COMMUTATIVE RINGS

Definition 1:

A commutative ring R is a set with two operations, addition and multiplication, such that:

(i) R is an abelian group under addition;

(ii) $ab = ba$ for all $a, b \in R$ (commutative law);

(iii) $a(bc) = (ab)c$ for any $a, b, c \in R$ (associative law);

(iv) there is an element $1 \in R$ with $1 \neq 0$ and with $1 \cdot a = a \cdot 1 = a$ for any $a \in R$;

(v) $a(b + c) = ab + ac$ for any $a, b, c \in R$ (distributive law).

Example:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings.
2. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a commutative ring.
3. $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a commutative ring.
4. $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Z}\}$ is not a ring. Moreover, $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$ is not a ring.
5. The set of all 2×2 matrices is a noncommutative ring.
6. $\mathbb{Z}_m$ is a commutative ring.

Theorem 1:

Let R be a commutative ring. Then:

(i) $0 \cdot a = 0$ for any $a \in R$.

(ii) If $-a$ is that number which, when added to a, gives 0, then $(-1)(-a) = a$ for any $a \in R$.

(iii) $(-1)a = -a$ for any $a \in R$.

Definition 2:

A subset S of a commutative ring R is a subring of R if:

(i) $1 \in S$;

(ii) if $a, b \in S$, then $a - b \in S$;

(iii) if $a, b \in S$, then $ab \in S$.

Example:

1. $\mathbb{Z}$ is a subring of $\mathbb{Q}$; $\mathbb{Q}$ is a subring of $\mathbb{R}$; $\mathbb{R}$ is a subring of $\mathbb{C}$;
2. $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

Definition 3:

A domain is a commutative ring R that satisfies the cancellation law for multiplication:

$$\text{if } ca = cb \text{ and } c \neq 0, \text{ then } a = b.$$

Example:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are domains.

2. $\mathbb{Z}_4$ is not a domain, since from $[2][2] = [2][0]$ does not follow $[2] = [0]$.

Theorem 2:

A commutative ring R is a domain if and only if the product of any two nonzero elements of R is nonzero.

Corollary:

$\mathbb{Z}_m$ is a domain if and only if m is a prime.

FIELDS

Definition 4:

A field F is a commutative ring such that for any nonzero $a \in F$ there exists $a^{-1} \in F$.

Example: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields. $\mathbb{Z}$ is not a field.

Definition 5:

An element u in a commutative ring R is called a unit if there exists $u^{-1} \in R$.

Example: All nonzero elements of $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are units.

Definition 4′:

A field F is a commutative ring in which every nonzero element of F is a unit.

Theorem 3:

Every field F is a domain.

Remark:

The converse of Theorem 3 is false. For example, $\mathbb{Z}$ is a domain, but not a field.

Theorem 4:

The commutative ring $\mathbb{Z}_m$ is a field if and only if m is a prime.

POLYNOMIALS

Definition 6:

If R is a commutative ring, then

$$R[x] = \{s_n x^n + \ldots + s_1 x + s_0,\ s_i \in R\}$$

is called the ring of polynomials over R. If

$$f(x) = s_n x^n + \ldots + s_1 x + s_0$$

is a polynomial over R, then s_n is called the leading coefficient and n is called the degree of $f(x)$, denoted by $\deg(f)$. If $s_n = 1$, then $f(x)$ is called a monic polynomial.

Theorem 5 (Division Algorithm):

Assume that k is a field and that $f(x), g(x) \in k[x]$ with $f(x) \neq 0$. Then there are unique polynomials $q(x), r(x) \in k[x]$ such that

$$g(x) = f(x)q(x) + r(x)$$

and either $r(x) = 0$ or $\deg(r) < \deg(f)$.

Example:

Let $g(x) = x^2 - 2x + 1,\ f(x) = x - 3$, then $x^2 - 2x + 1 = (x - 3)(x + 1) + 4$.

ROOTS OF POLYNOMIALS

Definition 7:

If $f(x) \in k[x]$, where k is a field, then a root of $f(x)$ in k is an element $a \in k$ with $f(a) = 0$.

