Characteristics of Rings.

If R is a ring, a positive integer n is called the characteristic of the ring R, if

$$nx = \underbrace{x + x + \cdots + x}_{n \text{ times}} = 0$$

$\forall x \in R$, and n is the smallest positive integer with this property.

If there is no such n, then we say the ring has characteristic 0.

Examples:

- $R = \mathbb{Z}_6 \times \mathbb{Z}_9$

$$n(a,b) = (0,0)$$
$$\Leftrightarrow na = 0 \text{ and } nb = 0$$
$$\Leftrightarrow n \text{ is a mult. of 6 and a multiple of 9.}$$

The LCM is the least such n, so

$$\boxed{n = 18}$$

- Lemma If R is an integral domain, then the characteristic $\text{char}(R)$ is either 0 or a prime number.

Proof: Suppose $n = ab \neq 0$ is the characteristic of R. for $a, b \in \mathbb{N}$. Then $n1 = ab1 = (a1)(b1) = 0$

$$(\underbrace{1+1+\cdots}_{a})(\underbrace{1+1\cdots 1}_{b})$$

$\Rightarrow a|=0$ or $b|=0$. Since n is minimal, one of a, b is n, the other is 1.

$\therefore$ char (R) is either prime or 0. ☑

• **Lemma:** If $\text{char}(R) \neq 0$ and R is a ring with 1, i.e. n

Then n is the least positive integer such that $n1=0$.

Proof: $\forall x \in R,\ x = 1x$

$nx = n|x = (n1)x = 0 \ \forall x \in R$

$\Leftrightarrow n|=0$. ☑

Multiple zeros of polynomials

zeros with multiplicity.

If $f(x) = (x-a)^k g(x)$, where $g(a) \neq 0$,

then k is called the multiplicity of the zero a.

From "calculus": we define for $f(x) \in F[x]$ (↑ field.)

if $f(x) = a_0 + a_1 x + \dots + a_k x^k$ with $k \in \mathbb{N} \cup \{0\}$,

we define $f'(x) = a_1 + 2a_2 x^1 + \dots + k a_k x^{k-1}$

or $f'(x) = 0$ if $k=0$

Note: the product rule works on polynomials.

k \in \mathbb{N}

Proposition. A polynomial $f(x) \in F[x]$ has a zero of multiplicity > 1 in some extension field E $\iff$ $\gcd(f(x), f'(x))$ is nonconstant.

Pf: Suppose $f(x) = (x-a)^k g(x)$ for some $k \geq 2$. $g(x) \in E[x]$.

Then $f'(x) = k(x-a)^{k-1} g(x) + (x-a)^k g'(x)$

$= (x-a)\left[k(x-a)^{k-2} g(x) + (x-a)^{k-1} g'(x)\right]$

$\therefore (x-a)$ is a common factor of $f(x)$ & $f'(x)$ in $E[x]$. ✓

$\therefore \gcd(f'(x), f(x))$ is nonconstant. ✓

Suppose $\gcd(f(x), f'(x))$ is nonconstant, so that it contains a linear factor $(x-c)$ in some $E[x]$ for an extension field E.

$\therefore$ c is a zero of both $f(x)$ & $f'(x)$ in E.

$\Rightarrow$ $f(x) = (x-c)\, g(x)$ for some $g(x) \in E[x]$.

Take derivative $f'(x) = g(x) + (x-c)\, g'(x)$

Plug in $x = c$ $f'(c) = g(c) + 0$

0 $\Rightarrow g(c) = 0 \iff$ $g(x)$ has $(x-c)$ factor.

$\Rightarrow$ $f(x) = (x-c)^2 \left(\tilde{g}(x)\right)$ for some $\tilde{g}(x) \in E[x]$. ✓ ☒

Cor (induction on above)

$\gcd(f(x), f'(x))$ has a zero of multiplicity k in Ext field $\iff$ $f(x)$ has a zero of mult $k+1$ in the extension field.

Thm Suppose $f(x)$ is irreducible over F.

If F has characteristic 0, then $f(x)$ has no multiple zeros.

If F has characteristic p, then $f(x)$ has a multiple zero only if $f(x)=g(x^p)$ for some $g(x) \in F[x]$.

Proof: Suppose $f(x)$ has a multiple zero c

Let $f(x) = a_0 + a_1 x + \cdots + a_k x^k$.

Then $f'(x) = a_1 + 2a_2 x + \cdots + k a_k x^{k-1}$

Plugging in $c \Rightarrow$ $a_0 + a_1 c + \cdots + a_k c^k$

and $a_1 + 2a_2 c + \cdots + k a_k c^{k-1} = 0$

$\hookrightarrow$ c is a root of $f'(x) \in F[x]$ lower degree.

But $f(x)$ is irred with root c

$\Rightarrow f(x)$ is m.

$\Rightarrow$ $j a_j = 0$ for $1 \le j \le k$

If $\text{char}(F) = 0 \Rightarrow a_j = 0$ for $1 \le j \le k$.

But that would mean $f(x)$ is a constant. ~~$\times$~~

$\therefore \text{char}(F) \neq 0$.

If $\text{char}(F) = p$, $a_j = 0$ when $p \nmid j$

$\Leftrightarrow f(x) = g(x^p)$

$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots a_{sp} x^{sp}$

Sp. $j a_j = 0$, $(j,p)=1$, $p a_j = 0$

$\Rightarrow$ (Bezout) $\exists\, r, s \in \mathbb{Z}$ s.t. $(rj + sp) = 1$

$\Rightarrow r j a_j + s p a_j = 1 a_j = 0$