ALGEBRAIC STRUCTURES

Definition. A structure $\mathbb{F}$ is a **field** if $+$, $-$, $\times$, and $\div$ satisfy their "usual properties". Suppose $a, b, c \in \mathbb{F}$.
For addition,

closure: $a+b$ gives a result in $\mathbb{F}$;
associative: $a+b+c$ gives one, unique result, regardless of whether we first evaluate $a+b$ or $b+c$;
commutative: $a+b=b+c$;
identity: we can find $0 \in \mathbb{F}$ such that $a+0=a$, $0+a=a$;
inverse: we can find $-a \in \mathbb{F}$.

For multiplication,

closure: $a \times b$ gives a result in $\mathbb{F}$;
associative: $a \times b \times c$ gives one, unique result, regardless of whether we first evaluate $a \times b$ or $b \times c$;
commutative: $a \times b = b \times a$;
identity: we can find $1 \in \mathbb{F}$ such that $a \times 1 = a$, $1 \times a = a$;
distributive: $a \times (b+c) = a \times b + a \times c$.

Subtraction is merely addition of the inverse.
For division,

multiplicative inverse: we can find $a^{-1} \in \mathbb{F}$.

Example (of fields)**.** The rationals $\mathbb{Q}$, arithmetic modulo a prime $\mathbb{Z}_p = \mathbb{F}_p$, finite fields $\mathbb{F}_{p^k}$.

Example (of non-fields)**.** The natural numbers $\mathbb{N}$ do not have additive inverses for nonzero numbers. The integers $\mathbb{Z}$ have division only for ± 1. Arithmetic modulo a non-prime $\mathbb{Z}_n$ does not have multiplicative inverses for numbers that share common divisors with n.

Remark. Some properties of a field that we mentioned in class can be proved "easily" from the ones listed here. For instance, the **zero product property** states that if a and b are members of a field and $ab = 0$, then $a = 0$ or $b = 0$. The reason is that if $ab = 0$ and $a \neq 0$, then the field properties imply that a^{-1} is in the field, and by substitution $a^{-1}(ab) = a^{-1} \cdot 0$, so $\left(a^{-1}a\right) b = 0$, so $1b = 0$, so $b = 0$.

If you are wondering how we know that $a^{-1} \cdot 0 = 0$, that is because for *any* b in a field, $b \cdot 0 = b \cdot (0+0) = b \cdot 0 + b \cdot 0$. Since $b \cdot 0$ is in the field, it has an additive inverse, so $-(b \cdot 0) + b \cdot 0 = -(b \cdot 0) + (b \cdot 0 + b \cdot 0)$, so $0 = [-(b \cdot 0) + b \cdot 0]$, so $0 = 0 + b \cdot 0$, so $0 = b \cdot 0$.

Definition. A structure R is a **ring** if $+$, $-$, and $\times$ satisfy their "usual properties", but perhaps not $\div$.

Example (of rings)**.** Fields are rings where division also satisfies its "usual properties", so every field is a ring. The integers $\mathbb{Z}$ are also a ring. Arithmetic modulo a non-prime $\mathbb{Z}_n$ is a ring.

Example (of non-rings)**.** The natural numbers $\mathbb{N}$ lack additive inverses for most elements.

Remark. Rings that are not fields lack some multiplicative inverses. So, they might not satisfy the zero product property. For example, in $\mathbb{Z}_6$ we have $4 \cdot 3 \equiv 0$ even though $4 \not\equiv 0$ and $3 \not\equiv 0$.

Definition. A structure G is an **abelian group** if its one operation acts like $+$, and satisfies its "usual properties".

Remark. A **general group** characterizes phenomena of interest whose operation is not commutative, but otherwise behaves as usual. Such phenomena include matrix multiplication, function composition, geometric translation and rotation, and list permutation. We do not study such phenomena in this class.

Definition. A structure V is a **vector space** if V is a group under addition, and if **scalar multiplication** of elements of V by elements of its **ground field** $\mathbb{F}$ satisfies the "usual properties". Suppose $a, b \in \mathbb{F}$ and $\mathbf{u}, \mathbf{v} \in V$. For scalar multiplication,

closure: $a\mathbf{v}$ gives a result in V;
compatibility: $ab\mathbf{v}$ gives one, unique result, regardless of whether we first evaluate ab or $b\mathbf{v}$;
identity: $1\mathbf{v} = \mathbf{v}$;
distribution of scalars: $(a+b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$;
distribution of vectors: $a(\mathbf{u}+\mathbf{v}) = a\mathbf{u} + a\mathbf{v}$.

Remark. A vectors space always has a **basis**, a set of linearly independent vectors whose linear combinations generate the space. For a given vector space, the size of a basis is constant.

Example. Three-space $\mathbb{R}^3$ is a vector space over $\mathbb{R}$, with basis $\{(0,0,1),(0,1,0),(1,0,0)\}$. The finite field $\mathbb{F}_8$ is a vector space over $\mathbb{F}_2$, with basis $\{1, x, x^2\}$. Notice that every element of $\mathbb{F}_8$ has the form $a \cdot 1 + b \cdot x + c \cdot x^2$, where $a, b, c \in \mathbb{F}_2$.

Remark. Some properties of a vector space that we mentioned in class can be proved from the ones listed here. For instance, we can show that $0\mathbf{v} = 0$ from the fact that

$$\mathbf{v} + 0\mathbf{v} = 1\mathbf{v} + 0\mathbf{v} = (1+0)\mathbf{v} = 1\mathbf{v} = \mathbf{v}.$$