UCD Math. Enrichment Programme 2019
Saturday April 27
Polynomials II.

In this lecture, the factorization of polynomials over the integers and rationals was discussed. The notes on this part are contained in pages 13 - 20 of the posted lecture notes for the April 6 lecture on Polynomials.

New material on Eisenstein's criterion and also on relating the coefficients of polynomials to the Newton power sums of their roots are presented here.

Examples

① $f(x) = x^3 + 6x^2 - 24x + 12$ is irreducible over the rationals as it satisfies Eisenstein's criterion with $p = 3$. (Not $p=2$ because of the 12 at the end).

② $x^4+2$ is irreducible over the rationals, as it satisfies Eisenstein's criterion with $p = 2$.

③ $x^2-8$ is irreducible (but does not satisfy Eisenstein's criterion) over $\mathbb{Q}$. Since it has degree 2, Gauss' Lemma says that if it can be factored over the rationals as a product of two polynomials of degree 1, then it can be factored as $(x-l_1)(x-l_2)$ with $l_1, l_2$ integers. The coefficient of $x$ is 0, so $l_2 = -l_1$ and $l_1^2 = 8$. This is a contradiction since $\sqrt{8}$ is not an integer.

(4) $x^4+4$ does not satisfy Eisenstein's conditions since for $p=2$, $p^2$ does divide 4. However $x^4+4 = x^4+4x^2+4-4x^2$ $= (x^2+2)^2 - (2x)^2 = (x^2-2x+2)(x^2+2x+2)$ is

(5) This example was first given by Eisenstein. Let $p$ be a prime and

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Then $f(x)$ is irreducible over the rationals.

<u>Solution</u>: Note that $f(x) = \dfrac{x^p - 1}{x - 1}$.

First consider $f(x+1) = \dfrac{(x+1)^p - 1}{x+1} = \dfrac{(x+1)^p - 1}{x}$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}.$$

Since $p$ is a prime, all the coefficients $\binom{p}{1}, \binom{p}{2}, \cdots, \binom{p}{p-1}$ are all integers divisible by $p$. To see this; for $1 \le j \le p-1$, $\binom{p}{j}$ is the number of ways of picking a team of $j$ people from $p$ people, so it is an integer. Also

$$\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{j(j-1)\cdots 2 \cdot 1}.$$

In cancelling terms from the numerator and denominators to get the fraction in lowest form, the $p$ does not cancel, since each factor $j, j-1, \cdots 2, 1$ are all less than $p$ and $p$ is prime. So after cancelling we get $pt$ for some integer $t$, since $\binom{p}{j}$ is an integer.

So $p$ divides $\binom{p}{j}$. The term $\binom{p}{p-1}$ $= \binom{p}{1} = p$ is not divisible by $p^2$.

Hence the conditions in Eisenstein's criterion are satisfied and therefore $f(x+1)$ is irreducible over the rationals.

Suppose for the sake of contradiction that $f(x)$ is reducible over the rationals, say $f(x) = g(x)\,h(x)$, where $g(x)$, $h(x)$ are polynomials of degree $r$, $p-1-r$, respectively with rational coefficients.

But then $f(x+1) = g(x+1)\,h(x+1)$, and $g(x+1)$, $h(x+1)$ have the same degrees as $g(x)$, $h(x)$, and they have rational coefficients. To see this last point, suppose $g(x) = b_0 x^r + b_1 x^{r-1} + \cdots + b_r$ where all $b_i$ are rational, then $g(x+1) = b_0(x+1)^r + b_1(x+1)^{r-1} + \cdots + b_r$. Now expand each $(x+1)^j = x^j + \binom{j}{1}x^{j-1} + \cdots + \binom{j}{j-1}x + 1$ and all the binomial coefficients involved

Substituting these expansions into the formula for $g(x+1)$, we get

$$g(x+1) = x^r + \gamma_1 x^{r-1} + \gamma_2 x^{r-2} + \cdots + \gamma_r ,$$

where each $\gamma_i$ is rational.

A similar argument shows that $h(x+1)$ has rational coefficients. But then the factorization $f(x+1) = g(x+1)h(x+1)$ contradicts the irreducibility of $f(x+1)$ over the rationals.

Hence $f(x)$ is irreducible over the rationals, as claimed.

(6) Suppose $p$ is a positive integer and $q > p+1$ a prime. Prove the polynomial

$$f(x) = x^n - px - q \text{ is irreducible}$$

over the rationals for every positive integer $n$.

