint.

Exercise 1. Identify some categories you've already seen in math. What are the objects? What are the morphisms? Do the morphisms satisfy the required axioms?

1 The Categories Ring and Rng

1.1 Ring Basics

Definition 1.1. We say R is a **ring** with operations $+, \cdot$ if

1. $(R, +)$ is an abelian group; we denote its additive identity by 0_R or 0 when the base ring is clear (i.e. $0 + a = a$ for all $a \in R$)

2. Multiplication is associative, that is, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, d \in R$.

3. The operations $+, \cdot$ are distributive, that is $(a+b) \cdot c = a \cdot c + b \cdot c \in R$ for all $a, b, c \in R$.

4. In the course, we will also require R to have a multiplicative identity, which we denote 1_R or 1 (i.e. $1 \cdot a = a \cdot 1 = a$ for all $a \in R$). If R satisfies the all but this last condition, we will call it a rng (some texts will not make this distinction).

Notation: We might write $a \cdot b$ as ab for convenience.

Remark 1.2. The category Ring is the category whose objects are rings with a multiplicative identity, and whose morphisms are ring homomorphisms, which we will define in the next section. The category of rings where a multiplicative identity is not required is denoted Rng.

Exercise 2. Let R be a ring, and $a, b \in R$. Recall that $-a$ denotes the additive inverse of a. Prove the following:

1. $0 \cdot a = 0 = a \cdot 0$

2. $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$

3. $(-a) \cdot (-b) = a \cdot b$

4. 1_R is unique.

Definition 1.3. A ring is called **commutative** if $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{R}$

Definition 1.4. Let R be a ring and $a \in R$. We say a is **invertible** (or, a is a **unit**) if there exists an element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Exercise 3. Let R be a ring and $a \in R$. Prove that if a is invertible, then a^{-1} is unique.

1.2 Types of Rings: Fields, Integral Domains

Definition 1.5. Let R be a ring with $1 \neq 0$. We say R is a **division ring** if every element of R is invertible. A commutative division ring is called a **field**.

Definition 1.6. Let R be a ring, and $a \in R$. We say a is a **zero-divisor** if there exists $b \in R \setminus \{0\}$ such that either $a \cdot b = 0$ or $b \cdot a = 0$.

Exercise 4. Prove that if k is a field, then 0 is its only zero-divisor.

Exercise 5. Find an example of a ring R whose only zero-divisor is 0, but which is not a field.

Exercise 6. Find all zero-divisors of $\mathbb{Z}/6\mathbb{Z}$.

Exercise 7. Let $R^* = \{u \in R \mid u \text{ is invertible}\}$, the set of units of R. Prove that $(R^*, \cdot)$ is a group.

Definition 1.7. Let R be commutative ring. Then we say R is an **integral domain** if every nonzero element of R is a non zero-divisor. Equivalently, $ab = 0 \implies a = 0$ or $b = 0$ for all $a, b \in R$.

Exercise 8. Find three examples of rings you already know, and ensure at least one example is not commutative, and at least one has a zerodivisor other than 0.

1.3 Subrings

Definition 1.8. Let R be a ring. We say that $S \subseteq R$ is a **subring** of R if $s \subseteq R$ is an additive subgroup and S is closed under multiplication ($x, y \in S \implies xy \in S$). Since we will work in the category Ring, we also require that $1_R \in S$.

Exercise 9. Check that if S is a subring of R, then S is also a ring itself, and $1_S = 1_R$.

1.4 Polynomial Rings

Definition 1.9. Let R be a commutative ring. Then we denote

$$R[x] := \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N}, a_i \in R\},$$

the set of polynomials in the indeterminant x with coefficients in R. If

$$f = a_0 + a_1 x + \cdots + a_n x^n \in R$$

with $a_n \neq 0$ then we say the **degree** of f is n, and denote this $\deg(f) = n$.

Exercise 10. Check that $R[x]$ is a commutative ring with respect to "the usual" operations of addition and multiplication of polynomials.

Proposition 1.10. *Let R be an integral domain, and let $f, g \in R[x]$. Then*

1. $\deg(fg) = \deg(f) + \deg(g)$
2. *$R[x]$ is an integral domain*
3. *If $f \in R[x]$ is a unit, then $f \in R$ and f is a unit in R.*

Exercise 11. Prove the proposition above.

Exercise 12. Find an example of a ring R and $f, g \in R[x]$ such that $\deg(fg) < \deg(f) + \deg(g)$.

