21/11

Irreducibility Criteria

Let R be an integral domain

① A polynomial $f(x) \in R[x]$ of degree 2 or 3 is reducible iff f has a factor of degree 1.

In particular, when R is a field, then a quadratic or a cubic polynomial is reducible $\Leftrightarrow f(x)$ has a root in R

② Suppose that R is an integral domain and $I \trianglelefteq R$. If $f(x) \in R[x]$ is reducible, then so is $\bar{f}(x)$ in $R/I[x]$

$$f(x) = a_0 + a_1 x + \cdots\cdots + a_n x^n$$
$$\tilde{f}(x) = (a_0 + I) + (a_1 + I)x + \cdots + (a_n + I)x^n$$

If $f(x) = g(x)h(x)$

$\Rightarrow \tilde{f}(x) = \tilde{g}(x)\tilde{h}(x)$

$x^2 + x + 1 \in \mathbb{Z}[x]$ is irreducible! (use previous property)

$x^2 + 1 \in \mathbb{Z}[x]$ is irreducible

Eisenstein's Criteria

Let R be an integral domain, P is a prime ideal of R.

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x]$

Suppose

① $a_0, \ldots, a_{n-1} \in P$

② $a_0 \notin P^2$

Then f is irreducible

suppose

$$f(x) = a_0 + a_1 x + \dots + a_n x^n$$
$$\bar{f}(x) = \bar{a_0} + \bar{a_1} x + \dots + \bar{a_n} x^n$$

$$\Rightarrow \bar{f}(x) = \bar{a_n} x^n$$

$$f(x) = g(x) h(x)$$
$$\Rightarrow \bar{f}(x) = \bar{g}(x) \tilde{h}(x)$$

[can't really comment about factorization]

$$g(x) = c_0 + c_1 x + \dots + c_r x^r$$
$$h(x) = d_0 + d_1 x + \dots + d_s x^s$$

$$g(x) h(x) = c_0 d_0 + (c_1 d_0 + c_0 d_1) x + \dots$$

Suppose $d_0 \notin P$

$\Rightarrow c_0 \in P$

$\Rightarrow c_1 d_0 \in P$

$\Rightarrow c_1 \in P$

$\Rightarrow c_0, c_1, \dots, c_r \in P$

$\Rightarrow$ Then $d_0 \in P$, $c_0 \in P$ $(\Rightarrow \Leftarrow)$

$a_0 = c_0 d_0 \in P^2$

① p^{th} – cyclotomic polynomial

$$\phi_p(x) = x^{p-1} + x^{p-2} + \dots + 1$$

(*) $\phi_p(x)$ is reducible $\Leftrightarrow$ $\phi_p(x+1)$ is irreducible

$$\phi_p(x) = \frac{x^p - 1}{x - 1}$$

$$\phi_p(x+1) = \frac{(x+1)^p - 1}{x}$$

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \dots + p$$

$p \mid \binom{p}{r}$ for all $r \leq p-1$, but $p^2 \nmid p$

$\Rightarrow \phi_p(x+1)$ is irreducible! [Eisenstein Criteria]

② Determinants

Let $A = \begin{bmatrix} x & y \\ w & z \end{bmatrix}$

$f(x, y, w, z) = \det A = xz - wy$ ← irreducible

$F(x, y, w, z) = F(y, z, w)[x]$

$f(x, y, w, z)$ is a linear polynomial in x

$F(y, z, w)/(w) = F(y, z)$

since $wy \in (w)$, $wy \notin (w^2)$

characteristic of a ring

Let R be a ring with 1

There is a natural homomorphism

$$\phi : \mathbb{Z} \to R$$
$$1 \to 1$$

Then $\ker(\phi) \trianglelefteq \mathbb{Z}$

$\Rightarrow$ There exists $m \in \mathbb{Z}_{>0}$ such that $\ker(\phi) = m\mathbb{Z}$

The number m is called the characteristic of R and is denoted by char R.

If char $R = m$, by First isomorphism theorem R contains an isomorphisc copy of $\mathbb{Z}/m\mathbb{Z}$

$\boxed{m = 0 \Rightarrow \text{copy of } \mathbb{Z}}$

If R is an integral domain and $m > 0$, then $\mathbb{Z}/m\mathbb{Z}$ is an integral domain

$\Rightarrow$ m is prime !