PRIME RINGS

Given a ring R, the ring homomorphism $\chi_R : \mathbb{Z} \to R$, $n \mapsto n 1_R$

$\operatorname{Ker} \chi_R = \mathbb{Z}n$, $n \in \mathbb{N}$ and n is unique. n = order of 1 in $(R, +)$.
~~Also~~ $n = \operatorname{char}(R)$.

Examples: (i) $\operatorname{char}(\mathbb{Z}) = 0$, (ii) $\operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{C}) = 0$, (iii) $\operatorname{char}(\mathbb{Z}_m) = m$, (iv) for any ordered field K, $\operatorname{char}(K) = 0$.

For ~~If~~ $\chi_R : \mathbb{Z} \to K$ (K is a field), if $\operatorname{Ker} \chi_R = 0$ then χ_R is injective $\Rightarrow \operatorname{char}(K) = 0$. Also, $\operatorname{char}(K) = 0 \Rightarrow \chi_R$ is injective. Since $\mathbb{Q}$ is the smallest field containing $\mathbb{Z}$, every field K whose $\operatorname{char}(K) = 0$, contains $\mathbb{Q}$.

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\chi_{\mathbb{Q}}", "\text{injective}"'] \arrow[d, "\chi_K"', "\text{injective}"] & \mathbb{Q} \arrow[dl, "\text{injective}"] \\
K &
\end{tikzcd}$$

16.1 Lemma: If R is an integral domain, then $\operatorname{char} R = 0$ or $p \in \mathbb{P}$.

Proof: Suppose $\operatorname{char} R \neq 0$, say it is n. Then $\operatorname{Ker} \chi_R = \mathbb{Z}n$. If $n \notin \mathbb{P}$, then $n = a, b$ $a, b \in \mathbb{N}^*$, $1 < a, b < n \Rightarrow (a \cdot b) \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R) = 0$
$\Rightarrow$ either $(a \cdot 1_R) = 0$ or $(b \cdot 1_R) = 0$ which is a contradiction because R is an integral domain, ~~and~~ and n is the smallest integer such that $n \cdot 1_R = 0$.

Prime ring: Let R be a ring. The smallest subring of R is called the prime ring of R. Prime ring of R is also the prime ring of any of its subring.

In other words, a ring R is called a prime ring if ~~its~~ it is a prime ring for itself. Examples:
(i) $\mathbb{Z} = \mathbb{Z}$ (ii) PR of $\mathbb{Q} = \mathbb{Z}$, (iii) PR of $\mathbb{Z}_n = \mathbb{Z}_n$.
$\mathbb{Z}$, $\mathbb{Z}_n$ are prime rings, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ are not prime rings.

16.1 Theorem: Let A be a prime ring of characteristic $n \in \mathbb{N}$.

1) m is +ve: Then $|A| = m$ and
$$A = \{n 1_A \mid 0 \leq n < m\}$$
$$r \cdot 1_A = s \cdot 1_A \cancel{\Rightarrow (r = s)}$$
$$\Longrightarrow r \equiv s \pmod{m} \quad \forall\, r, s \in \mathbb{Z}$$
$\forall\, r \in \mathbb{Z}$, $r \cdot 1_A$ is a non-zero divisor in A
$$\Longleftrightarrow r \cdot 1_A \in A^\times \Longleftrightarrow \gcd(r, m) = 1$$

2) $m = 0$: Then $A = \{n \cdot 1_A \mid n \in \mathbb{Z}\}$

$a \cdot 1_A \neq b \cdot 1_A \Rightarrow a \neq b$, Also A is an integral domain, and $A^\times = \{\pm 1_A\}$.

Corollary 1: Let A be a prime ring of Char $m > 0$. Then the following are equivalent.
(a) A is a field, (b) A is an integral domain, (c) m is prime.

Corollary 2. If A is a prime ring with char $m > 0$, then $\operatorname{ord} A^\times = \phi(m)$

Corollary 3. Let $m \in \mathbb{N}$, $m \neq 0$, $r \in \mathbb{Z}$, $\gcd(r, m) = 1$, then
$$r^{\phi(m)} \equiv 1 \pmod{m}$$ (Also called Euler's theorem).

Corollary 4: Fermat's little theorem: Let $r \in \mathbb{Z}$, $p \in \mathbb{P}$ with $p \nmid r \Rightarrow$
$$r^{p-1} \equiv 1 \bmod (p).$$

Proof: ~~Taken the set~~ Take $m = p$ in Corollary 3.

Another proof: ETPT $r^p \equiv r \pmod{p}$. Consider any prime ring A with characteristic p. ETPT $a^p = a$, $\forall\, a \in A$, $a \neq 0$. Since $a \in A$, $a = s \cdot 1_A \Rightarrow a^p = (s \cdot 1_A)^p = (1_A + 1_A + \dots 1_A)^p$. Using binomial expansion and $p \cdot 1_A = 0$, show that $a^p = s \cdot 1_A = a$. Thus proved

Generally, If R is a Ring, $a, b \in R$, char $R = p$, $p \in \mathbb{P}$, $n \in \mathbb{N}^*$, then $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ ~~pro~~.

If K is a field, and char $K = 0 \Rightarrow \mathbb{Q} \subseteq K$.
If char $K > 0 \Rightarrow$ char K is prime. ~~$\mathbb{Z}$~~
Also K contains $\mathbb{Z}_p$. (prime ring of K). $\mathbb{Z}_p$ is also a field.
Therefore $\mathbb{Q}$, and $\mathbb{Z}_p$, $p \in \mathbb{P}$ are the only prime fields.

Modules & Algebras

17/1.

Module: Let R be a ring. V is a R-module if
(a) $(V, +)$ is a abelian group
(b) There is a scalar multiplication of R on V such that: $R \times V \longrightarrow V$
$$(a, x) \longrightarrow ax$$
(c) The scalar multiplication has the following properties
(i) $a(bx) = (ab)x$ (associative)
(ii) $(a+b)x = ax + bx$ (distributive)
(iii) $a(x+y) = a.x + b.y$
(iv) $1.x = x$

Examples: 1. An ring ~~is~~ R is an R-module.
2. An ideal A in R is a R-module.
3. V is any R-module, I any set
$$V^I = \{f : I \longrightarrow V\}, \quad I \text{ tuples in } V.$$
Show that this is a R-module, with the operations $(f+g)(i) = f(i) + g(i)$, $(af)(i) = a f(i)$, $f, g \in V^I$, $a \in R$.
Verify that $V^{(I)}$ is also a module (a sub-module of V^I).

~~R is a submodule of a V module V, if $R \subseteq V$~~