1.5 Ring homomorphisms

Definition 1.11. Let R and S be rings. A map $\varphi : R \to S$ is called a **ring homomorphism** if for all $a, b \in R$,

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$,
2. $\varphi(ab) = \varphi(a)\varphi(b)$, and
3. $\varphi(1_R) = 1_S$ (This last condition is not required for morphisms in the category Rng).

Exercise 13. Prove that for any ring homomorphism $\varphi : R \to S$, we have that $\varphi(0_R) = 0_S$.

Exercise 14. Let R be a subring of a ring S, and let $a \in R$. Decide which of the following are ring homomorphisms:

1. The *inclusion map*, $\iota : R \hookrightarrow S$, sending $r \mapsto r$.
2. The projection map $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sending $z \mapsto [z]_n$
3. The "multiplication by 2" map $\varphi : \mathbb{Z} \to \mathbb{Z}$ sending $z \mapsto 2z$.
4. The "evaluation at 1" map: $\varphi_1 : R[x] \to R$, sending $f \mapsto f(1)$.
5. The "evaluation at a" map: $\varphi_a : R[x] \to R$, sending $f \mapsto f(a)$.

Definition 1.12. Let $\varphi : R \to S$ be any map.
Recall that φ is **injective** if $\varphi(a) = \varphi(b) \implies a = b$ and is **surjective** if for all $s \in S$ there exists an $r \in R$ such that $\varphi(r) = s$.
We say φ is **bijective** if it is both injective and surjective.
A bijective ring homomorphism is called an **isomorphism**.

Remark 1.13. Note that a bijective ring homorphism φ has a unique inverse φ^{-1}.

Definition 1.14. Let $\varphi : R \to S$ be a ring homomorphism. Then we define the **kernel** of φ by

$$\ker \varphi =: \{x \in R \mid \varphi(x) = 0\}$$

and the **image** of φ by

$$\operatorname{im} \varphi =: \{\varphi(x) \mid x \in R\}$$

Exercise 15. Let $\varphi : R \to S$ be a ring homomorphism. Show that $\operatorname{im} \varphi$ is a subring of S.

Proposition 1.15. *Let $\varphi : R \to S$ be a ring homomorphism. The following are equivalent:*

1. *φ is injective*
2. *$\varphi(x) = 0 \implies x = 0$*
3. *$\ker \varphi = \{0\}$*

Exercise 16. Prove the proposition above.

1.6 Ideals

Definition 1.16. Let R be a ring. We say $I \subseteq R$ is a **right (respectively left) ideal** of R if:

1. I is a subgroup of $(R, +)$.
2. For every $a \in I$ and $r \in R$, we have $ar \in I$ (respectively $ra \in I$)

When I is both a right and left ideal, we call it a **two-sided ideal**, or just an **ideal**.

Example 1.17. For any $n \in \mathbb{Z}$, the set $n\mathbb{Z} = \{nz \mid z \in Z\}$ forms an ideal of $\mathbb{Z}$

Exercise 17. Let R be a ring, and let $a \in R$. Prove that the set $aR = \{ar \mid r \in R\}$ is a right ideal of R.
Is $RaR = \{ras \mid r, s \in R\}$ a two sided ideal of R?

Exercise 18. Let R be a ring and let $I \subseteq R$ be a subset of R. Explain why in order to check that I is a left ideal, it suffices to check that for every $a, b \in I$ and $r \in R$, $r \cdot (a - b)$ is an element of I (and similarly for right, two-sided).

Exercise 19. Let $\varphi : R \to S$ be a ring homomorphism. Show that $\ker \varphi$ is a two-sided ideal of R.

Note: We will soon see that every two-sided ideal of a ring R is the kernel of some ring homomorphism.

1.7 Operations with Ideals

Notation 1.18. Let R be a ring and let I, J be ideals of R. Denote:

$$I + J := \{i + j \mid i \in I, j \in J\}$$

and

$$IJ := I \cdot J := \{i_1 j_1 + \dots i_n j_n \mid n \in \mathbb{N}, i_k \in I, j_k \in J \text{ for all } k\}$$

Proposition 1.19. *Let I, J be ideals of a ring R. Then $I + J$ is the smallest ideal containing both I and J.*

Exercise 20. Prove the proposition above.

Exercise 21. Find an example of two ideals I, J in a ring R, such that $I \cup J$ is not an ideal.

Exercise 22. Let I, J be ideals of a ring R. Prove that IJ is an ideal of R.

Proposition 1.20. *Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a family of ideals of a ring R. Then $\bigcap_{\lambda\in\Lambda} I_\lambda$ is an ideal of R.*

Exercise 23. Prove the proposition above.

