Theorem: uniqueness of factorization

Let F be a field and let $f(x) \in F[x]$ be a non-constant polynomial. Then we can express $f(x)$ as a product of irreducible polynomials

$$f(x) = p_1(x)p_2(x) \dots p_r(x),$$

unique up to changing order and multiplication by units.

Proposition

In $\mathbb{R}[x]$, all irreducible polynomials have degree 1 or 2.

Note. In $\mathbb{C}[x]$, all irreducible polynomials have degree 1.

Proposition

If $\alpha \in \mathbb{C}$ is a root of $f(x) \in \mathbb{R}[x]$, then so is $\overline{\alpha}$.

Note. Sum and product of pair of conjugates are real. That is,

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}.$$

This can help us find roots in $\mathbb{C}[x]$.

Remark. It's better to work with monic polynomials and ignore multiply by units.

Theorem: 23.11: Gauss's Lemma special case

Let $f(x) \in \mathbb{Q}[x]$ (but with integer coefficients). If $f(x) = g(x)h(x)$, where $g, h \in q[x]$ with lower degrees, then it is possible to factor $f(x) = a(x)b(x)$ with $a(x), b(x) \in \mathbb{Z}[x]$ with lower degrees.

Example. $x^4 + 1 \in \mathbb{Q}[x]$ is irreducible. Reduce to degree 2 in $\mathbb{R}[x]$ and to degree 1 in $\mathbb{C}[x]$. In general for degree 4 polynomial, we can have irreducible quartic, irreducible cubic+linear, irreducible quadratic, 1 quadratic two linear, and 4 linear.

Example. Consider $x^2 - 5x + 6 \in \mathbb{Q}[x]$. The lemma ensures that we can factor into $(x - 2)(x - 3)$ with integer coefficients.

Example. There is a quick way to show $x^4 + 1 \in \mathbb{Q}[x]$ is irreducible using Gauss's lemma.

If x^4+1 can be factorized, it can be factorized over $\mathbb{Z}$.

$$\begin{aligned} x^4+1 &= (x^2+ax\pm 1)(x^2-ax\pm 1) \text{ since } a+b=0 \\ &= x^2 \pm (2\mp a^2)x+1 \end{aligned}$$

But either case wouldn't work because $2-a^2 \neq 0, -2-a^2 \neq 0$ since coefficient of x^3, a, is zero.

Theorem

Let $f(x) \in \mathbb{Q}[x]$ and coefficients are integers (we can always obtain this by multiplying by units to find roots). Suppose

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

Suppose $\frac{p}{q} \in f(x)$ is a root in $\mathbb{Q}$ of $f(x)$ and that $\frac{p}{q}$ is in lowest terms *i.e.* $\gcd(p,q)=1$. Then the numerator of the root divides the constant term and the denominator of the root divides the leading coefficient.

Proof

$$a_n\left(\frac{p}{q}\right)^n + \ldots + a_0 = 0$$
$$a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 p q^{n-1} + a_0 q^n = 0 \text{ multiply by } q^n$$

1st term is a multiple of q since everything else is multiple of q. Similarly, last term is a multiple of p since everything else is a multiple of p. So $q/a_n p^n$, since $\gcd(q,p)=1 \Rightarrow \gcd((q,p^n)=1$.

Claim. If a/bc and $\gcd(a,b)=1$, then a/c.

So we have q/a_n. Similarly, $\gcd((p,q^n), p/a_0q^n \Rightarrow p/a_0$. $\square$

Example. $3x^3-4x+6 \in \mathbb{Q}[x]$. Prove this is irreducible. We can think of roots because it has degree 3.

Suppose $\frac{p}{q} \in \mathbb{Q}$ is a root. Then $q/3, p/6, \gcd(p,q)=1$. Then $q \in \{\pm 1, \pm 3\}$ but we can assume $q>0$. And $p \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. So the candidates for roots are

$$\pm 1, \pm 2, \pm 3, \pm 6, \pm\frac{1}{3}, \pm\frac{2}{3}.$$

Theorem: Eisenstein Criterion

Let $f(x) \in \mathbb{Q}[x]$ with integer coefficients:

$$f(x) = a_n x^n + \ldots + a_1 x + a_0.$$

If there exists a prime such that p doesn't divide a_n, p^2 doesn't divide a_0, but p divides every other coefficients, then $f(x)$ is irreducible over $\mathbb{Q}[x]$.

Note. Eisenstein works for any degree.

Example. Using Eisenstein for the above example, we can try $p = 2$ and it works.

Example. $25x^5 - 9x^4 - 3x^2 - 12$. Take $p = 3$ and it works so it's irreducible. "It's Eisenstein by $p = 3$.

Example. $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ is irreducible. This equals to $\frac{x^5-1}{x-1}$. Change $x - 1$ to y, so x becomes $y + 1$. And

$$\begin{aligned}\frac{x^5 - 1}{x - 1} &= \frac{(y+1)^5 - 1}{y} \\ &= y^4 + 5y^3 + 10y^2 + 10y + 5 \text{ using binomial theorem}\end{aligned}$$

This works because if p is prime, then the pth line of Pascal triangle are all multiples of p.

Theorem

$x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Q}[x]$ is irreducible for p prime.

Example.

$$\frac{x^6 - 1}{x - 1} = x^5 + x^4 + x^3 + x^2 + x + 1 = (x + 1)(x^4 + x^2 + 1).$$

Since we can always group them into two. This doesn't work.

Claim. Over $\mathbb{R}$, there is no irreducible polynomials of degree ≥ 3. For odd degree it's because of Calculus. For even degree we use complex conjugate, so two linear factors of complex conjugates already give us a degree two polynomial in $\mathbb{R}[x]$, and any even degree ≥ 4 would have some degree 2 polynomials as factors if we consider the complex roots.