VECTOR SPACES

Loose definition: A *field* F is a set of numbers (scalars) with $+$, $-$, $\times$, $\div$ behaving similarly to the way they do with real numbers. Examples: $\mathbf{R}$, $\mathbf{Q}$ (rationals, = fractions), $\mathbf{C}$ (complex numbers). But NOT $\mathbf{Z}$ (integers): e.g., $2 \div 3 \notin \mathbf{Z}$, cannot divide and stay in $\mathbf{Z}$.

Definition: A *vector space* (or *linear space*) over a field F consists of a set V with operations of addition and scalar multiplication satisfying these rules:
V is an *abelian group* under $+$:
(V1) $u + v$ exists in V for all $u, v \in V$ (closed).
(V2) $u + v = v + u$ for all $u, v \in V$ (commutative).
(V3) $u + (v + w) = (u + v) + w$ for all $u, v, w \in V$ (associative).
(V4) There exists $0 \in V$ so that $v + 0 = 0 + v = v$ for all $v \in V$ (identity).
(V5) For every $v \in V$ there exists $-v \in V$ such that $v + (-v) = (-v) + v = 0$ (inverses).
Scalar multiplication properties:
(V6) αv exists in V for all $\alpha \in F, v \in V$.
(V7) $1v = v$ for all $v \in V$.
(V8) $\alpha(\beta v) = (\alpha\beta)v$ for all $\alpha, \beta \in F, v \in V$.
Distributive laws:
(V9) $(\alpha + \beta)v = \alpha v + \beta v$ for all $\alpha, \beta \in F, v \in V$ (scalar multn distributes over scalar addn).
(V10) $\alpha(u + v) = \alpha u + \alpha v$ for all $\alpha \in F, u, v \in V$ (scalar multn distributes over vector addn).
These ten rules are the *vector space axioms*.

FIELDS

So what is a field? We want operations of addition and multiplication, and also their inverse operations of subtraction and division, that behave similarly to the way they do in the real numbers.

Definition: A *field* consists of a set F with two binary operations $+$ and $\times$ satisfying the following rules.
F is an *abelian group* under $+$:
(F1) $\alpha + \beta$ exists in F for all $\alpha, \beta \in F$ (closed).
(F2) $\alpha + \beta = \beta + \alpha$ for all $\alpha, \beta \in F$ (commutative).
(F3) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for all $\alpha, \beta, \gamma \in F$ (associative).
(F4) There exists $0 \in F$ so that $\alpha + 0 = 0 + \alpha = \alpha$ for all $\alpha \in F$ (identity).
(F5) For every $\alpha \in F$ there exists $-\alpha \in F$ such that $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$ (inverses).
F is almost an abelian group under $\times$:
(F6) $\alpha\beta = \alpha \times \beta$ exists in F for all $\alpha, \beta \in F$ (closed).
(F7) $\alpha\beta = \beta\alpha$ for all $\alpha, \beta \in F$ (commutative).
(F8) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ for all $\alpha, \beta, \gamma \in F$ (associative).
(F9) There exists $1 \in F$, $1 \neq 0$, so that $\alpha \times 1 = 1 \times \alpha = \alpha$ for all $\alpha \in F$ (identity).
(F10) For every $\alpha \in F - \{0\}$ there exists $\alpha^{-1} \in F$ such that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$ (inverses for NONZERO elements).
Distributive law:
(F11) $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ for all $\alpha, \beta, \gamma \in F$.
These eleven rules are the *field axioms*.

Notes: (1) F is not an abelian group under $\times$. But if we exclude 0 and let $F^* = F - \{0\}$ (this is common notation) then F^* is actually an abelian group under $\times$, called the *multiplicative group of* F.

(2) The restriction $1 \neq 0$ excludes a trivial field with exactly one element.

(3) We can define subtraction by $\alpha - \beta = \alpha + (-\beta)$, and division by $\alpha \div \beta = \alpha\beta^{-1}$ $(\beta \neq 0)$.

Infinite fields: The fields we are already familiar with are infinite: $\mathbf{R}$ (obviously), $\mathbf{Q}$ (rationals, i.e., fractions p/q, p, q integer, $q \neq 0$), $\mathbf{C}$ (complex numbers, i.e. $a + ib$, $i^2 = -1$, $a, b \in \mathbf{R}$). Notice $\mathbf{Q}$ is *subfield* of $\mathbf{R}$, $\mathbf{C}$ is *extension* of $\mathbf{R}$.

Other examples: (1) $\mathbf{Q}(\sqrt{2})$, which consists of all numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbf{Q}$.

(2) $\mathbf{Q}(i)$, the *complex (or Gaussian) rational numbers*, which consists of all numbers of the form $a + bi$ where $a, b \in \mathbf{Q}$.

Finite fields: For any integer $n \geq 1$ we can define $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$, with addition and multiplication done *modulo* n. Modulo n means do operation normally, then take remainder after dividing by n. If p is a prime, $\mathbf{Z}_p$ is a field.

Examples: (1) In $\mathbf{Z}_7$, $4 + 4 = 1$, $4 \times 5 = 6$, $6 + 1 = 0$ so $-1 = 6$, $2 \times 4 = 1$ so $4^{-1} = 2$.