Example:

The polynomial $f(x) = x^2 + 1 \in \mathbb{R}[x]$ has no roots in $\mathbb{R}$. However, since $f(x)$ is also from $\mathbb{C}[x]$, it has roots $x_1 = i,\ x_2 = -i$ in $\mathbb{C}$.

Lemma 1:

Let k be a field and let $f(x) \in k[x]$. Then for any $a \in k$ there exists $q(x) \in k[x]$ such that

$$f(x) = (x - a)q(x) + f(a).$$

Proof:

By the Division Algorithm we have

$$f(x) = (x - a)q(x) + r(x),$$

where $\deg(r) < \deg(x - a) = 1$, and therefore $\deg(r) = 0$, i.e. $r(x) = r$ is a constant. So,

$$f(x) = (x - a)q(x) + r \quad \Longrightarrow \quad f(a) = (a - a)q(a) + r = r = r(x). \blacksquare$$

Lemma 2:

Let k be a field and let $f(x) \in k[x]$. Then $a \in k$ is a root of $f(x)$ in k if and only if $x-a$ divides $f(x)$ in $k[x]$, i.e. there exists $q(x) \in k[x]$ such that

$$f(x) = (x-a)q(x).$$

Proof:

$\Longrightarrow$) If a is a root of $f(x)$ in k, then $f(a) = 0$, therefore by Lemma 1 we get

$$f(x) = (x-a)q(x) + f(a) = (x-a)q(x).$$

$\Longleftarrow$) If $f(x) = (x-a)q(x)$, then

$$f(a) = (a-a)q(a) = 0,$$

which means that a is a root of $f(x)$. ■

Theorem 6:

Let k be a field and let $f(x) \in k[x]$. Let also $f(x)$ has degree n. Then $f(x)$ has at most n roots in k.

Proof:

We will use induction by n. If $n = 0$, then $f(x)$ is a constant, and we are done. Suppose the theorem is true for some $n = m \geq 0$. We prove it for $n = m+1$. In fact, if $f(x)$ has no roots in k, then we are done, since $0 < n$. Otherwise, we may assume that there exists $a \in k$ such that $f(a) = 0$. Then by Lemma 2 we have

$$f(x) = q(x)(x-a) \quad \text{and} \quad \deg(q) = m.$$

If there is a root $b \in k$ with $b \neq a$, then

$$0 = f(b) = q(b)(b-a).$$

Since $b - a \neq 0$, we have $q(b) = 0$, so that b is a root of $q(x)$. Now $\deg(q) = m$, so that the inductive hypothesis says that $q(x)$ has at most m roots in k. Therefore, $f(x)$ has at most $m+1$ roots in k. ■

Corollary 1:

Let k be a field and let $f(x), g(x) \in k[x]$. If $\deg(f) \leq \deg(g) = n$ and if $f(a) = g(a)$ for $n+1$ values $a \in k$, then $f(x) = g(x)$.

Proof:

Suppose to the contrary that $f(x) \neq g(x)$. Then

$$h(x) = f(x) - g(x) \neq 0$$

and

$$\deg(h) \leq \max(\deg(f),\ \deg(g)) = n.$$

By hypothesis, there are $n+1$ elements $a \in k$ such that

$$h(a) = f(a) - g(a) = 0,$$

which contradicts Theorem 6. ■.

Corollary 2:

Let k be a field and let $f(x) \in k[x]$. Let also $f(x)$ has degree n and $\alpha_1, \ldots, \alpha_n$ are distinct roots of $f(x)$ in k. Then there exists $c \in k$ such that

$$f(x) = c(x - \alpha_1) \ldots (x - \alpha_n).$$

GREATEST COMMON DIVISOR

Definition 8:

Let k be a field and let $f(x), g(x) \in k[x]$. A common divisor of $f(x)$ and $g(x)$ is a polynomial $c(x) \in k[x]$ such that $c(x) \mid f(x)$ and $c(x) \mid g(x)$. The greatest common divisor (gcd) is a monic common divisor of the highest degree.

