1. Fields and polynomials

1.1. Basic properties of fields

- **Definition**: ring R is **field** if every element of $R - \{0\}$ has mutliplicative inverse and $1 \neq 0 \in R$.
- **Lemma**: every field is integral domain.
- **Definition**: field homomorphism is a ring homomorphism $\varphi : K \to L$ between fields:
  - $\varphi(a + b) = \varphi(a) + \varphi(b)$
  - $\varphi(ab) = \varphi(a)\varphi(b)$
  - $\varphi(1) = 1$

These imply $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$, $\varphi(a^{-1}) = \varphi(a)^{-1}$.

- **Lemma**: let $\varphi : K \to L$ homomorphism.
  - $\text{im}(\varphi) = \{\varphi(a) : a \in K\}$ is a field.
  - $\ker(\varphi) = \{a \in K : \varphi(a) = 0\} = \{0\}$, i.e. φ is injective.
- **Definition**: **subfield** K of field L is subring of L where K is a field. L is a **field extension** of K.
- The above lemma shows the image of $\varphi : K \to L$ is a subfield of L.
- **Lemma**: intersections of subfields are subfields.
- **Prime subfield** of L: intersection of all subfields of field L.
- **Definition**: **characteristic** $\text{char}(K)$ of field K is

  $$\text{char}(K) \coloneqq \min(\{0\} \cup \{n \in \mathbb{N} : \chi(n) = 0\})$$

  where $\chi : \mathbb{Z} \to K$, $\chi(m) = 1 + \cdots + 1$ (m times).
- **Example**: $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$, $\text{char}(\mathbb{F}_p) = p$ for p prime.
- **Lemma**: for any field K, $\text{char}(K)$ is either 0 or a prime.
- **Theorem**:
  - $\text{char}(K) = 0$ iff $\mathbb{Q}$ is the prime subfield of K.
  - $\text{char}(K) = p > 0$ iff $\mathbb{F}_p$ is the prime subfield of K.
- Note $p \mid \binom{p}{i}$ so $(a + b)^p = a^p + b^p$.