§1 11-08

Proposition 1.1 (16.15)
For commutative ring with unity:

D is an integral domain $\Leftrightarrow$ for all nonzero $a \in D$, $ab = ac \Leftrightarrow b = c$

Theorem 1.2 (16.16)
Finite integral domain $\Rightarrow$ field.

Let $a \in D^* = D \setminus \{0\}$

Then $\varphi : D^* \to D^*$ where $\varphi(x) = ax$ for all $x \in D^*$.

φ is injective because $\varphi(x_1) = \varphi(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$

φ is surjective because $|D^*| < \infty$

Thus, $1 = \varphi(x)$ for some $x \in D^*$. Hence $ax = 1$ for some x, so a^{-1} exists.

Definition 1.3. The [Characteristic] of R is the smallest n such that $nr = 0$ for all $r \in R$. If there isn't such a smalest n, we say that R has characteristic 0.

Example 1.4
$\mathbb{Z}_n$ has characteristic n.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic 0.

$\mathbb{F}_4$ has characteristic 2.

$$\mathbb{F}_4 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

Lemma 1.5
If R is a ring with unity, then $\text{char}(R)$ equals the smallest n such that $n_1 = 0$. i.e. the order of 1 is $(R, +)$.

"It is enough to find the additive order of the multiplicative identity element".

Proof.

$$nr = \underbrace{r + r + \cdots + r}_{n}$$

Let n denote n_1 for a ring with unity.

$$nr = (n1)r = 0r = 0$$

holds for all r! n is minimal with this property because $n = |1|$ in $(\mathbb{R}, +)$. □

Theorem 1.6

The characteristic of an integral domain is either 0 or p prime.

Proof. Suppose $\text{char}(R)$ is $m = ab$ with $1 < a, b < m$.

Then $a1, b1 \neq 0$. But $(a1)(b1) = ab1 = m1 = 0$. Contradiction because this contradicts integral domain.

$$(n_1 r_1)(n_2 r_2) = n_1 n_2 (r_1 r_2)$$

□

§1.1 Ring Homomorphisms Ideals

A ring homomorphism $\varphi : R \to S$ satisfies:

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

A bijective ring homomorphism is an isomorphism.

Example 1.7

$\varphi : \mathbb{Z} \to \mathbb{Z}_n$. $\varphi(a) = a \mod (n)$ is a homomorphism.

Proposition 1.8

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

1. $\varphi(R)$ is a subring of S.
2. If R is commutative, then $\varphi(R)$ is commutative.
3. $\varphi(0) = 0$
4. If R and S are rings with unity 1_R and 1_S and φ is surjective, then $\phi(1_R) = 1_S$
5. If R is a field, then either $\varphi(R) = 0$ or $\varphi(R)$ is a field.

Proof.

3. $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$ so $\varphi(0_R) = 0_S$
1. $0_S \in \varphi(R)$.

   $a, b \in \varphi(R) \Rightarrow a - b \in \varphi(R)$ because $a = \varphi(a')$ and $b = \varphi(b')$ for some $a', b' \in R$ so $a - b = \varphi(a') - \varphi(b') = \varphi(a' - b') \in \varphi(R)$

   Likewise, $ab = \varphi(a')\varphi(b') = \varphi(a'b') \in \varphi(R)$.
2. If $a'b' = b'a'$, then:

$$ab = \varphi(a')\varphi(b') = \varphi(a'b') = \varphi(b'a') = \varphi(b')\varphi(a') = ba$$

4. Let $x \in R$ such that $\varphi(x) = 1_S$. Then $1_S = \varphi(x) = \varphi(1_R x) = \varphi(1_R)\varphi(x) = \varphi(1_R)(1_S) = \varphi(1_R)$

□