Exercise 24. Let $m, n \in \mathbb{Z}$, and let $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$. Describe the following sets:

1. $I \cap J$
2. $I \cdot J$
3. $I + J$
4. $I \cup J$

Exercise 25. Let I, J be ideals of a ring R. Show that $I \cdot J \subseteq I \cap J$, and then give an example where $I \cdot J \neq I \cap J$.

1.8 Quotient Rings

Definition 1.21. Let R be a ring, and $I \subseteq R$ a two-sided ideal. We can define an equivalence relation on R be $a \sim b \iff a - b \in I$, and denote by $\bar{a} = \{r \in R | r \sim a\}$. Then we define the **quotient ring**:

$$R/I = \{\bar{r} \mid r \in R\}$$

with $+, \cdot$ inherited from R, that is, $\overline{a} + \overline{b} := \overline{a+b}$ and $\overline{a} \cdot \overline{b} := \overline{ab}$.

Exercise 26. Explain what it means for the operations $+, \cdot$ on R/I to be *well-defined*, and then check that they are well-defined. Further, check that R/I is a ring. Why do we need I to be a two-sided ideal?

Example 1.22. For any $n \in \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ forms the quotient ring with elements $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

Exercise 27. Consider the map $\pi : R \to R/I$ defined by $r \mapsto \overline{r}$. Prove that π is a surjective ring homomorphism and then compute $\ker \pi$.

1.9 Isomorphism Theorems

Theorem 1.23 (The First Isomorphism Theorem)**.** *Let $\varphi : R \to S$ be a ring homomorphism. Then*

$$\frac{R}{\ker \varphi} \cong \operatorname{im} \varphi$$

Exercise 28. Prove this theorem by checking that φ induced a well-defined ring homomorphism $\tilde{\varphi} : R/\ker \varphi \to \operatorname{im} \varphi$, and then check that it is an isomorphism.

Theorem 1.24 (The Second Isomorphism Theorem)**.** *Let R be a ring and let S be a subring of R, and I and ideal of R. Then $S + I$ is a subring of R and*

$$\frac{S+I}{I} \cong \frac{S}{S \cap I}$$

Exercise 29. Prove this theorem by defining a map $\varphi : S \to (S + I)/I$, and then applying the first isomorphism theorem.

Theorem 1.25 (The Third Isomorphism Theorem)**.** *Let $I \subseteq J$ be ideals of a ring R. Then J/I is an ideal of R/I and*

$$\frac{R/I}{J/I} \cong R/J$$

Exercise 30. Prove this theorem by defining a map $\varphi : R/I \to R/J$, and then applying the first isomorphism theorem.

Theorem 1.26. *Let I be an ideal of a ring R. Then there is a one-to-one correspondence*

$$\{\textit{ideals of } R \textit{ that contain } I\} \longleftrightarrow \{\textit{ideals of } R/I\}$$

and similarly

$$\{\textit{subrings of } R \textit{ that contain } I\} \longleftrightarrow \{\textit{subrings of } R/I\}$$

Exercise 31. Prove the first correspondence in the theorem above (the second will be similar). Define a map (of sets) $\varphi : \{\text{ideals of } R \text{ that contain } I\} \to \{\text{ideals of } R/I\}$ by $\varphi(J) = J/I$ and a map $\psi : \{\text{ideals of } R/I\} \to \{\text{ideals of } R \text{ that contain } I\}$ by $\psi(K) = \{x \in R \mid \bar{x} \in K\}$, and show these maps are inverses (and so are both bijections of sets).

1.10 Properties of Ideals

Definition 1.27. Let R be a ring with $1 \neq 0$. Let $A \subseteq R$ be a subset. We define the (two-sided) **ideal generated by** A by

$$(A) := \bigcap_{\substack{I \supseteq A \\ I \text{ ideal}}} I.$$

Some texts will denote (A) by $\langle A \rangle$. Note that since this is an intersection of ideals, it is also an ideal. Moreover, by the way it is defined, it is the *smallest* ideal that contains A.

Proposition 1.28. *Let $A \subseteq R$ be a subset, and let R be a ring. Then the ideal generated by A is given by* $(A) = \{r_1a_1s_1 + r_2a_2s_2 + \cdots + r_na_ns_n \mid n \in \mathbb{N},\ a_i \in A,\ r_i, s_i \in R\}$.

Proof. First, note that the set $L = \{r_1a_1s_1 + \cdots + r_na_ns_n \mid n \in \mathbb{N},\ a_i \in A,\ r_i, s_i \in R\}$ is an ideal of R (you should think about why!).

