Week 13

Rings of Polynomials

Defn. Let R be a ring. A polynomial $f(x)$ with coefficients in R is an infinite formal sum $\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$, where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of i.
a_i : coefficients of $f(x)$.

$(*)$ If there exists an $i \geq 0$ such that $a_i \neq 0$, the largest value of i is the degree of $f(x)$. On the other hand, if $a_i = 0$ for all i, then $f(x)$ is a zero polynomial, its degree is defined to be "$-\infty$". (Or "undefined" in some textbook.)

$(*)$ A polynomial $f(x) = a_0 + a_1 x + \cdots$ with $a_i = 0$ for each $i \geq 1$ is called a constant polynomial.

Defn. The set of all polynomials with coefficients in R is denoted by $R[x]$. (The idea of using x as an "indeterminate" x was invented by René Descartes (1596-1650).)

Theorem The set $R[x]$ with addition and multiplication defined below is a ring provided that R is a ring. Moreover, if R is a commutative ring, then $R[x]$ is also a commutative ring.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$
$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n + \cdots$$

(Addition) $f(x)+g(x)=\sum_{i=0}^{\infty}c_ix^i$ where $c_i=a_i+b_i$.

(Multiplication) $f(x)g(x)=\sum_{i=0}^{\infty}d_ix^i$ where $d_m=\sum_{j=0}^{m}a_jb_{m-j}$.

Proof. $[(\sum_{i=0}^{\infty}a_ix^i)(\sum_{j=0}^{\infty}b_jx^j)](\sum_{k=0}^{\infty}c_kx^k)$

$=(\sum_{m=0}^{\infty}(\sum_{i=0}^{m}a_ib_{m-i})x^m)(\sum_{k=0}^{\infty}c_kx^k)$

$=\sum_{n=0}^{\infty}\sum_{j=0}^{n}[(\sum_{i=0}^{j}a_ib_{j-i})c_{n-j}]x^n$

$=\sum_{n=0}^{\infty}(\sum_{i+j+k=n}a_ib_jc_k)x^n$

$=\cdots=\sum_{i=0}^{\infty}a_ix^i[(\sum_{j=0}^{\infty}b_jx^j)(\sum_{k=0}^{\infty}c_kx^k)]$

Associative law holds. The others are easy to check. ■

$(*)$ For the rest of this study, a polynomial can be written as $a_0+a_1x+a_2x^2+\cdots+a_nx^n$ where n is the degree of the polynomial.

The Evaluation Homomorphisms

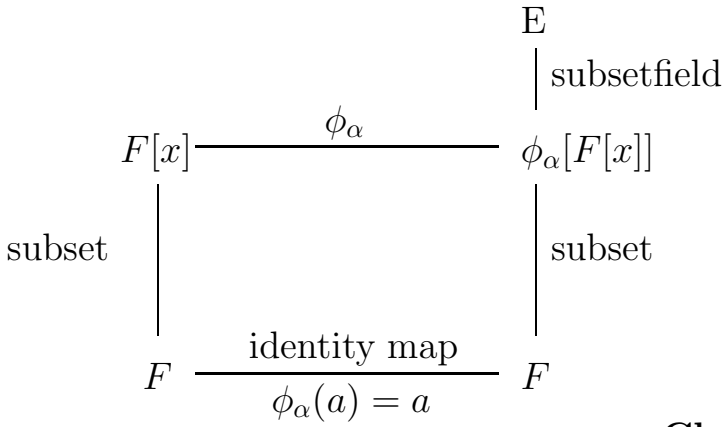
Defn. Let E and F be fields with F a subfield of E, i.e., $F\leq E$. Then we say E is an extension field of F.

$(*)$ The following theorem is very important in "solving a polynomial equation."

Theorem (The Evaluation Homomorphisms for Field Theory)

Let $F\leq E$, $\alpha\in E$ and x be an indeterminate. Then the map $\phi_\alpha:F[x]\to E$ defined by $\phi_\alpha(\sum_{i=0}^{n}a_ix^i)=\sum_{i=0}^{n}a_i\alpha^i$ for $\sum_{i=0}^{n}a_ix\in F[x]$ is a homomorphism of $F[x]$ into E. Also, $\phi_\alpha(x)=\alpha$, and $\phi_\alpha(a)=a$ $\forall\ a\in F$. The homomorphism ϕ_α is the evaluation of $\sum_{i=0}^{n}a_ix^i$ at α.