(2) Complete operation tables in $\mathbf{Z}_5$:

$$\begin{array}{c|ccccc} + & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 3 & 4 & 0 \\ 2 & 2 & 3 & 4 & 0 & 1 \\ 3 & 3 & 4 & 0 & 1 & 2 \\ 4 & 4 & 0 & 1 & 2 & 3 \end{array}, \qquad \begin{array}{c|ccccc} \times & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 \\ 2 & 0 & 2 & 4 & 1 & 3 \\ 3 & 0 & 3 & 1 & 4 & 2 \\ 4 & 0 & 4 & 3 & 2 & 1 \end{array}.$$

(3) And in $\mathbf{Z}_2$:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}, \qquad \begin{array}{c|cc} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}.$$

Here $+$ is logical XOR (exclusive or) operation, and $\times$ is logical AND operation.

General finite fields: It turns out there is a finite field with q elements precisely when q is a prime power. So there are fields of order $2, 3, 4, 5, 7, 8, 9$ but not of order 6 or 10. When q is a prime power, the field of order q is denote $GF(q)$.

When p is a prime, $GF(p)$ just means $\mathbf{Z}_p$. But when q is not a prime, $GF(q)$ is not the same as $\mathbf{Z}_q$. When $q = p^k$, p prime, we can construct $GF(q)$ by adding an extra number satisfying a particular type of polynomial equation to $\mathbf{Z}_p$, like adding i satisfying $i^2 = -1$ to $\mathbf{R}$ to get $\mathbf{C}$.

Example: (4) We can think of $GF(4)$ as obtained from $\mathbf{Z}_2$ by throwing in x with $x^2 = x + 1$. Then $GF(4) = \{0, 1, x, x + 1\}$ with addition and multiplication as follows:

$$\begin{array}{r|rrrr} + & 0 & 1 & x & x+1 \\ \hline 0 & 0 & 1 & x & x+1 \\ 1 & 1 & 0 & x+1 & x \\ x & x & x+1 & 0 & 1 \\ x+1 & x+1 & x & 1 & 0 \end{array}, \qquad \begin{array}{r|rrrr} \times & 0 & 1 & x & x+1 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & x & x+1 \\ x & 0 & x & x+1 & 1 \\ x+1 & 0 & x+1 & 1 & x \end{array}.$$

Fields $GF(2^k)$ are particularly important; vector spaces over these fields are often used to construct error-correcting codes.

Subfields

To prove that something is a subfield, we have a theorem very similar to the Subspace Theorem for vector spaces.

Subfield Theorem: Suppose F is a field and $E \subseteq F$. Then E is a subfield of F (a field using the operations of addition and multiplication inherited from F) if and only if the following five conditions hold.

(SF1) $0 \in E$.

(SF2) $1, -1 \in E$.
(SF3) E is closed under addition: if $\alpha, \beta \in E$, then $\alpha + \beta \in E$.
(SF4) E is closed under multiplication: if $\alpha, \beta \in E$, then $\alpha\beta \in E$.
(SF5) E is closed under taking reciprocals (multiplicative inverses) of nonzero elements: if $\alpha \in E - \{0\}$, then $\alpha^{-1} \in E$.

Characteristic of a field: If it is possible to add up a finite positive number of 1's to get 0 in F, the minimum number of 1's needed to get 0 is the *characteristic* $\operatorname{char} F$ of the field. For example, $\operatorname{char} \mathbf{Z}_2 = 2$, $\operatorname{char} GF(4) = 2$, $\operatorname{char} \mathbf{Z}_5 = 5$. In general, $\operatorname{char} GF(p^k) = p$ for p prime.

If we cannot get 0 by adding up a finite positive number of 1's then we say $\operatorname{char} F = 0$. So $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{C}$ all have characteristic 0. (But there exist infinite fields with nonzero characteristic.)

Some results fail for fields of nonzero characteristic, or for fields of characteristic 2 in particular. Characteristic 2 is peculiar because in those fields addition is the same thing as subtraction.

Practice Problems

X2. Use the Subfield Theorem to show that $\mathbf{Q}(\sqrt{2})$ is a subfield of $\mathbf{R}$. (Hint: you should know how to rationalize a denominator.)

X3. Show that $\mathbf{Q}(i)$ is a subfield of $\mathbf{C}$.

X4. (a) Construct the addition and multiplication tables for $\mathbf{Z}_7$.
(b) Using these tables, write down a two-column table with α and $-\alpha$ for each $\alpha \in \mathbf{Z}_7$, and another two-column table with α and α^{-1} for $\alpha \in \mathbf{Z}_7 - \{0\}$.
(c) What are $4 - 6$ and $4 \div 3$ in $\mathbf{Z}_7$?

X5. We can define $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with addition and multiplication modulo n even if n is not a prime. But when n is not a prime, this is not a field.
(a) Construct the multiplication table for $\mathbf{Z}_6$, and use it to explain why $\mathbf{Z}_6$ is not a field.
(b) Generalize your answer to (a) to explain why $\mathbf{Z}_n$ is not a field when $n \geq 4$ is not prime.