Math 461 F **Spring 2011**
Descartes' Factor Theorem **Drew Armstrong**

Descartes' *La Géométrie* (1637) is the oldest work of mathematics that makes sense to our modern eyes, because it was the first work to use our modern symbolic notation. *La Géométrie* is famous for introducing the idea of coordinate geometry — indeed the "Cartesian" plane is named after Descartes — but it also contains an important result in the theory of polynomials, called the Factor Theorem. I will give a modern treatment of this result.

Let $\mathbb{F}$ be any field (if you don't like the word "field" you can think "number system") and let $\mathbb{F}[x]$ be the ring of polynomials with coefficients in $\mathbb{F}$ (if you don't like the word "ring" you can just ignore it). Then we have the following.

The Factor Theorem. Let $f(x) \in \mathbb{F}[x]$ be a polynomial of degree n and suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}$ (we say α is a root of $f(x)$). Then we can write

$$f(x) = (x - \alpha)g(x),$$

where $g(x) \in \mathbb{F}[x]$ is a polynomial of degree $n - 1$.

Proof. For any positive integer d we have

$$x^d - \alpha^d = (x - \alpha)\varphi_d$$

where $\varphi_d = x^{d-1} + x^{d-2}\alpha + x^{d-3}\alpha^2 + \cdots + x\alpha^{d-2} + \alpha^{d-1}$. To see this, just expand the right side and observe that all the terms cancel except $x^d - \alpha^d$. Now suppose that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_n \neq 0$. Since $f(\alpha) = 0$, we may write $f(x) = f(x) - f(\alpha)$. On the other hand, we have

$$\begin{aligned}
f(x) - f(\alpha) &= a_n(x^n - \alpha^n) + a_{n-1}(x^{n-1} - \alpha^{n-1}) + \cdots + a_1(x - \alpha) \\
&= a_n(x - \alpha)\varphi_n + a_{n-1}(x - \alpha)\varphi_{n-1} + \cdots + a_1(x - \alpha) \\
&= (x - \alpha)\left[a_n\varphi_n + a_{n-1}\varphi_{n-1} + \cdots + a_2\varphi_2 + a_1\right] \\
&= (x - \alpha)\left[a_n x^{n-1} + \text{ lower terms }\right].
\end{aligned}$$

$\square$

This result is really at the beginning of algebra, and it eventually leads to Galois theory. Let me present a few important consequences.

Corollary. Let $f(x) \in \mathbb{F}[x]$ have degree n. Then $f(x)$ has **at most n roots** in $\mathbb{F}$.

Proof. We will prove this by induction on n. It is certainly true for $n = 1$ since $ax + b = 0$ has the unique solution $x = -b/a$. Now let $f(x) \in \mathbb{F}[x]$ have degree $k \geq 2$. If $f(x)$ has zero roots, we are done. So suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}$. By the factor theorem we can write $f(x) = (x - \alpha)g(x)$, where $g(x) \in \mathbb{F}[x]$ has degree $k-1$. But now any **other** root of $f(x)$ must be a root of $g(x)$, and by induction $g(x)$ has at most $n-1$ roots. Hence $f(x)$ has at most n roots. $\square$

We say that a field $\mathbb{F}$ is algebraically closed if every polynomial $f(x) \in \mathbb{F}[x]$ of degree n has **exactly** n **roots** in $\mathbb{F}$. Note that the real numbers $\mathbb{R}$ are **not** algebraically closed because the polynomial x^2+1 has no real roots. It is a celebrated fact that that the complex numbers $\mathbb{C}$ **are** algebraically closed, which is called the Fundamental Theorem of Algebra. (I hope to present a proof in this course.)

Here is another important corollary of the Factor Theorem.

Corollary. Suppose that $f(x) = ax^2 + bx + c$ has roots r and s. Then

$$ax^2 + bx + c = a(x-r)(x-s).$$

As a consequence, we get $r + s = -b/a$ and $rs = c/a$.

Proof. Since $f(r) = 0$, the Factor Theorem says that $f(x) = (x-r)g(x)$, where $g(x)$ is a linear (degree 1) polynomial. Now we must have $g(s) = 0$ and the Factor Theorem implies that $g(x) = (x-s)h(x)$, where $h(x)$ is a degree 0 polynomial. That is, $h(x)$ is just a number, say $h(x) = C \in \mathbb{F}$. We conclude that

$$f(x) = C(x-r)(x-s) = Cx^2 - C(r+s)x + Crs.$$

But we already know that the coefficient of x^2 is a, hence $C = a$. $\square$

That is, the polynomial $(x-r)(x-s)$ is the **unique** polynomial with roots r and s. (We could multiply it by a constant, but in the theory of polynomials we don't really care about constant multiples.) Using the same method of proof, we could show the following.

Corollary. Let $f(x) \in \mathbb{F}[x]$ be a polynomial of degree n which has a full set of roots $r_1, r_2, \ldots, r_n \in \mathbb{F}$. It follows that

$$f(x) = C(x-r_1)(x-r_2)\cdots(x-r_n),$$

for some constant $C \in \mathbb{F}$.

[Note: The results on this handout are extremely important, and you should not pass the course if you do not understand them.]