

§23 Factorization of polynomials over a field

F : field (= commutative ring with mult. ident.

$a \in F, a \neq 0 \Rightarrow \exists$ multiplicative inverse $a^{-1} \in F$)

$\leadsto$ ring of polynomials with coeff. in F , $F[X]$,

behaves much like $\mathbb{Z}$: analogue of prime factoriz.

Ex. $F = \mathbb{C}$ any polynom $f(x) \in \mathbb{C}[X]$ has a factorization

$$f(X) = c \cdot (X - \alpha_1) \cdots (X - \alpha_n) \quad c, \alpha_i \in \mathbb{C}$$

$F = \mathbb{R}$ similar factorization

$$f(X) = c \cdot (X - \alpha_1) \cdots (X - \alpha_n) (X^2 + \beta_1 X + \gamma_1) \cdots (X^2 + \beta_m X + \gamma_m)$$

$$\alpha_i, \beta_j, \gamma_j \in \mathbb{R}, \quad \beta_j^2 < 4\gamma_j$$

Thm 23.1 (Euclidean division for polynomials)

Given $f(X), g(X) \in F[X]$, $\deg g(X) > 1$ we can find unique solutions

for the eq. $f(X) = g(X)q(X) + r(X)$ subj. to $\begin{cases} r(X) = 0 \text{ or} \\ \deg r(X) < \deg g(X) \end{cases}$

"quotient" "remainder"

Proof for existence

idea: $q_s(X)$ will be the minimizing choice for
 $(\deg 0 = -\infty) \quad \deg(f(X) - g(X)s(X)) \quad s(X) \in F[X]$

Case 1 $\min(\deg(\text{above})) = -\infty$

take $q_s(X)$ for such $s(X)$ then $r(X) = 0$

Case 2 $k = \min(\deg(\text{above})) > -\infty$

take $q_s(X) = s(X)$ ~~that~~ ~~that~~ that gives k

$$r(X) = f(X) - g(X)q_s(X)$$

We need to show $k = \deg r(X) < \deg g(X)$

We argue by proof by contradiction

(assume $k \geq \deg g(X)$ and derive a contradiction)

write $g(X) = b_0 + b_1 X + \dots + b_m X^m$ $m = \deg g(X)$

$$r(X) = c_0 + c_1 X + \dots + c_k X^k$$

(so $b_m \neq 0 \neq c_k$)

Put $s(X) = q(X) + \frac{c_k}{b_m} X^{k-m}$ $\leftarrow$ used that F is a field

$$\leadsto g(X)s(X) = g(X)q(X) + c_k X^k + \text{lower ord. terms}$$

$$\leadsto f(X) - g(X)s(X) = \underbrace{r(X) - c_k X^k - \text{lower ord. terms}}_{\text{order at most } k-1}$$

$\leadsto$ contradicts the minimality of $\deg(f(X) - g(X)q(X))$

Proof for uniqueness

$$g(X)q_1(X) + r_1(X) = f(X) = g(X)q_2(X) + r_2(X)$$

$$\leadsto g(X)(q_1(X) - q_2(X)) = \underbrace{r_2(X) - r_1(X)}_{\text{deg. smaller than } g(X)}$$

$$\leadsto q_1(X) - q_2(X) \text{ must be } 0 \quad \text{i.e. } q_1(X) = q_2(X)$$

$$\leadsto r_1(X) - r_2(X) \text{ must be } 0 \quad \text{i.e. } r_1(X) = r_2(X) \quad \square$$

Cor. $a \in F$ is a root (zero) of $f(X) \in F[X]$

$$\Leftrightarrow f(X) = (X - a)q(X) \quad \text{for some } q(X) \in F[X]$$

$$\therefore f(X) = (X - a)q(X) + c \quad c \in F \text{ by Thm.}$$

$$c = f(a) \quad \text{from } (a - a) \cdot q(a) = 0 \cdot q(a) = 0 \quad \square$$

Cor. if $a_1, \dots, a_k \in F$ are different roots of $f(X) \in F[X]$
then $k \leq \deg f(X)$

$$\therefore \text{by induction } f(X) = (X - a_1) \cdots (X - a_k) q_k(X) \\ \text{for some } q_k(X) \in F[X] \quad \square$$

[Cor. Write $F^\times = \{a \in F \mid a \neq 0\}$ group with multiplication
If $G \subset F^\times$ is a finite subgroup, then G is cyclic: $\exists b \in G$ s.t. $G = \{b^n \mid n \in \mathbb{Z}\}$

Def. $f(x) \in F[x]$ is irreducible ^{over F} if $\deg f(x) > 0$
 and there are no solutions to $f(x) = g(x)h(x)$
 $\deg g(x), \deg h(x) > 0$

Ex. $f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$
 but not irred. over $\mathbb{R}$ $f(x) = (x + \sqrt{2})(x - \sqrt{2})$

$f(x) = x^2 + 1$ is irred. over $\mathbb{R}$, not over $\mathbb{C}$

Rem this is an analogue of prime numbers in $\mathbb{Z}$

Ex. $f(x) = x^{n-1} + x^{n-2} + \dots + 1 = \frac{x^n - 1}{x - 1}$ for prime n

is irreducible over $\mathbb{Q}$ (the n -th cyclotomic polynomial)

$f(x) = \prod_{\substack{\zeta: \text{prim. } n\text{-th} \\ \text{root of 1}}} (x - \zeta)$ for gen. n

Other facts about $F[x]$

- If $p(x)$ is irred. over F and divides $r(x) \cdot s(x)$, then $p(x)$ divides $r(x)$ or $s(x)$
- General $f(x)$ ~~is~~ can be factored as

$$f(x) = p_1(x) \cdots p_k(x)$$
 $p_i(x)$: irred. over F
 unique up to reordering & scalar multiplication

1947

1. The first part of the report is a general survey of the situation in the country. It is a very interesting and informative study of the country's development.

2. The second part of the report is a detailed study of the country's economic situation. It is a very thorough and comprehensive study of the country's economic development.

3. The third part of the report is a detailed study of the country's social situation. It is a very thorough and comprehensive study of the country's social development.

4. The fourth part of the report is a detailed study of the country's political situation. It is a very thorough and comprehensive study of the country's political development.

5. The fifth part of the report is a detailed study of the country's cultural situation. It is a very thorough and comprehensive study of the country's cultural development.

6. The sixth part of the report is a detailed study of the country's environmental situation. It is a very thorough and comprehensive study of the country's environmental development.

7. The seventh part of the report is a detailed study of the country's international situation. It is a very thorough and comprehensive study of the country's international development.

8. The eighth part of the report is a detailed study of the country's future development. It is a very thorough and comprehensive study of the country's future development.

9. The ninth part of the report is a detailed study of the country's present development. It is a very thorough and comprehensive study of the country's present development.

10. The tenth part of the report is a detailed study of the country's past development. It is a very thorough and comprehensive study of the country's past development.

11. The eleventh part of the report is a detailed study of the country's future development. It is a very thorough and comprehensive study of the country's future development.

12. The twelfth part of the report is a detailed study of the country's present development. It is a very thorough and comprehensive study of the country's present development.