Proof.



Check!

Defn. (zero of $f(x)$)

If $f(\alpha) = \phi_\alpha(f(x)) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$, then α is a zero of $f(x)$. (f(α) can be obtained by using evaluation homo.)

Basic Goal

$(*)$ Solving polynomial equations!

$(**)$ Solving polynomial equations with coefficients from any field.

上述的工作前後積了超過兩千年的努力!

Factorization of polynomials over a Field

Note. If $f(x) = g(x)h(x)$, then

$f(\alpha) = \phi_\alpha(f(x)) = \phi_\alpha(g(x)h(x)) = \phi_\alpha(g(x))\phi_\alpha(h(x)) = g(\alpha)h(\alpha)$.

(Homomorphism works.)

Theorem (Division Algorithm for $F[x]$)

Let F be a field, $f(x)$ and $g(x)$ be two polynomials in $F[x]$ where $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$, where either $r(x) = 0$ or $deg(r(x)) < deg(g(x))$.

Proof. Let $S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$.

If $0 \in S$, then let $q(x) = s(x)$ and $r(x) = 0$, we are done. Note that if $f(x) = 0$, then $q(x) = 0$ and $r(x) = 0$. On the other hand if $0 \notin S$, then let $r(x)$ be an element in $S \subseteq F[x]$ which is of minimal degree and $r(x) = f(x) - g(x)q(x)$. Now we claim $deg(r(x)) < deg(g(x))$.

Let $\quad f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$

$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ and

$r(x) = c_0 + c_1x + c_2x^2 + \cdots + c_tx^t$.

Assume that $t \geq m$. Then

$f(x) - g(x)q(x) - (c_t/_{b_m})x^{t-m}g(x) = r(x) - (c_t/_{b_m})x^{t-m}g(x)$.

$f(x) - g(x)\underbrace{[q(x) - (c_t/_{b_m})x^{t-m}]}_{q'(x)} = r'(x)$.

Since $q'(x) \in F[x]$, $r'(x) \in S$. But $deg(r'(x)) < deg(r(x))$, this is a contradiction. That is, $deg(r(x)) < deg(g(x))$.

Next, we claim the uniqueness of $q(x)$ and $r(x)$. Assume that $f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$. Then

$g(x)(q_1(x) - q_2(x)) = r_1(x) - r_2(x)$.

Since $deg(r_1(x) - r_2(x)) < deg(g(x))$, or $r_1(x) - r_2(x) = 0$, $q_1(x) - q_2(x)$ must be 0. Hence $q_1(x) = q_2(x)$ and then we have $r_1(x) = r_2(x)$. ■

Corollary (Factor Theorem)

An element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$, i.e., $f(x) = (x - a)q(x)$ where $q(x) \in F[x]$.

Proof. Let $f(x) = (x - a)q(x) + r(x)$ as mentioned in above theorem. Since $(x - a)$ is of degree 1, $r(x)$ is a constant c.
($\Rightarrow$) By evaluation homomorphism $0 = f(a) = c$. Hence
$f(x) = (x - a)q(x)$.
($\Leftarrow$) Since $f(x) = (x - a)q(x)$, a is clearly a zero of $f(x)$. ■

Example Factoring $f(x) = x^4 + 3x^3 + 2x + 4$ in $\mathbb{Z}_5[x]$.

Since 1 is a zero of $f(x)$, $(x - 1) \mid f(x)$. Also, 4 is a zero of $f(x)$, $(x - 4) \mid f(x)$. In fact $f(x) = (x - 1)^3(x - 4) = (x + 4)^3(x + 1)$.

Corollary (zeros in F)

A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in F.

Proof. If a is a zero of $f(x)$ in F, then $f(x) = (x - a)q(x)$. If $f(x)$ has another zero b, then $f(x) = (x - a)(x - b)q_1x$. Clearly, now $deg(g(x)) = n - 2$. Therefore, by a routine argument $f(x)$ has at most n zero in F. ■

.