Theorem 7:

Let k be a field and let $f(x), g(x) \in k[x]$. Then their gcd is a linear combination of $f(x)$ and $g(x)$.

Proof:

Part I. Consider the following set:

$$I = \{s(x)f(x) + t(x)g(x) : s(x), t(x) \in k[x]\}.$$

Pick a polynomial $d(x) \in I$ of the smallest degree. We have

$$d(x) = s(x)f(x) + t(x)g(x). \qquad (*)$$

By the Division Algorithm we obtain

$$f(x) = d(x)q(x) + r(x), \quad \text{where} \quad r(x) = 0 \quad \text{or} \quad \deg(r) < \deg(d). \qquad (**)$$

From $(*)$ and $(**)$ it follows that

$$\begin{aligned} r(x) = f(x) - d(x)q(x) &= f(x) - [s(x)f(x) + t(x)g(x)]q(x) \\ &= [1 - s(x)q(x)]f(x) - t(x)q(x)g(x) \in I. \end{aligned}$$

So, $r(x)$ is a linear combination of $f(x)$ and $g(x)$ and $\deg(r) < \deg(d)$. This is a contradiction. Therefore $r(x) = 0$, which means $d(x) \mid f(x)$. A similar argument shows that $d(x) \mid g(x)$.

Part II. We now prove that $d(x)$ is the greatest common divisor of $f(x)$ and $g(x)$. In fact, assume to the contrary that $c(x)$ is the gcd of $f(x)$ and $g(x)$. Then $c(x) \mid f(x)$ and $c(x) \mid g(x)$. Hence

$$c(x) \mid d(x) = s(x)f(x) + t(x)g(x).$$

Since $c(x)$ and $d(x)$ are monic polynomials, it follows that $\deg(c) < \deg(d)$, which is a contradiction. ■

EUCLIDEAN ALGORITHM

Theorem 8 (Euclidean Algorithm):

Let k be a field and let $f(x), g(x) \in k[x]$. Then there is an algorithm for computing the gcd $(f(x), g(x))$.

Proof:

To find the greatest common divisor of two polynomials $f(x)$ and $g(x)$ we apply the algorithm, similar to the Euclidean Algorithm in $\mathbb{Z}$:

$$\begin{aligned} g(x) &= f(x)q_1(x) + r_1(x) \\ f(x) &= r_1(x)q_2(x) + r_2(x) \\ r_1(x) &= r_2(x)q_3(x) + r_3(x) \\ &\cdots \\ r_{n-2}(x) &= r_{n-1}(x)q_n(x) + r_n(x) \\ r_{n-1}(x) &= r_n(x)q_{n+1}(x), \end{aligned}$$

therefore the gcd $(f(x), g(x)) = r_n(x)$.

Example:

Find the gcd $(x^3 + 1, x^5 + 1)$ and express it as a linear combination of $x^3 + 1$ and $x^5 + 1$.

Solution:

We have

$$\begin{aligned} x^5 + 1 &= (x^3 + 1)x^2 + (-x^2 + 1) \\ x^3 + 1 &= (-x^2 + 1)(-x) + (x + 1) \\ -x^2 + 1 &= (x + 1)(-x + 1) \end{aligned}$$

therefore gcd $(x^3 + 1, x^5 + 1) = x + 1$. Finally, we have

$$x+1 = (x^3+1)-(-x^2+1)(-x) = (x^3+1)-[x^5+1-(x^3+1]x^2)(-x) = (x^3+1)(x^3-1)+(x^5+1)x.$$

EUCLIDS LEMMA

Definition:

Let k be a field. A polynomial $p(x) \in k[x]$ is irreducible over k if $\deg(p) = n \geq 1$ and there is no factorization in $k[x]$ of the form $p(x) = f(x)g(x)$ in which both factors have degree smaller than n.

