Lemma 1. If F is a field, then the charcteristic is 0 or p, a prime.

Theorem 2. If $\text{char}F = 0$, then there is a natural injection $\phi : \mathbb{Q} \to F$.

One ponders if we then get an isomorphism onto the field of the image!

Theorem 3. If $\text{char}F = p$, then there is a natural injection $\phi : \mathbb{Z}_p \to F$.

Lemma 4. If F is a field and F is finite, then $|F| = p^k$ for some prime p and some $k \geq 1$.

It will turn out that there is a field of order p^k for every prime p and every integer $k \geq 1$, which we denote $\mathbb{F}_{p^k}$.

Lemma 5. Let $\phi : R \to S$ be a ring homomorphism between rings R, S. Then $\ker\phi$ is an additive subgroup of R, and if $k \in \ker\phi$ then:

$$a \cdot k \in \ker\phi \text{ and } k \cdot a \in \ker\phi, \text{ for all } a \in R$$

Proof. (1) follows as ϕ is a group homomorphism with respect to addition, and so we can apply the first isomorphism theorem (or a simpler argument).

For (2), observe that $\phi(a \cdot k) = \phi(a) \cdot \phi(k) = \phi(a) \cdot 0_S = 0_S$. A symmetric argument follows for the other side. □

Definition (Ideal). Given a ring R, an **ideal** I of R is an additive subgroup of R that is closed under multiplication with all ring elements, i.e. it "absorbs" in the sense that for $i \in I$:

$$a \cdot i \in \ker\phi \text{ and } i \cdot a \in \ker\phi, \text{ for all } a \in R$$

Example: Suppose $R = \mathbb{Z}$. Then any subgroup of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for $m \geq 0$. These are all ideals!

Definition (Principal Ideal). Let R be a commutative ring, and let $a \in R$. Then the set $\{ar : r \in R\}$ is an ideal of R. It is the **principal ideal** generated by a.

Lemma 6. The principal ideal generated by a is an ideal.

Proof. We verify the principal ideal is an additive subgroup first. Consider two elements $ar, as \in aR$. Then:

$$ar - as = a(r - s) \in aR$$

So it is an additive subgroup. We verify now that is closed under outside multiplication. If $ar \in aR, s \in R$, then $ar \cdot s = asr \in aR$. □

Example: Let $R = \mathbb{Z}[x]$. Then the set $I \subseteq R$ consisting of all polynomials whose constant term is even is an ideal. This is obvious. We claim however it is not principal!

Why is this? Note that we have constant polynomials $2\mathbb{Z} \subseteq I \to a = 2$ or $a = -2$.

But if we consider $x \in I$ and $x \notin 2\mathbb{Z}[x]$.

Lemma 7. A commutative ring R is a field if and only if the only ideals are 0 and R itself.

Proof. We begin with the forward implicatin. Suppose R is a field, and suppose $I \subseteq R$ is an ideal, and $I \neq 0$.

If $I \neq 0$, then by definition $\exists a \neq 0, a \in I$. Then a^{-1} exists, and so $aa^{-1} = 1 \in I$. This clearly has that everything is in I.

For the reverse implication, take $a \in R, a \neq 0$. Consider the principal ideal generated by a, denoted aR. By assumption $aR = R$, so there is some b such that $ab = ba = 1$. So a is a unit. □

Recall some basic facts about quotient groups. Then when we have $N \subseteq G$ a normal subgroup, the elements of G/N are cosets of N.

Definition (Quotient Ring). Let R be a ring, $I \subseteq R$ an ideal. As a set, the quotient ring R/I is the ring of cosets of I in R.