Mathematics 4300 – Foundations of Algebra – Fall 1999

10. The Fundamental Theorem of Algebra. The fundamental theorem of algebra says that every polynomial over the field of complex numbers has a root. One reason this is so important is that it tells us that no vector space over the complex numbers can be a field. In other words it tells us that the complex numbers are the end of the road for number systems which are also fields. Of course we've now found all sorts of new ways of building fields via clock arithmetic and rational functions, but although they are very interesting and important, they aren't number systems.

A field F is **algebraically closed** if every polynomial in $F[x]$ has a root.

Observation: F is algebraically closed if and only if the linear polynomials in $F[x]$ are the only primes.

Proof: Suppose F is algebraically closed and $f(x)$ has degree 2 or more. Then $f(x)$ has a root r, so $x - r$ divides $f(x)$. So $f(x)$ is not prime.

On the other hand, suppose F is a field and the only primes in $F[x]$ are linear. Then any polynomial $f(x)$ factors all the way down to a product of linear factors, so $f(x)$ has a root...in fact, it may have many roots.

Examples of fields that are not algebraically closed:

(a) $x^2 - 2$ does not have a root in $\mathbf{Q}$.

(b) $x^2 + 1$ does not have a root in $\mathbf{R}$.

(c) $x^2 + x + 1$ does not have a root in $\mathbf{F}_2$.

Proposition: None of the finite fields is algebraically closed.

Proof: This is Euclid's argument! If F is a finite field, let $r_1, r_2, ..., r_n$ be all the elements of F. Then the polynomial:

$$f(x) = (x - r_1)(x - r_2)...(x - r_n) + 1$$

cannot have a root because $f(r) = 1$ for all elements $r \in F(!)$

In light of these examples, the following may be somewhat surprising:

The Fundamental Theorem of Algebra: $\mathbf{C}$ is algebraically closed.

A Pseudo-Proof: To give a satisfactory proof of this requires more mathematics than we have developed here. But using calculus of several variables, I will try to convince you that the theorem is true.

Let's first analyze how a polynomial in $\mathbf{R}[x]$ may not have a root. A polynomial $a_d x^d + a_{d-1}x^{d-1} + ...a_0$ with $a_d \neq 0$ will have a root if and only if the polynomial we get when we divide by a_d: $f(x) = x^d + \frac{a_{d-1}}{a_d}x^{d-1} + ... + \frac{a_0}{a_d}$ has a root. So we will concentrate on $f(x)$.

First, consider the case where d is odd. In this case,

$$\lim_{r\to-\infty} f(x) = -\infty \text{ and } \lim_{r\to+\infty} f(x) = +\infty$$

so by the intermediate value theorem, there must be some r so that $f(r) = 0$ (and there may be many!). In other words, $f(x)$ has a root.

The case where d is even is somewhat different since in this case:

$$\lim_{r\to-\infty} f(x) = +\infty \text{ and } \lim_{r\to+\infty} f(x) = +\infty$$

We can conclude from this that if $f(x)$ does not have a root, then $f(x)$ must have a minimum value, say at r, and that $f(r) > 0$. This is a critical point of the function $f(x)$. That is, $f'(r) = 0$ and nearby r, the function gets larger. For example, if:

$$f(x) = x^2 + 1$$

then $f'(x) = 0$ occurs at $x = 0$, and by the second derivative test, $f''(0) = 2$, so 0 is a local minimum. It is also an absolute minimum because there are no other critical points! Since $f(0) = 1 > 0$, there are no real roots.

In contrast, let's consider polynomials $f(z)$ as above, but belonging to $\mathbf{C}[z]$ (it is customary to use z instead of x when the field is $\mathbf{C}$). Then the absolute value $|f(z)|$ is a real number when z is a complex number, so we can think of:

$$|f| : \mathbf{R}^2 = \mathbf{C} \to \mathbf{R}$$

as a function from $\mathbf{R}^2$ to $\mathbf{R}$. This function is differentiable whenever $f(z) \neq 0$ but at a root of $f(z)$ it is not differentiable(!) We can analyze $|f|$ as we analyzed polynomials in $\mathbf{R}[x]$ of even degree. Namely, the value $|f(z)|$ is very large when $|z|$ is very large (that is, when z is outside a very large circle around 0) and it follows that $|f|$ **must** have a minimum somewhere.

