§9 polynomials over $\mathbb{Q}$.

$\boxed{\text{Example 1}}$ $f(x) = \frac{2}{3}x^4 - 2x^2 - \frac{2}{5}x$ (over $\mathbb{Q}$)

$$= \frac{1}{15}[10x^4 - 30x^2 - 6x] = \frac{2}{15}[5x^4 - 15x^2 - 3x] = \frac{2}{15}p(x)$$

$f(x)$ is an associate of a polynomial $p(x)$, which has integer coefficients, and the greatest common divisior of these coefficients is 1.

$\boxed{\text{Facts}}$. Any polynomial over $\mathbb{Q}$ is an associate of a polynomial with integer coefficients.

(A) Gauss's Lemma.

$\boxed{\text{Def 1.}}$ A polynomial $f(x)$ over $\mathbb{Z}$ is called primitive if its coefficients are relatively prime, that is, the greatest common divisor of its coefficients is 1.

$\boxed{\text{Note}}$: (1) A primitive polynomial is not the zero polynomial.

2) Any polynomial in $\mathbb{Q}[x]$ is an associate of a primitive polynomial.

$\boxed{\text{Lemma 1.}}$ If $g(x)$ is primitive, $f(x)$ is in $\mathbb{Z}[x]$, and $f(x) = ag(x)$ for some $a \in \mathbb{Q}$, then $a \in \mathbb{Z}$. If $f(x)$ is also primitive, then $a = 1$ or $a = -1$.

proof. Write $a = \frac{r}{s}$ with r, s coprime integers. Then

$$sf(x) = rg(x) \Leftrightarrow sa_i = rb_i,\ 0 \le i \le n.$$

Since r and s are coprime, s must divide all the coefficients of $g(x)$. But $g(x)$ is primitive, so $s = 1$ or $s = -1$. Thus a is an integer. If also $f(x)$ is primitive, then by the same argument, r must be 1 or -1. Hence $a = 1$ or $a = -1$.

$\square$.

Theorem 1. (Gauss's Lemma) The product of two primitive polynomials is primitive.

Proof. Let
$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$
$$g(x) = b_0 + b_1x + \cdots + b_mx^m .$$
be two primitive polynomials. Let us assume that, on the contrary, $h(x) = f(x)g(x)$ is not primitive. Thus, there exists a prime element $p \in \mathbb{Z}$ such that p divides every coefficient of $h(x)$. Choose the least indices s and t such that
$$p \nmid a_s \quad \text{and} \quad p \nmid b_t,$$
Since $f(x)$ and $g(x)$ are primitive. The coefficient of x^{s+t} in $h(x)$ is
$$c_{s+t} = a_sb_t + (a_{s+1}b_{t-1} + a_{s+2}b_{t-2} + \cdots) + (a_{s-1}b_{t+1} + a_{s-2}b_{t+2} + \cdots).$$
Since we have assumed that a_{s-i} and b_{t-i} are divisible by p for $i > 0$, and since $p \mid c_{s+t}$, we have $p \mid a_sb_t$. This means $p \mid a_s$ or $p \mid b_t$, a contradiction. This proves our claim that $f(x)g(x)$ is primitive. $\square$.

By the content $d(f)$ of a polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, we mean the greatest common divisor of all the cofficients of $f(x)$. Hence we can write any polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ in the form
$$f(x) = d(f)f_0(x), \quad g(x) = d(g)g_0(x)$$
where $f_0(x)$ and $g_0(x)$ are primitive polynomials. Since $f(x)g(x) = d(f)d(g)f_0(x)g_0(x)$, and we have proved that $d(f_0g_0) = 1$ (Gauss's Lemma), it follows that
$$d(fg) = d(f)d(g).$$

Thm2 (Gauss) Let $f(x)$ be a polynomial with integer coefficients. Suppose $f(x)=a(x)b(x)$ with $a(x)$ and $b(x)$ in $\mathbb{Q}[x]$. Then there are polynomials $a_1(x)$ and $b_1(x)$ in $\mathbb{Z}[x]$, which are associates of $a(x)$ and $b(x)$, respectively, so that $f(x)=a_1(x)b_1(x)$.

proof. Let $a_0(x)$ and $b_0(x)$ be primitive polynomials in $\mathbb{Z}[x]$ that are associates of $a(x)$ and $b(x)$, respectively, so that

$$a(x)=c\,a_0(x), \quad b(x)=d\,b_0(x)$$

with c, d some rational numbers. Then

$$f(x)=cd\,a_0(x)\,b_0(x).$$

Now $a_0(x)b_0(x)$ is primitive by Gauss's Lemma. Hence,

$$d(f)=cd$$

and so that cd is an integer. Therefore,

$$f(x)=(cd\,a_0(x))\,b_0(x)$$

is a factorization in $\mathbb{Z}[x]$ where $cd\,a_0(x)$ and $b_0(x)$ are associates of $a(x)$ and $b(x)$, respectively. That completes the proof. $\square$

Gauss Theorem: Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then $f(x)$ is reducible over $\mathbb{Z}$.