Theorem Let F be a field with finite elements. Then $< F^*, \cdot >$ is a

cyclic group, so are their subgroups.

Proof. Since $< F^*, \cdot >$ is a finite abelian group, $F^* \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_t}$ and then $|F^*| = d_1 d_2 \cdots d_t$ where d_i's are primes. Let $m = l.c.m.(d_1, d_2, \cdots, d_t)$ $(m \leq d_1 d_2 \cdots d_t)$. Then $\forall\ a \in F^*$, $a^m = 1$, i.e., the order of a is m, $m \mid |F^*|$. Hence, consider the polynomial $x^m - 1$, $x^m - 1$ has at least $|F^*|$ zeros in F. This implies that $m \geq d_1 d_2 \cdots d_t$. Thus, $m = d_1 d_2 \cdots d_t$. But $m = l.c.m.(d_1, d_2, \cdots, d_t)$. So, $d_1, d_2, \cdots, d_t$ are distinct primes. This concludes the proof by the fact that $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_t}$ is cyclic if $d_1, d_2, \cdots, d_t$ are distinct primes. ■

Defn. (Irreducible polynomial)

A nonconstant polynomial $f(x) \in F[x]$ is irreducible over F or is an irreducible polynomial in $F[x]$ if $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two polynomials $g(x)$ and $h(x)$ in $F[x]$ both of lower degree than $deg(f(x))$. If $f(x)$ is not irreducible, then $f(x)$ is reducible.

Theorem Let $f(x) \in F[x]$, and $deg(f(x)) = 2$ or 3. Then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

Theorem If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ can be factored into a product of two polynomials of lower degree r and s in $\mathbb{Q}[x]$ if and only if it has such a factorization with polynomials of the same degrees r and s in $\mathbb{Z}[x]$.

Corollary If $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n$ is in $\mathbb{Z}[x]$ with $a_0 \neq 0$, and if $f(x)$ has a zero in $\mathbb{Q}$, then it has a zero m in $\mathbb{Z}$, and $m \mid a_0$.

Example $f(x) = x^4 - 2x^2 + 8x + 1$ is a irreducible over $\mathbb{Q}$.

$(*)$ If $f(x)$ has a zero in $\mathbb{Q}$, then the zero must be either +1 or -1. But $f(1) = 8$ and $f(-1) = -8$, hence no zeros in $\mathbb{Q}$.

$(*)$ If $f(x) = (x^2 + ax + b)(x^2 + cx + d)$, then $bd = 1$, $ad + bc = 8$, $ac + b + d = -2$ and $a + c = 0$.
Since $b, d \in \mathbb{Z}$, $bd = 1$, we have $b = d = 1$ or $b = d = -1$. In either case $b = d$, $ad + bc = ab + bc = b(a + c) = 8$. $\rightarrow\leftarrow$ ■

Theorem (Eisenstein Criterion)

Let p be prime. Suppose that $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ is in $\mathbb{Z}[x]$, and $a_n \equiv 0 \pmod{p}$, but $a_i \equiv 0 \pmod{p}$ for all $i < n$, with $a_n \equiv 0 \pmod{p^2}$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. Omitted.

Example $25x^5 - 9x^4 - 3x^2 - 12$ is irreducible over $\mathbb{Q}$. Take $p = 3$.

$(*)$**Example** The polynomial $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible over $\mathbb{Q}$ for any prime p.

Tricky solution

If $\Phi_p(x)$ is reducible over $\mathbb{Q}$, then $\Phi_p(x+1)$ is also reducible over $\mathbb{Q}$. But $\Phi_p(x+1) = \frac{(x+1)^p-1}{(x+1)-1} = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{1}$. Since $\forall\ 0 < r < p$, $\binom{p}{r}$ is divisible by p, and $p \equiv 0 \pmod{p^2}$, $\Phi_p(x+1)$ is irreducible over $\mathbb{Q}$. This implies that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$.

Theorem (Unique factorization)

If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique except for order and for unit (nonzero constant) factors in F.

Proof. By induction. ■

End of Algebra (I).

Happy New Year!