

1 Reducible/Irreducible polynomial

1.1 Reducible

$f(x)$ can be written as a product of two polynomials in $\mathbb{F}[x]$ both of positive degree.

1.2 Irreducible

otherwise

1.3 Example in $\mathbb{R}[x]$

$x^2 - a$ is reducible. but $x^2 + 1$ is irreducible but reducible over $\mathbb{C}[x]$.

2 Conjugate Roots Theorem

Let $f(x) \in \mathbb{C}[x]$ have all coefficients real. If $c \in \mathbb{C}$ is a root of $f(x)$ then so is \bar{c} (complex conjugate).

3 Example

Let $f(x) = x^4 + 3x^2 + 5x + 4$ in \mathbb{Z}_7 . Write table to find all roots.

x	0	1	2	3	4	5	6
f(x)	4	6	0	1	6	1	3

so $x=2$ is the only root of $f(x)$. Thus $(x-2)$ is a factor.

Apply DAP over \mathbb{Z}_7 divide $f(x)$ by $(x-2)$

Answer $h(x) = x^3 + 2x^2 + 5$

Key Point If α is a root of $h(x)$ then by FT and TD α is a root of $f(x)$.

2 is a root of $h(x)$ so $h(2)=0$

divide by $(x-2)$ to get $k(x) = x^2 + 4x + 1$

Check root of $k(x)$ to be root of $f(x)$. $k(2) = 2 \neq 0$

Thus $k(x)$ has no roots over \mathbb{Z}_7

hence $k(x)$ is irreducible over \mathbb{Z}_7 **Conclusion** $f(x) = (x-2)^2(x^2 + 4x + 1)$.

4 Proof of CPN

Restate CPN: Let $f(x) \in \mathbb{C}[x]$ of degree n . Then $\exists n$ complex roots not necessarily distinct.