3 A bit of review + generalizations

3.1 Fields and Vector Spaces

Definition 3.1. A **field** is a set $\mathbb{F}$ equipped with two associative and commutative binary operations $+$ and $\cdot$ such that

- $(\mathbb{F}, +)$ is an abelian group, with identity 0
- $(\mathbb{F}^\times = \mathbb{F} - \{0\}, \cdot)$ is an abelian group, with identity 1
- $a(b+c) = ab + ac$ (distributivity of $\cdot$ over $+$).

In other words, a field is a set where you can add, subtract, multiply, and divide just as you do with the real numbers.

Example 3.2. Here are some examples of fields:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ where p is prime (see next section)

Definition 3.3. A **vector space** over a field $\mathbb{F}$ is a set V with the two operations

- addition: $v + w$ for $v, w \in V$ and
- scalar multiplication: cv for $c \in \mathbb{F}$, $v \in V$

where

- $(V, +)$ is an abelian group with identity the *zero vector* $\vec{0}$
- $(ab)v = a(bv)$ for $a, b \in \mathbb{F}$ and $v \in V$ (associativity of scalar multiplication)
- $1v = v$
- $a(v+w) = av + aw$ and $(a+b)v = av + bv$ for $a, b \in \mathbb{F}$, $v, w \in V$ (distributivity).

Exercise 3.4. Note that if $0 = 0_{\mathbb{F}}$, then for any $v \in V$, $0v = \vec{0}$ (use distributivity). We usually just write the symbol 0 for both zeroes, because of this relationship.

Example 3.5. Here are some examples of vector spaces over a field $\mathbb{F}$. These are all probably quite familiar if you let $\mathbb{F} = \mathbb{R}$.

- $V = \mathbb{F}$
- $V = \mathbb{F}^n = \mathbb{F} \times \mathbb{F} \times \cdots \times \mathbb{F}$
- $V = M_{n \times n}(\mathbb{F})$, the set of all $n \times n$ matrices with entries in $\mathbb{F}$
- $V = \mathbb{F}[x]$, the set of polynomials in x with coefficients in $\mathbb{F}$

Definition 3.6. A **subspace** W of a vector space V over a field $\mathbb{F}$ is a *nonempty* subset closed under the operations of addition and scalar multiplication.

A subspace W is **proper** if it is neither $\{0\} \subset V$ nor $V \subset V$.

Example 3.7. The set of all continuous functions $\mathbb{R} \to \mathbb{R}$, denoted $C^0(\mathbb{R})$, is a vector space over $\mathbb{R}$. Observe that $\mathbb{R}[x]$ is a vector **subspace** of $C^0(\mathbb{R})$. [7]

Definition 3.8. Let V, W be vector spaces over a field $\mathbb{F}$. A **linear map** (which is short for "$\mathbb{F}$-linear map") is a function $\phi : V \to W$ that preserves the structure of vector spaces:

[7] We write $C^r(\mathbb{R})$ for the set of all r-times differentiable functions from $\mathbb{R} \to \mathbb{R}$. Notice that $\mathbb{R}[x] \subset C^\infty(\mathbb{R}) \subset \cdots \subset C^r(\mathbb{R}) \subset C^{r-1}(\mathbb{R}) \subset \cdots \subset C^1(\mathbb{R}) \subset C^0(\mathbb{R})$.

- $\phi(\vec{0}_V) = \vec{0}_W$
- $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$ for $v_1, v_2 \in V$
- $\phi(cv) = c\phi(v)$ for $v \in V$, $c \in \mathbb{F}$

Remark 3.9. In general, the word **linear** indicates that a map behaves like a linear function $f(x) = ax + b$, in the sense that if we have two coefficients c_1, c_2 and two elements x_1, x_2, then

$$f(c_1x_1 + c_2x_2) = c_1f(x_1) + c_2f(x_2).$$

This will come up in 150B when you talk about modules over rings, which are generalizations of vector spaces over fields.