Example:

One can show that $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, but it is reducible in $\mathbb{C}[x]$:

$$x^2 + 1 = (x + i)(x - i).$$

Theorem 9 (Euclid's Lemma):

Let k be a field and let $f(x), g(x) \in k[x]$. If $p(x)$ is an irreducible polynomial in $k[x]$ and $p(x) \mid f(x)g(x)$, then either $p(x) \mid f(x)$ or $p(x) \mid g(x)$. More generally, if $p(x) \mid f_1(x) \dots f_n(x)$, then $p(x) \mid f_i(x)$ for some index i.

Lemma:

Let k be a field and let $p(x), f(x) \in k[x]$. Let also $d(x) = (p(x), f(x))$ be the gcd of $p(x)$ and $f(x)$. If $p(x)$ is a monic irreducible polynomial, then

$$d(x) = \begin{cases} 1 & \text{if } p(x) \nmid f(x) \\ p(x) & \text{if } p(x) \mid f(x). \end{cases}$$

Proof:

Since $p(x)$ is monic and irreducible, it follows that the only monic divisors of $p(x)$ are 1 and $p(x)$. If $p(x) \mid f(x)$, then $d(x) = p(x)$, since $p(x)$ is monic. If $p(x) \nmid f(x)$, then the only monic common divisor is 1, and so $d(x) = 1$. ■

Proof of Euclid's Lemma:

If $p(x) \mid f(x)$, we are done. Suppose $p(x) \nmid f(x)$. Then the lemma above says that the gcd $(p(x), f(x)) = 1$. Therefore by Theorem 7 there are polynomials $s(x)$ and $t(x)$ with

$$1 = s(x)p(x) + t(x)f(x) \quad \Longrightarrow \quad g(x) = s(x)p(x)g(x) + t(x)f(x)g(x).$$

Since $p(x) \mid f(x)g(x)$, it follows that $p(x) \mid g(x)$ as desired. The second statement follows by induction on $n \geq 2$. ■

Theorem 10:

Let k be a field, then every polynomial $f(x) \in k[x]$ of degree ≥ 1 is a product of a nonzero constant and monic irreducible polynomials. Moreover, if $f(x)$ has two such factorizations

$$f(x) = ap_1(x) \dots p_m(x)$$

and

$$f(x) = bq_1(x) \dots q_n(x),$$

where a and b are nonzero constants and p's and q's are monic irreducible polynomials, then $a = b$, $m = n$, and q's may be reindexed so that $q_i = p_i$ for all i.

Proof:

Step 1: We first prove by induction that the factorization does exist. In fact, if $\deg f = 1$, then

$$f(x) = ax + c = a(\underbrace{x + a^{-1}c}_{\text{irred.}}).$$

Suppose this is true for any $f(x) \in k[x]$ with $\deg f \leq n$. We prove it for $f(x)$ with $\deg f \leq n+1$. If $f(x)$ is irreducible, then $f(x) = a(a^{-1}f(x))$, and we are done. If $f(x)$ is reducible, i.e. $f(x) = g(x)h(x)$, then $\deg g \leq n$ and $\deg h \leq n$, therefore the factorization does exist for them by the inductive hypothesis, and we are done again.

Step 2: We now prove by induction that the factorization is unique. In fact, suppose

$$ap_1(x) \dots p_m(x) = f(x) = bq_1(x) \dots q_n(x).$$

Put

$$M = \max(m, n).$$

If $M = 1$, we have

$$ap_1(x) = bq_1(x).$$

Since $p(x)$ and $q(x)$ are monic, it follows that $a = b$ and $p_1(x) = q_1(x)$. Suppose the theorem is true for some $M \geq 1$. We prove it for $M + 1$. By Euclid's Lemma there is some i with $p_m(x) \mid q_i(x)$. Since $p_m(x)$ and $q_i(x)$ are monic, it follows that $p_m(x) = q_i(x)$. Canceling this factor, we have

$$a \underbrace{p_1(x) \dots p_{m-1}(x)}_{\leq M \text{ terms}} = b \underbrace{q_1(x) \dots q_{i-1}q_{i+1} \dots q_n(x)}_{\leq M \text{ terms}},$$

therefore the factorization is unique by the inductive hypothesis. ■

Definition 1:

