2025/9/11
讲义习题1.1:1,3,5,6,9-12.

1.1.1

Suppose $x, y, z \in F$ and $z \neq 0$, and $xz = yz$, prove that $x = y$.
Proof:

$$x = x(zz^{-1}) = xz \cdot z^{-1} = yz \cdot z^{-1} = y.$$

1.1.3

Prove that for any $x \in F \backslash \{0\}$, $x^{-1} \neq 0$, and the mapping $\psi : F \backslash \{0\} \to F \backslash \{0\}, x \mapsto x^{-1}$ is a bijection such that $\psi^{-1} = \psi$.
Proof: Since $x^{-1} \cdot x = 1 \neq 0$, $x^{-1} \neq 0$. For any $y \in F \backslash \{0\}$, $\psi(y^{-1}) = y$ so ψ is surjective. If $\psi(x) = \psi(y)$ i.e. $x^{-1} = y^{-1}$ then multiply xy on both sides we obtain $x = y$, so ψ is injective. Hence ψ is a bijection.
Since $xx^{-1} = x^{-1}x = 1$, $(x^{-1})^{-1} = x$, therefore $\psi^{-1} = \psi$.

1.1.5

Prove that for any $x \in F \backslash \{0\}$, $(-x)^{-1} = -(x^{-1})$.
Proof:

$$\begin{aligned} 0 &= (-x) \cdot (x^{-1} + (-x^{-1})) = (-x) \cdot x^{-1} + (-x) \cdot (-x^{-1}), \\ 0 &= (x + (-x))x^{-1} = x \cdot x^{-1} + (-x)x^{-1} = 1 + (-x)x^{-1}. \end{aligned}$$

Therefore $1 = (-x) \cdot (-x)^{-1}$ i.e. $(-x)^{-1} = -(x^{-1})$.

1.1.6

Prove that for any $x, y \in F$, $(-x)y = x(-y) = -(xy)$, and $(-x)(-y) = xy$.
Proof: Note that $0 = (x + (-x))y = xy + (-x)y$ and $0 = x(y + (-y)) = xy + x(-y)$ so $(-x)y = x(-y) = -(xy)$. Apply it twice to obtain $(-x)(-y) = xy$.

1.1.9

For $x \in F$ and $n \in \mathbb{N}$, let $x^n = x \cdots x$. For $x \neq 0$ and $n \in N$, further define $x^0 = 1$, $x^{-n} = (x^{-1})n$. Prove that for any $x \in F \backslash \{0\}$ and $m, n \in \mathbb{Z}$,

$$x^m x^n = x^{m+n},\ (x^m)^n = x^{mn},\ (xy)^n = x^n y^n.$$

Proof: Note that $x^n x = x^{n+1}$ so by induction we know $x^m x^n = x^{m+n}$. Likewise by induction on n we infer $(x^m)^n = x^{mn}$, and $(xy)^n = x^n y^n$.

1.1.10

Prove that for any $n \in \mathbb{Z}$, $(-1)^{2n} = 1$, $(-1)^{2n+1} = -1$.
Proof: Note that from 1.1.6, $(-1) \cdot (-1) = 1$ and $1 \cdot (-1) = -1$, so by induction

$$(-1)^{2n} = 1,\ (-1)^{2n+1} = -1.$$

1.1.11

Let $\mathrm{char}(F) = p \neq 0$. Prove that $(x+y)^p = x^p + y^p, \forall x, y \in F$.
Proof: Since $+, \cdot$ are both communicative,

$$(x+y)^p = \sum_{k=0}^{p} x^k y^{p-k} \binom{p}{k} = x^p + y^p + \sum_{k=1}^{p-1} x^k y^{p-k} p \binom{p-1}{k-1} / k = x^p + y^p.$$

(It is well know that for any $1 \leqslant k \leqslant p-1, p \mid \binom{p}{k}$.)

1.1.12

Suppose F is a finite field, and $|F| = q$. Prove that for any $x \in F$, $x^q = x$.
Proof: Suppose $x \neq 0$, otherwise it is trivial. Consider the mapping $\varphi : F \to F,\ a \mapsto xa$, then for any $b \in F$, $\varphi(x^{-1}b) = b$ so φ is surjective. If $\varphi(a) = \varphi(b)$ then $xa = xb$ so $a = b$ (by $x \neq 0$), hence φ is a bijection. Therefore

$$\prod_{a \in F \backslash \{0\}} a = \prod_{a \in F \backslash \{0\}} xa = x^{q-1} \prod_{a \in F \backslash \{0\}} a \implies x^{q-1} = 1,$$

i.e. $x^q = x$.
Another proof: $F \backslash \{0\}$ is a multiplicative group of order $q-1$, so by Lagrange's theorem, the order of any element $x \in F \backslash \{0\}$ is a factor of $q-1$, hence $x^{q-1} = 1$.