Ex: We saw last time that

$$\mathbb{Z}_n^\times = U(n) = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\},$$

and that every non-zero element of $\mathbb{Z}_n$ which isn't a unit is a zero divisor. Thus

- For every prime p, $\mathbb{Z}_p$ is a field.
- For every composite n, $\mathbb{Z}_n$ is not an integral domain.

Observation: Every field is an integral domain.

Why? $F^\times = F \setminus \{0\}$, so every non-zero element is a unit, hence not a zero divisor.

The converse holds for finite rings.

Thm: Let R be a finite integral domain. Then R is a field.

Proof: We must show $R^\times = R \setminus \{0\}$.

Certainly, $R^\times \subseteq R \setminus \{0\}$. So take $a \in R \setminus \{0\}$.

Define the "multiply by a" map

$$f : R \to R$$
$$x \mapsto ax.$$

Since R is an integral domain and $a \neq 0$, we have

$$ax_1 = ax_2 \implies x_1 = x_2$$

for any $x_1, x_2 \in R$. So f is injective.

Since R is finite, f is also surjective.

Thus, $1 \in R$ is in the range of f. That is,

$$1 = f(b) = ab$$

for some $b \in R$. Thus, $b = a^{-1}$ and so $a \in R^\times$ is a unit. ∎

Subrings

Def: Let $R = (R, +, \cdot)$ be a ring. A subset $S \subseteq R$ is a subring if

- S is closed under $+$,
- S is closed under $\cdot$,
- $(S, +, \cdot)$ is also a ring.

Thm: Let R be a ring and $S \subseteq R$. Then S is a subring if and only if

- $(S,+)$ is a subgroup of $(R,+)$.
- S is closed under $\cdot$

Proof: This is just a restatement of the definition. $\blacksquare$

Ex: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Ex: For $n \in \mathbb{N}$, $n\mathbb{Z} \subseteq \mathbb{Z}$.

Ex: $\{n \times n \text{ upper triangular matrices}\} \subseteq M_n(\mathbb{R})$

Note: No special notation for subrings. We just use $\subseteq$.

Ring Homomorphisms

Def: Let R and S be rings. A <u>ring homomorphism</u> is a function $\varphi : R \to S$ such that

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$

for all $a, b \in R$.

If φ is a bijective ring homomorphism, then we call it an <u>isomorphism</u> and write $R \cong S$.

Def: Let $\varphi : R \to S$ be a ring homomorphism. The *image* of φ is

$$\varphi(R) = \{ \varphi(r) \mid r \in R \} \subseteq S$$

and the *kernel* of φ is

$$\ker \varphi = \{ r \in R \mid \varphi(r) = 0 \} \subseteq R.$$

Note: These are just the image and kernel of φ considered as a *group* homomorphism $(R,+) \to (S,+)$.

Thm: Let $\varphi: R \to S$ be a ring homomorphism. Then

① $\varphi(R)$ is a subring of S.

② $\ker \varphi$ is a subring of R.

③ For all $a \in \ker \varphi$ and $r \in R$, we have $ra \in \ker \varphi$ and $ar \in \ker \varphi$.

Proof: Next time.

Def: Let R be a ring. An <u>ideal</u> in R is a subring $I \subseteq R$ such that for all $a \in I$, $r \in R$, we have $ra \in I$ and $ar \in I$.

So kernels are ideals!