A commutative ring R is a set with two operations, addition and multiplication, such that:

(i) R is an abelian group under addition;

(ii) $ab = ba$ for all $a, b \in R$ (commutative law);

(iii) $a(bc) = (ab)c$ for any $a, b, c \in R$ (associative law);

(iv) there is an element $1 \in R$ with $1 \neq 0$ and with $1 \cdot a = a \cdot 1 = a$ for any $a \in R$;

(v) $a(b+c) = ab+ac$ for any $a, b, c \in R$ (distributive law).

Example:

1. Z, Q, R, C are commutative rings.
2. $Z[i] = \{a + bi : a, b \in Z\}$ is a commutative ring.
3. $\{a+b\sqrt{2} : a, b \in Z\}$ is a commutative ring.
4. $\{a + b\sqrt[3]{2} : a, b \in Z\}$ is not a ring. Moreover, $\{a + b\sqrt[3]{2} : a, b \in Q\}$ is not a ring.
5. The set of all 2×2 matrices is a noncommutative ring.
6. Z_m is a commutative ring.

Theorem 1:

Let R be a commutative ring. Then:

(i) $0 \cdot a = 0$ for any $a \in R$.

(ii) If $-a$ is that number which, when added to a, gives 0, then $(-1)(-a) = a$ for any $a \in R$.

(iii) $(-1)a = -a$ for any $a \in R$.

Definition 2:

A subset S of a commutative ring R is a subring of R if:

(i) $1 \in S$;

(ii) if $a, b \in S$, then $a - b \in S$;

(iii) if $a, b \in S$, then $ab \in S$.

Example:

1. Z is a subring of Q; Q is a subring of R; R is a subring of C;

2. $Z[i]$ is a subring of C.

Definition 3:

A domain is a commutative ring R that satisfies the cancellation law for multiplication:

$$\text{if } ca = cb \text{ and } c \neq 0, \text{ then } a = b.$$

Example:

1. Z, Q, R, C are domains.
2. Z_4 is not a domain, since from

$$[2][2] = [2][0]$$

does not follow $[2] = [0]$.

Theorem 2:

A commutative ring R is a domain if and only if the product of any two nonzero elements of R is nonzero.

Corollary:

Z_m is a domain if and only if m is a prime.

Definition 4:

A field F is a commutative ring such that for any nonzero $a \in F$ there exists $a^{-1} \in F$.

Example:

Q, R, C are fields. Z is not a field.

Definition 5:

An element u in a commutative ring R is called a unit if there exists $u^{-1} \in R$.

Example:

All nonzero elements of Q, R, and C are units.

Definition $4'$:

A field F is a commutative ring in which every nonzero element of F is a unit.

Theorem 3:

Every field F is a domain.

Remark:

The converse of Theorem 3 is false. For example, Z is a domain, but not a field.

Theorem 4:

The commutative ring Z_m is a field if and only if m is a prime.

Definition 6:

If R is a commutative ring, then

$$R[x] = \{s_n x^n + \ldots + s_1 x + s_0,\ s_i \in R\}$$

is called the ring of polynomials over R. If

$$f(x) = s_n x^n + \ldots + s_1 x + s_0$$

is a polynomial over R, then s_n is called the leading coefficient and n is called the degree of $f(x)$, denoted by $\deg(f)$. If $s_n = 1$, then $f(x)$ is called a monic polynomial.

Theorem (Division Algorithm):
Assume that k is a field and that

$$f(x), g(x) \in k[x]$$

with $f(x) \neq 0$. Then there are unique polynomials $q(x), r(x) \in k[x]$ with

$$g(x) = f(x)q(x) + r(x)$$

and either $r(x) = 0$ or $\deg(r) < \deg(f)$.

Example:
Let $g(x) = x^2 - 2x + 1,\ f(x) = x - 3$, then

$$x^2 - 2x + 1 = (x - 3)(x + 1) + 4.$$

Definition:

If $f(x) \in k[x]$, where k is a field, then a root of $f(x)$ in k is an element $a \in k$ with $f(a) = 0$.