Example 3.10. Let $A \in M_{n\times m}(\mathbb{R})$. (That is, n rows, m columns.) View A as a linear map $A : \mathbb{R}^m \to \mathbb{R}^n$. (Here, the **domain** of the function A is $\mathbb{R}^m$ and the **codomain** of the function A is $\mathbb{R}^n$.)

- The **nullspace** of A is the set of all vectors in the domain that are sent to 0 by A:

$$\text{null}(A) = \{v \in \mathbb{R}^m \mid Av = 0 \in \mathbb{R}^n\}.$$

- The **range** of A is the set of all output vectors in the codomain of A:

$$\text{range}(A) = \{Av \in \mathbb{R}^n \mid v \in \mathbb{R}^m\}.$$

Check that $\text{null}(A)$ is a subspace of $\mathbb{R}^m$, and $\text{range}(A)$ is a subspace of $\mathbb{R}^n$.

Exercise 3.11. How many elements are there in the vector space $\mathbb{F}_p^2$? How many different *proper* subspaces of $\mathbb{F}_p^2$ are there? HW04

3.2 Equivalence classes and partitions

A **partition** P of a set S is a subdivision of S into nonoverlapping, nonempty subsets. Here is a precise definition.

Definition 3.12. Let S be a set. A **partition** $P = \{P_i\}_{i\in I}$ is a set of subsets of S such that the following conditions hold:

- For all i, $P_i \neq \emptyset$.
- If $i \neq j$, then $P_i \cap P_j = \emptyset$.
- $P = \bigcup_{i\in I} P_i$.

In other words, a partition $P = \{P_i\}_{i\in I}$ is a collection of nonempty subsets of S such that for all $s \in S$, $s \in P_i$ for *exactly one* $i \in I$.

In this case, S is the *disjoint union* of the subsets in P:

$$S = \coprod_{i\in I} P_i.$$

Exercise 3.13. What are all the partitions of the set $[4]$?

Recall that a **relation** R on a set S is a subset of $S \times S$. (This is more general than a *function*.) If $(a, b) \in R$, we usually write $a \sim b$; however, note that a priori, we don't know if this relationship is symmetric, since $(a, b) \neq (b, a)$ in $S \times S$.

We care more about equivalence relations, though:

Definition 3.14. An **equivalence relation** on a set S is a relation $\sim$ that is

- **reflexive**: $a \sim a$
- **symmetric**: if $a \sim b$ then $b \sim a$
- **transitive**: if $a \sim b$ and $b \sim c$, then $a \sim c$

for all $a, b, c \in S$.

Definition 3.15. Let $\sim$ be an equivalence relation on S. Let $a \in S$. The **equivalence class of** a, denoted $[a]$ or $\bar{a}$, is the subset of S consisting of all elements that are related to a by $\sim$:

$$[a] = \{b \in S \mid a \sim b\}.$$

We say that a is a **representative** of its equivalence class.

Exercise 3.16. Let a, b be elements in a group G. We say a is **conjugate** to b if there exists $g \in G$ such that $b = gag^{-1}$. Prove that **conjugacy** is an equivalence relation. HW03

The following proposition states that *equivalence relations* and *partitions* are actually one and the same.

Proposition 3.17. An equivalence relation $\sim$ on a set S determines a partition P, and vice versa.

Proof. HW03 □

Remark 3.18. Let P denote the partition given by the equivalence relation $\sim$ on S. By the Axiom of Choice, no matter how large the cardinality of P is, we are able to choose a representative from each subset in P. That is, if $P = \{P_\alpha\}_{\alpha \in I}$ where I is an indexing set, it is possible to pick out a collection $\{s_\alpha\}_{\alpha \in I}$.

Remark 3.19. If S is empty, then the only partition is $P = \{\}$, i.e. P itself is the empty set. Then the conditions that make P a partition are vacuously true.

3.3 Modular arithmetic

We have talked a bit about $\mathbb{Z}/n\mathbb{Z}$ as well as the fields $\mathbb{F}_p$. Let's review their construction now using the ideas of equivalence classes / partitions, and discuss what it means for a function (i.e. set map) to be *well-defined*.

