2.3 Rings, fields, characteristic

We have seen that a unit of a ring is an element with multiplicative inverse in R, and we have seen that there can be "very few" units (for instance, $U(\mathbb{Z}) = \{\pm 1\}$) or many of them (for instance $U(\mathbb{R}) = \mathbb{R}\setminus\{0\}$). When all non-zero elements of the ring have multiplicative inverse then the ring has a special name.

Definition (Division ring, field)

- Let R be a ring. If every nonzero element of R is a unit then R is a division ring.
- We call field a commutative division ring.

Example

- $(\mathbb{R},+,\cdot)$ is a field. So are $(\mathbb{Q},+,\cdot)$ and $(\mathbb{C},+,\cdot)$
- $(\mathbb{Z}_{12},+,\cdot)$ is not a field (we have seen that $U(\mathbb{Z}_{12}) = \{1,5,7,11\} \neq \mathbb{Z}_{12}\setminus\{0\}$.
- Consider $\mathbb{Z}_5 = \{0,1,2,3,4\}$. Here

$$2\cdot 3 = 1, \text{ and}$$
$$4^2 = 1.$$

So $U(\mathbb{Z}_5) = \{1,2,3,4\}$ and therefore $(\mathbb{Z}_5,+,\cdot)$ is a field.

- $(\mathbb{Z},+,\cdot)$ is not a field.

Remark Note that the definition of field is equivalent to:
$(R,+,\cdot)$ is a field if $(R,+,\cdot)$ is a commutative ring & $(R\setminus\{0\},\cdot)$ is a group.

If every non-zero element has a multiplicative inverse then the ring has no zero divisors:
Call F our field, then if $a,b \in F$ with $a \neq 0$ and $ab = 0$:

$$ab = 0 \xrightarrow{\text{multiply both sides by } a^{-1}} a^{-1}ab = a^{-1}\cdot 0 \Leftrightarrow 1\cdot b = 0, \text{ that is } b = 0.$$

We have just proved

Thm(A) Every field F is an integral domain.

The converse to this is not -in general- true. For instance, $\mathbb{Z}$ is an integral domain which is not a field.
When the ring (field) is finite it is true:

Thm(B) Every finite integral domain is a field.

We have seen that the finite ring $\mathbb{Z}_{12}$ has various zero divisors. Therefore it is not an integral domain and not a field.
The zero divisors in $\mathbb{Z}_{12}$ are $2,3,4,6,8,9,10$. These are precisely the integers mod 12 which are not coprime with 12.
In fact, this holds in general in the rings $\mathbb{Z}_n$.

Thm The zero divisors in $\mathbb{Z}_n$ are $\{m \in \mathbb{Z}_n : \gcd(m,n) \neq 1\}$

Recall that this means: integers between 1 and $n-1$ with some common divisor with n (greater than 1).

If $d = \gcd(m,n) \neq 1$ then $m \cdot \left(\frac{n}{d}\right) = \left(\frac{m}{d}\right) \cdot n$ (this is a multiple of n, so it's zero in $\mathbb{Z}_n$)

So m is a zero divisor if $\gcd(m,n) \neq 1$.

[The other direction follows from: suppose $m \in \mathbb{Z}_n$ with $\gcd(m,n)=1$ and suppose $m \cdot s = 0$ for some $s \in \mathbb{Z}_n$. Then n divides ms. But n and m are coprime, so n must divide s. So $s = 0 \in \mathbb{Z}_n$]

This tells us that whenever n is a composite (i.e. non-prime numbers >1) number, $\mathbb{Z}_n$ is not an integral domain.

On the other hand:

Thm(C) • If p is a prime then $\mathbb{Z}_p$ has no zero divisors. (follows from thm (B))
• If p is a prime then $\mathbb{Z}_p$ is a field (follows from thm(B) + (A)).

The integer n in $\mathbb{Z}_n$ has the property that $n \cdot a = 0$ for all $a \in \mathbb{Z}_n$.

Definition (Characteristic of a Ring)

• If for a ring R there exists a positive integer n such that $n \cdot a = 0 \ \forall a \in R$ then the least positive integer with this property is called the characteristic of the ring R.
(↑ we know this exists..)

• If no such positive integer exists, then we say that the ring has characteristic 0.

Examples • $\mathbb{Z}_n$ has characteristic n
• $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic 0.

We will mostly talk about characteristic of a field.

Luckily, there is a very easy way to test what the characteristic of a ring (or field) is.

Criterion A ring R has positive characteristic if and only if there is a least positive integer n such that $n \cdot 1 = 0$.

Our considerations on $\mathbb{Z}_p$ give us a way to prove a result from number theory.

Fermat's little theorem If $a \in \mathbb{Z}$ and p is a prime not dividing a. Then $a^{p-1} \equiv 1 \pmod p$.

Also, $a^p \equiv a \pmod p$ for all $a \in \mathbb{Z}$ and any prime p.

The key is to use Lagrange's thm for finite groups (i.e. if $H \leq G$ then the order of H divides $|G|$)

The second statement in thm(C) above tells us that $(\mathbb{Z}_p^*, \cdot)$ is a group of order $p-1$.

If we take any $a \in \mathbb{Z}_p^*$ then $\langle a \rangle = \{1, a, \ldots a^{\text{ord}(a)}\}$ is a finite cyclic subgroup of order $\text{ord}(a)$. By lagrange's thm, $\text{ord}(a)$ divides $p-1$ and therefore $a^{p-1} \equiv 1 \pmod p$.

We shall see that a generalisation of this thm holds.