Example:

The polynomial $f(x) = x^2 + 1 \in R[x]$ has no roots in R. However, since $f(x)$ is also from $C[x]$, it has roots $x_1 = i$, $x_2 = -i$ in C.

Lemma 1:

Let k be a field and let $f(x) \in k[x]$. Then for any $a \in k$ there exists $q(x) \in k[x]$ such that

$$f(x) = (x - a)q(x) + f(a).$$

Proof:

By the Division Algorithm we have

$$f(x) = (x - a)q(x) + r(x),$$

where $\deg(r) < \deg(x - a) = 1$, and therefore $\deg(r) = 0$, i.e. $r(x) = r$ is a constant. So,

$$f(x) = (x - a)q(x) + r$$

$$\Downarrow$$

$$f(a) = (a - a)q(a) + r = r = r(x). \blacksquare$$

Lemma 2:

Let k be a field and let $f(x) \in k[x]$. Then $a \in k$ is a root of $f(x)$ in k if and only if $x - a$ divides $f(x)$ in $k[x]$, i.e. there exists $q(x) \in k[x]$ such that

$$f(x) = (x - a)q(x).$$

Proof:

$\Longrightarrow$) If a is a root of $f(x)$ in k, then $f(a) = 0$, therefore by Lemma 1 we get

$$f(x) = (x-a)q(x)+f(a) = (x-a)q(x).$$

$\Longleftarrow$) If $f(x) = (x - a)q(x)$, then

$$f(a) = (a - a)q(a) = 0,$$

which means that a is a root of $f(x)$. ■

Theorem 6:

Let k be a field and let $f(x) \in k[x]$. Let also $f(x)$ has degree n. Then $f(x)$ has at most n roots in k.

Proof:

We will use induction by n. If $n = 0$, then $f(x)$ is a constant, and we are done. Suppose the theorem is true for some $n = m \geq 0$. We prove it for $n = m + 1$. In fact, if $f(x)$ has no roots in k, then we are done, since $0 < n$. Otherwise, we may assume that there exists $a \in k$ such that $f(a) = 0$. Then by Lemma 2 we have

$$f(x) = q(x)(x - a) \quad \text{and} \quad \deg(q) = m.$$

If there is a root $b \in k$ with $b \neq a$, then

$$0 = f(b) = q(b)(b - a).$$

Since $b - a \neq 0$, we have $q(b) = 0$, so that b is a root of $q(x)$. Now $\deg(q) = m$, so that the inductive hypothesis says that $q(x)$ has at most m roots in k. Therefore, $f(x)$ has at most $m + 1$ roots in k. ■

Corollary 1:

Let k be a field and let $f(x), g(x) \in k[x]$. If $\deg(f) \leq \deg(g) = n$ and if $f(a) = g(a)$ for $n+1$ values $a \in k$, then $f(x) = g(x)$.

Proof:

Suppose to the contrary that $f(x) \neq g(x)$. Then

$$h(x) = f(x) - g(x) \neq 0$$

and

$$\deg(h) \leq \max(\deg(f),\ \deg(g)) = n.$$

By hypothesis, there are $n+1$ elements $a \in k$ such that

$$h(a) = f(a) - g(a) = 0,$$

which contradicts Theorem 6. ■.

Corollary 2:

Let k be a field and let $f(x) \in k[x]$. Let also $f(x)$ has degree n and $\alpha_1, \ldots, \alpha_n$ are distinct roots of $f(x)$ in k. Then there exists $c \in k$ such that

$$f(x) = c(x - \alpha_1) \ldots (x - \alpha_n).$$

Definition 8:

Let k be a field and let $f(x), g(x) \in k[x]$. A common divisor of $f(x)$ and $g(x)$ is a polynomial $c(x) \in k[x]$ such that $c(x) \mid f(x)$ and $c(x) \mid g(x)$. The greatest common divisor (gcd) is a monic common divisor of the highest degree.