Two integers $a, b \in \mathbb{Z}$ are **congruent mod** n if $a - b \in n\mathbb{Z}$. In this case, we write $a \equiv b \mod n$.

Exercise 3.20. Check that $\equiv$ is an equivalence relation.

Let $\bar{a}$ denote the equivalence class of a under the equivalence relation $\equiv$. Observe that by the division algorithm, the set of numbers $\{0, 1, \ldots, n-1\}$ is a complete set of representatives (i.e. we have one representative from every equivalence class). So, the partition corresponding to $\equiv$ is

$$P = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\},$$

and we really think of $\bar{k}$ as the subset

$$\bar{k} = k + n\mathbb{Z} \subset \mathbb{Z}.$$

Proposition 3.21. Addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$, induced by $+, \cdot$ on $\mathbb{Z}$, are **well-defined.**

Proof. Check that if $a \equiv a'$ and $b \equiv b'$, then

1. $(a + b) \equiv (a' + b')$ and
2. $ab \equiv a'b'$.

□

The concept of "well-definedness" doesn't come from cold, hard mathematics, but rather our human tendency to make errors when trying to define a function (i.e. a set map).

Sometimes mathematicians ask whether a function is well defined. What they mean is this: "Does the rule you propose really assign to each element of the domain one and only one value in the codomain?"

- *The Art of Proof*, by Matthias Beck and Ross Geoghegan.

Example 3.22. If I try to define a function $f : \mathbb{N} \to \mathbb{R}$ by saying "$f(n)$ is the real number that squares to n", then I have not succeeded in defining a function, because, for example, it's ambiguous what $f(4)$ should be. You would then tell me, "f is not a well-defined function." By saying this you are not saying that f was ever actually a mathematical function at all; you are saying that this rule doesn't define a function.

Exercise 3.23. HW03 This exercise will show you an example of an assignment that is actually not well-defined, and is therefore not a function, as well as an example where a function is actually defined successfully.

(a) Prove that the following assignment is **not** a well-defined function between sets:

$$\begin{aligned} \varphi : \mathbb{Z}/10\mathbb{Z} &\to \mathbb{Z}/7\mathbb{Z} \\ \bar{k} &\mapsto \bar{k}. \end{aligned}$$

(Recall that $\bar{k}$ denotes the equivalence class of k in $\mathbb{Z}/n\mathbb{Z}$.)

(b) Prove that the following assignment **is** a well-defined function between sets:

$$\begin{aligned} \varphi : \mathbb{Z}/10\mathbb{Z} &\to \mathbb{Z}/5\mathbb{Z} \\ \bar{k} &\mapsto \bar{k}. \end{aligned}$$

4 Maps between groups

4.1 Homomorphisms

Definition 4.1. Let $(S, \square)$ and $(T, \blacktriangle)$ be groups. A **homomorphism**

$$\varphi : (S, \square) \to (T, \blacktriangle)$$

is a (set) map $\varphi : S \to T$ such that for all $a, b \in S$,

$$\varphi(a \,\square\, b) = \varphi(a) \blacktriangle \varphi(b).$$

Here's a more standard-looking definition of a group homomorphism:

Definition 4.2. Let G, G' be groups, written with multiplicative notation. A **homomorphism**

$$\varphi : G \to G'$$

is a map from G to G' such that for all $a, b \in G$,

$$\boxed{\varphi(ab) = \varphi(a)\varphi(b).}$$

This homomorphism condition is probably the most important equation in this class.

Example 4.3. Here are some familiar examples of homomorphisms.

- $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$
- $\operatorname{sgn} : S_n \to \{\pm 1\}$
- $i : S_n \to S_m$ where $n \leq m$
- $\exp : \mathbb{R}^+ \to \mathbb{R}^\times$, where $x \mapsto e^x$
- $\varphi : \mathbb{Z}^+ \to G$ where $\varphi(n) = a^n$ for a fixed element $a \in G$
- $|\cdot| : \mathbb{C}^\times \to \mathbb{R}^\times$