<u>Proof</u> Using Gauss' Lemma, it suffices to show that $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two monic polynomials $g(x)$, $h(x)$ with integer coefficients and degree less than $n$.

Suppose that such a factorization is possible.

Suppose that $f(x) = g(x)\,h(x)$, where

$$g(x) = x^r + b_1 x^{r-1} + b_2 x^{r-2} + \cdots + b_r ,$$
$$h(x) = x^s + c_1 x^{s-1} + c_2 x^{s-2} + \cdots + c_s ,$$

where $1 \le r \le n-1$, $s = n-r$, and $b_1, \cdots, b_r, c_1, \cdots, c_s$ are all integers.

Comparing the coefficients of $x^0$ in the formula $f(x) = g(x)\,h(x)$, we get

$$-q = b_r c_s .$$

But $q$ is prime and $b_r, c_s$ both integers, so one of $b_r, c_s$ must be $\pm 1$. Say $b_r = \pm 1$.

Over the complex numbers, we can write

$$g(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)$$

for some complex numbers $\alpha_1, \cdots, \alpha_r$, and comparing the coefficient of $x^0$, we get

$b_r = (-1)^r \alpha_1 \cdots \alpha_r$, and taking absolute values, we get

$$1 = |b_r| = |\alpha_1| \cdots |\alpha_r| .$$

So, for some $j$, $|\alpha_j| \le 1$. But $f(\alpha_j) = 0$, so $\alpha_j^n - p\alpha_j = q$ and thus

$$q = |q| = |\alpha_j^n - p\alpha_j| \le |\alpha_j^n| + p|\alpha_j| \le 1 + p,$$

since $|\alpha_j| \le 1$, contradicting $q > p+1$.

Example. Let $f(x) = x^n + ax^{n-1} + b$, where $n > 1$, $b$ is prime and $a$ is an integer such that $b$ does not divide $a(a \pm 1)$.
Prove $f(x)$ is irreducible over the rationals.

Proof. Suppose for the sake of contradiction that $f(x)$ is reducible over the rationals. Then by Gauss' Lemma,

$$f(x) = g(x)\,h(x) \quad \ldots (1)$$

for some monic polynomials $g(x)$, $h(x)$, of degree $k$, $n-k$, for some integer $k$ with $1 \leq k < n$, with $g(x)$, $h(x)$ having integer coefficients.

Putting $x = 0$ in equation (1) gives

$$b = f(0) = g(0)\,h(0).$$

Since $b$ is prime and $g(0)$, $h(0)$ are integers, one of the numbers $g(0)$, $h(0)$ must be $\pm 1$. We may assume that $g(0) = \pm 1$.

Since $g(x)$ has degree $k$, we can find its roots $\alpha_1, \ldots, \alpha_k$ (in the complex numbers) so that

$$g(x) = (x - \alpha_1) \cdots (x - \alpha_k) \quad \ldots (2)$$

Since $\alpha_i$ is a root of $f(x) = 0$,

for $i = 1, 2, \cdots, k$, we have

$$\alpha_i^n + a\alpha_i^{n-1} + b = 0,$$

that is

$$\alpha_i^{n-1}(-a - \alpha_i) = b. \quad \ldots (3)$$

Multiply those equations together for $i = 1, 2, \ldots, k$. Notice that

$$(-a-\alpha_1)(-a-\alpha_2)\cdots(-a-\alpha_k)$$

$$= g(-a) \quad \text{by (2)}.$$

Also $g(0) = (-1)^k \alpha_1 \cdots \alpha_k$ and $g(0) = \pm 1$.

So $\alpha_1^{n-1}\alpha_2^{n-1}\cdots\alpha_k^{n-1} = (\alpha_1\alpha_2\cdots\alpha_k)^{n-1} = \pm g(0)^{n-1}$.

So (3) yields

$$g(-a) = \pm b^k. \quad \ldots (4).$$

Also $f(-a) = (-a)^n + a(-a)^{n-1} + b = b$

and $f(-a) = g(-a)\, h(-a)$.

Since $g(-a)$, $h(-a)$ are integers and $b$ is prime, we find $|g(-a)| = 1$ or $b$.