Theorem 7:

Let k be a field and let $f(x), g(x) \in k[x]$. Then their gcd is a linear combination of $f(x)$ and $g(x)$.

Proof:

Part I. **Consider the following set:**

$$I = \{s(x)f(x)+t(x)g(x) : s(x), t(x) \in k[x]\}.$$

Pick a polynomial $d(x) \in I$ of the smallest degree. We have

$$d(x) = s(x)f(x) + t(x)g(x). \qquad (*)$$

By the Division Algorithm we obtain

$$f(x) = d(x)q(x) + r(x), \qquad (**)$$

where $r(x) = 0$ or $\deg(r) < \deg(d)$. From $(*)$ and $(**)$ it follows that

$$r(x) = f(x) - d(x)q(x)$$
$$= f(x) - [s(x)f(x) + t(x)g(x)]q(x)$$
$$= [1 - s(x)q(x)]f(x) - t(x)q(x)g(x) \in I.$$

So, $r(x)$ is a linear combination of $f(x)$ and $g(x)$ and $\deg(r) < \deg(d)$. This is a contradiction. Therefore $r(x) = 0$, which means $d(x) \mid f(x)$. A similar argument shows that $d(x) \mid g(x)$.

Part II. **We now prove that $d(x)$ is the greatest common divisor of $f(x)$ and $g(x)$. In fact, assume to the contrary that $c(x)$ is the gcd of $f(x)$ and $g(x)$. Then $c(x) \mid f(x)$ and $c(x) \mid g(x)$. Hence**

$$c(x) \mid d(x) = s(x)f(x) + t(x)g(x).$$

Since $c(x)$ and $d(x)$ are monic polynomials, it follows that $\deg(c) < \deg(d)$, which is a contradiction. ■

Theorem 8 (Euclidean Algorithm):

Let k be a field and let $f(x), g(x) \in k[x]$. Then there is an algorithm for computing the gcd $(f(x), g(x))$.

Proof:

To find the greatest common divisor of two polynomials $f(x)$ and $g(x)$ we apply the algorithm, similar to the Euclidean Algorithm in Z :

$$\begin{aligned} g(x) &= f(x)q_1(x) + r_1(x) \\ f(x) &= r_1(x)q_2(x) + r_2(x) \\ r_1(x) &= r_2(x)q_3(x) + r_3(x) \\ &\cdots \\ r_{n-2}(x) &= r_{n-1}(x)q_n(x) + r_n(x) \\ r_{n-1}(x) &= r_n(x)q_{n+1}(x), \end{aligned}$$

therefore the gcd $(f(x), g(x)) = r_n(x)$.

Example:

Find the gcd (x^3+1, x^5+1) and express it as a linear combination of x^3+1 and x^5+1.

Solution:

We have

$$\begin{aligned} x^5+1 &= (x^3+1)x^2 + (-x^2+1) \\ x^3+1 &= (-x^2+1)(-x) + (x+1) \\ -x^2+1 &= (x+1)(-x+1) \end{aligned}$$

therefore gcd $(x^3+1, x^5+1) = x+1$. **Finally, we have**

$$\begin{aligned} & x+1 \\ &= (x^3+1) - (-x^2+1)(-x) \\ &= (x^3+1) - [x^5+1-(x^3+1)x^2](-x) \\ &= (x^3+1)(x^3-1) + (x^5+1)x. \end{aligned}$$

Definition:

Let k be a field. A polynomial $p(x) \in k[x]$ is irreducible over k if $\deg(p) = n \geq 1$ and there is no factorization in $k[x]$ of the form $p(x) = f(x)g(x)$ in which both factors have degree smaller than n.

Example:

One can show that $x^2 + 1$ is irreducible in $R[x]$, but it is reducible in $C[x]$:

$$x^2 + 1 = (x + i)(x - i).$$

Theorem (Euclid's Lemma):

Let k be a field and let $f(x), g(x) \in k[x]$. If $p(x)$ is an irreducible polynomial in $k[x]$ and $p(x) \mid f(x)g(x)$, then either $p(x) \mid f(x)$ or $p(x) \mid g(x)$. More generally, if $p(x) \mid f_1(x) \dots f_n(x)$, then $p(x) \mid f_i(x)$ for some index i.