(By Lemma 1)

Corollary 1. A polynomial $f(x)\in\mathbb{Z}[x]$ which is irreducible over $\mathbb{Z}$ is also irreducible over $\mathbb{Q}$.

Corollary 2. If $f(x)$ is in $\mathbb{Z}[x]$ and $f(x)=g(x)h(x)$ in $\mathbb{Q}[x]$ with $g(x)$ primitive, then $h(x)$ is in $\mathbb{Z}[x]$.

proof. By Theorem 2, $f(x)=g(x)(ch_1(x))$, for some $c\in\mathbb{Q}$, and $h_1(x)$ is primitive. Hence $d(f)=c$. So $c\in\mathbb{Z}$ and $h(x)=c\,h_1(x)$ is in $\mathbb{Z}[x]$. $\square$

Theorem 3. (Descarte's Rational Root Theorem). Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

be in $\mathbb{Z}[x]$. Suppose $\frac{r}{s}$ is a rational root of $f(x)$ where $r, s \in \mathbb{Z}$ with $(r, s) = 1$. Then $s \mid a_n$ and $r \mid a_0$. In particular, if $f(x)$ is a monic polynomial, then every rational root of $f(x)$ is in $\mathbb{Z}$ and divides a_0.

Proof. Since r/s is a root of $f(x)$, we can write $f(x) = (sx - r) g(x)$ for some polynomial

$$g(x) = b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$$

in $\mathbb{Q}[x]$. By Corollary 2, and since $sx - r$ is primitive, $g(x) \in \mathbb{Z}[x]$. Clearly, $b_{n-1} s = a_n$ and $-b_0 r = a_0$. Hence $s \mid a_n$ and $r \mid a_0$. $\square$.

Example 2. Consider finding a rational root of the polynomial $f(x) = x^3 + 2x^2 + 2$. Since $\pm 1, \pm 2$ are all divisors of 2, they are candidates for a possible root of $f(x)$. But it turns out that $f(x)$ has no roots in $\mathbb{Q}$.

(B) Testing for irreducibility

Theorem 4 (Eisenstein's Irriducible Criterion) Suppose

$$f(x) = a_n x^n + \cdots + a_0$$

is in $\mathbb{Z}[x]$ and there exists a prime number p such that

[i] $p \nmid a_n$,

[ii]. $p \mid a_{n-1}, a_{n-2}, \ldots, a_0$,

[iii]. $p^2 \nmid a_0$.

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

proof. Suppose that, on the contrary, there is a factorization $f(x)=g(x)h(x)$, with

$$g(x)=b_r x^r+\dots+b_1x+b_0$$

$$h(x)=c_s x^s+\dots+c_1x+c_0$$

and $b_r\neq 0$, $c_s\neq 0$, $r>0$, $s>0$ and $r+s=n$. From

$$a_0=b_0c_0,\quad p\mid a_0,\quad p^2\nmid a_0,$$

we conclude that precisely one of b_0 and c_0 is divisible by p. We may assume

$$p\mid b_0,\quad p\nmid c_0.$$

Not all the b_i are divisible by p, since, otherwise, all the a_i would be divisible by p whereas $p\nmid a_n$. Let k denote the least subscript such that b_k is not divisible by p so that

$$p\mid b_0,\ p\mid b_1,\ \dots,\ p\mid b_{k-1},\ p\nmid b_k.$$

By the fact that

$$a_k=b_kc_0+b_{k-1}c_1+\dots+b_0c_k,$$

we have $p\nmid a_k$. This contradicts the hypothesis that $p\mid a_k$ for $k<n$. So the theorem is proved. □.

$\boxed{\text{Example 3}}$. It is easy to construct examples where Eisenstein's criterin applies. The simplest are rational polynomials x^n-b, where b has a prime factor p such that p^2 does not divide b, such as

$$x^9-12,\ \text{or}\ x^4-45,\ \text{or}\ x^n-2.$$

$\boxed{\text{Fact:}}$ A rational irreducible polynomial could have any positive degree.