So (4) implies $|g(-a)| = b$ and that $k = 1$. But $k = 1$ implies that

$g(x) = x - \alpha_1$ and $\alpha_1$ is an integer.
Since $f(\alpha_1) = 0$, we have

$$\alpha_1^{n-1}(\alpha_1 + a) + b = 0 \quad \text{---}(5)$$

If $n > 2$, this implies that $\alpha_1^2$ divides $b$. Since $b$ is prime, $\alpha_1^2 = \pm 1$ and, since $\alpha_1$ is an integer, $\alpha_1 = \pm 1$ and $b$ divides $a + \alpha_1 = a \pm 1$. This contradicts our hypotheses. Suppose $n = 2$. Then $\alpha_1$ divides $b$ and since $b$ is prime, $\alpha_1 = \pm b$ or $\pm 1$. If $\alpha_1 = \pm 1$, we again get $b$ dividing $a \pm 1$, giving a contradiction. Suppose $\alpha_1 = \pm b$. Then (5) implies that

$$\pm(a \pm b) + b = 0$$

and thus that $b$ divides $a$, contrary to hypothesis. So we have reached a contradiction, as desired. Hence our assumption that $f(x)$ is reducible over the rationals is false. So $f(x)$ is irreducible over the rationals, as claimed.

## Relating roots of a polynomial to its coefficients.

Suppose $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ is a polynomial of degree $n$, so $a_0 \neq 0$.

Suppose the roots of the equation $f(x) = 0$ are $\alpha_1, \alpha_2, \cdots, \alpha_n$. Then we can factor $f(x)$ as

$$f(x) = a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

If we multiply out the right-hand-side, and compare coefficients we get:

Number of $x^{n-1}$: $a_1 = -a_0(\alpha_1 + \alpha_2 + \cdots + \alpha_n)$

$x^{n-2}$: $a_2 = +a_0(\alpha_1\alpha_2 + \cdots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \cdots + \alpha_{n-1}\alpha_n) = +a_0 \sum_{1 \le i < j \le n} \alpha_i\alpha_j$.

$x^{n-3}$: $a_3 = -a_0(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \alpha_1\alpha_2\alpha_n + \alpha_2\alpha_3\alpha_4 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n)$

$= -a_0 \sum_{1 \le i < j < k \le n} \alpha_i\alpha_j\alpha_k$

$\vdots$

$x^0$: $= (-1)^n a_0\alpha_1\alpha_2\cdots\alpha_n$.

If $f(x)$ is a monic polynomial (so $a_0 = 1$), we can write

$$f(x) = x^n - p_1 x^{n-1} + p_2 x^{n-2} - \cdots + (-1)^k p_k x^{n-k} + \cdots + (-1)^n p_n ,$$

where

$$p_1 = \alpha_1 + \cdots + \alpha_n ,$$

$$p_2 = \sum_{1 \le i < j \le n} \alpha_i \alpha_j ,$$

$$p_3 = \sum_{1 \le i < j < k \le n} \alpha_i \alpha_j \alpha_k ,$$

$$\vdots$$

$$p_n = \alpha_1 \alpha_2 \cdots \alpha_n .$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of the equation $f(x) = 0$.

The numbers $p_1, p_2, \ldots, p_n$ are called the elementary symmetric functions of $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Note in particular that $p_1$ is the sum of the roots and $p_n$ is the product of the roots of $f(x) = 0$.

Let $s_k = \alpha_1^k + \cdots + \alpha_n^k$ be the sum of the $k$th powers of the roots $\alpha_1, \cdots, \alpha_n$.
The numbers $s_k$ are called the <u>Newton power sums</u> of $\alpha_1, \cdots, \alpha_k$.

Note that $s_1 = p_1$, $s_1^2 = (\alpha_1 + \alpha_2 + \cdots + \alpha_n)^2$

$$= \alpha_1^2 + \alpha_2^2 + \cdots + \alpha_n^2 + 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \cdots + \alpha_2\alpha_n + \alpha_3\alpha_4 + \cdots + \alpha_{n-1}\alpha_n)$$

$= s_2 + 2p_2$, that is $s_2 - s_1^2 + 2p_2 = 0$.

$s_2 - s_1 p_1 + 2p_2 = 0$

Similarly one can check that

$$s_3 - s_2 p_1 + s_1 p_2 - 3p_3 = 0.$$

In general,

$$s_k - s_{k-1}p_1 + s_{k-2}p_2 - s_{k-3}p_3 + \cdots + (-1)^k k p_k = 0.$$

These equations are called <u>Newton's Identities</u>.

Notice in particular that they imply that if all the coefficients of the <u>monic</u> polynomial $f(x)$ are integers, then all the Newton power sums of the roots of $f(x) = 0$ are integers also.