Lemma:

Let k be a field and let $p(x), f(x) \in k[x]$. Let also $d(x) = (p(x), f(x))$ be the gcd of $p(x)$ and $f(x)$. If $p(x)$ is a monic irreducible polynomial, then

$$d(x) = \begin{cases} 1 & \text{if } p(x) \nmid f(x) \\ p(x) & \text{if } p(x) \mid f(x). \end{cases}$$

Proof:

Since $p(x)$ is monic and irreducible, it follows that the only monic divisors of $p(x)$ are 1 and $p(x)$. If $p(x) \mid f(x)$, then $d(x) = p(x)$, since $p(x)$ is monic. If $p(x) \nmid f(x)$, then the only monic common divisor is 1, and so $d(x) = 1$. ■

Proof of Euclid's Lemma:

If $p(x) \mid f(x)$, we are done. Suppose $p(x) \not\mid f(x)$. Then the lemma above says that the gcd $(p(x), f(x)) = 1$. Therefore by Theorem 7 there are polynomials $s(x)$ and $t(x)$ with

$$1 = s(x)p(x) + t(x)f(x)$$

$$\Downarrow$$

$$g(x) = s(x)p(x)g(x) + t(x)f(x)g(x).$$

Since $p(x) \mid f(x)g(x)$, it follows that $p(x) \mid g(x)$ as desired. The second statement follows by induction on $n \geq 2$. ■

Theorem 10:

Let k be a field, then every polynomial $f(x) \in k[x]$ of degree ≥ 1 is a product of a nonzero constant and monic irreducible polynomials. Moreover, if $f(x)$ has two such factorizations

$$f(x) = ap_1(x) \dots p_m(x)$$

and

$$f(x) = bq_1(x) \dots q_n(x),$$

where a and b are nonzero constants and p's and q's are monic irreducible polynomials, then $a = b$, $m = n$, and q's may be reindexed so that $q_i = p_i$ for all i.

Proof:

Step 1: **We first prove by induction that the factorization does exist. In fact, if** $\deg f = 1$**, then**

$$f(x) = ax + c = a(\underbrace{x + a^{-1}c}_{\text{irred.}}).$$

Suppose this is true for any $f(x) \in k[x]$ **with** $\deg f \leq n$**. We prove it for** $f(x)$ **with** $\deg f \leq n+1$**. If** $f(x)$ **is irreducible, then** $f(x) = a(a^{-1}f(x))$**, and we are done. If** $f(x)$ **is reducible, i.e.** $f(x) = g(x)h(x)$**, then** $\deg g \leq n$ **and** $\deg h \leq n$**, therefore the factorization does exist for them by the inductive hypothesis, and we are done again.**

Step 2: **We now prove by induction that the factorization is unique. In fact, suppose**

$$ap_1(x)\dots p_m(x) = f(x) = bq_1(x)\dots q_n(x).$$

Put

$$M = \max(m, n).$$

If $M = 1$, we have

$$ap_1(x) = bq_1(x).$$

Since $p(x)$ and $q(x)$ are monic, it follows that $a = b$ and $p_1(x) = q_1(x)$. Suppose the theorem is true for some $M \geq 1$. We prove it for $M + 1$. By Euclid's Lemma there is some i with $p_m(x) \mid q_i(x)$. Since $p_m(x)$ and $q_i(x)$ are monic, it follows that $p_m(x) = q_i(x)$.

Canceling this factor, we have

$$a \underbrace{p_1(x) \dots p_{m-1}(x)}_{\leq M \text{ terms}}$$
$$= b \underbrace{q_1(x) \dots q_{i-1} q_{i+1} \dots q_n(x)}_{\leq M \text{ terms}},$$

therefore the factorization is unique by the inductive hypothesis. ■