Now $A \subseteq L$ because for any $a \in A$, $a = 1 \cdot a \cdot 1 \in L$. Thus, $\langle A \rangle \subseteq L$, since L is one of our ideals in the intersection defining A.

Now we will show that $L \subseteq \langle A \rangle$. Let $\ell = r_1a_1s_1 + \cdots + r_na_ns_n \in L$, where by definition, $a_i \in A$. Now let $I \subseteq A$ be an ideal. Then $r_ia_is_i \in I$ since I is a two sided ideal, and so $\ell \in I$ since I is also closed under addition. Thus, since I was arbitrary, we have

$$\ell \in \bigcap_{\substack{I \supseteq A \\ I \text{ ideal}}} I = \langle A \rangle.$$

$\square$

Note: You could similarly define the left ideal or right ideal generated by A.

Definition 1.29. Let I be an ideal. If I is generated by a single element $a \in R$, so that $I = (\{a\})$, we say I is a **principal ideal**, which we typically denote by $I = (a)$.

Definition 1.30. If A is a finite set $A = \{a_1, \ldots, a_n\}$ and $I = (A)$, then we say I is a **finitely generated ideal**, which we typically denote by $I = (a_1, \ldots, a_n)$.

Definition 1.31. An ideal I such that $I \neq R$ is called a **proper** ideal.

Exercise 32. For each of the following rings, decide whether or not all ideals in the ring are principle. If not, give an example of a non-principal ideal.

1. $\mathbb{Z}$
2. $\mathbb{Z}[x]$
3. $\mathbb{R}[x]$
4. $\mathbb{Z}/6\mathbb{Z}$

Example 1.32. Hilbert's Basis Theorem tells us that if k is a field, all ideals in $k[x_1, \ldots, x_n]$ are finitely generated. The proof of this fact is typically covered in a commutative algebra or algebraic geometry class. Rings with this property (that all ideals are finitely generated) are called *Noetherian.*

Exercise 33. Let R be a ring, and I an ideal of R. Prove that $I = R$ if and only if I contains a unit.

Proposition 1.33. *Let R be a ring. Then R is a field if and only if its only ideals are (0) and R.*

Exercise 34. Prove the proposition above.

Corollary 1.34. *Let $\varphi : k \to S$ be a ring homomorphism, where k is a field. Then either $\varphi = 0$ (the map sending every element to 0) or φ is injective.*

Proof. Since $\ker \varphi$ is an ideal of k by Exercise 19, we see by Proposition 1.33 that $\ker \varphi = 0$, in which case φ is injecive by Proposition 1.15, or $\ker \varphi = R$, in which case φ is the map that sends every element of R to 0. $\square$

Definition 1.35. We say an ideal $\mathfrak{m}$ is **maximal** if $\mathfrak{m} \neq R$ and if $\mathfrak{m} \subseteq J$ for some ideal J, then $J = R$ or $J = \mathfrak{m}$.

Proposition 1.36. *Let R be a commutative ring. Then $\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field*

Exercise 35. Prove the proposition above. (Hint: Use Proposition 1.33).

Theorem 1.37. *Let R be a ring with $0 \neq 1$. Then every proper ideal is contained in a maximal ideal.*

We will prove this theorem in a homework problem, using Zorn's Lemma.

Exercise 36. Which ideals in $\mathbb{Z}$ are maximal?

Definition 1.38. Let R be a commutative ring with $1 \neq 0$. Then we say an ideal $P \in R$ is **prime** if $ab \in P \implies a \in P$ or $b \in P$.

Exercise 37. Find an ideal $\mathbb{Z}$ which is not prime, and prove your claim.

Proposition 1.39. *Let R be a commutative ring with $1 \neq 0$. Then an ideal $P \subseteq R$ is prime if and only if R/P is an integral domain.*

Exercise 38. Prove the proposition above.

Corollary 1.40. *Every maximal ideal is prime.*

Proof. If $\mathfrak{m}$ is a maximal ideal, then $R/\mathfrak{m}$ is a field by Proposition 1.36, which is also an integral domain by a homework exercise, so $\mathfrak{m}$ is prime by Proposition 1.39. $\square$

Proposition 1.41. *Let R be a commutative ring with $1 \neq 0$, and let $x \in R$. Then x is not a unit if and only if there exists a maximal ideal $\mathfrak{m}$ with $x \in \mathfrak{m}$.*

Exercise 39. Prove the proposition above. You may freely use that every proper ideal is contained in some maximal ideal.