Here is the part I am not going to prove for you:

All the critical points of $|f|$ are saddle points!

So where can the minimum be? Well, it has to be at a point where the function is not differentiable, that is, it has to be at a point where $f(z) = 0$. In other words, $f(z)$ **must have a complex root!**

Example: Think of $f(z) = z^2 + 1$. Then

$$|f(z)| = |(x+iy)^2 + 1| = \sqrt{((x^2 - y^2) + 1)^2 + 4x^2y^2}$$

has a critical point at 0 and $f(0) = 1$ as in the real case. But $f(\epsilon) = \epsilon^2+1 > 1$ and $f(\epsilon i) = 1 - \epsilon^2 < 1$ for (real) ϵ. That is, moving in the x direction lowers $|f|$ and moving in the y direction raises $|f|$. This is a saddle.

Corollary: Every polynomial in $\mathbf{C}[z]$ factors completely:

$$f(z) = a_d(z - r_1)(z - r_2)...(z - r_d)$$

where $r_1, ..., r_d$ are the roots of $f(z)$, and a is the coefficient of z^d

Proof: $f(z)$ has a root by the theorem, so $f(z) = (z - r_1)q_1(z)$, and likewise $q_1(z) = (z - r_2)q_2(z)$, etc. At the end, we have $q_{d-1}(z) = (z - r_d)a_d$.

Notice that there may be fewer than d roots of $f(x)$ because some of the $r_1, r_2, ..., r_d$ may be the same. But there can never be **more** than d roots of a polynomial of degree d. Also notice that the d roots of:

$$f(z) = z^d - a$$

are exactly the dth roots of a, which we found in our tour of the complex numbers. In that case, there were exactly d of them, and we could write them down explicitly. It is **much** harder to find the roots of an arbitrary polynomial. This will occupy the final five weeks of the course.

Before we do this, however, let's revisit the:

(End-of-the-Line) Theorem: The only finite dimensional vector spaces over $\mathbf{R}$ which are also fields are $\mathbf{R}$ itself and $\mathbf{C}$.

Step 1: Complex roots of real polynomials come in conjugate pairs.

That is, if $f(x) \in \mathbf{R}[x]$ and $f(s+it) = 0$, then $f(s-it) = 0$. We can see this by conjugating the whole polynomial:

$$0 = f(s+it) = a_d(s+it)^d + a_{d-1}(s+it)^{d-1} + ... + a_0, \text{ so}$$

$$0 = \overline{f(s+it)} = a_d\overline{(s+it)}^d + a_{d-1}\overline{(s+it)}^{d-1} + ... + a_0 = f(s-it)$$

because all the coefficients are real!

Consequence: Every prime in $\mathbf{R}[x]$ is either linear or quadratic.

Proof: Suppose $f(x)$ is a prime in $\mathbf{R}[x]$. Then $f(z)$ has a complex root. If the complex root is real, call it r. Then $x - r$ divides $f(x)$, so $f(x)$ must be linear, since it is prime. If the root is complex, call it $s + it$. Then $s - it$ is also a root by Step 1, so $(z - (s+it))(z - (s-it))$ divides $f(z)$. But:

$$(z - (s+it))(z - (s-it)) = z^2 - 2sz + (s^2 + t^2)$$

is in $\mathbf{R}[x]$. So $x^2 - 2sx + (s^2 + t^2)$ divides $f(x)$. So $f(x)$ must be quadratic!

Step 2: $f(x)$-clocks are always vector spaces over F.

Suppose $f(x) = a_dx^d + a_{d-1}x^{d-1} + ... + a_0$. Then I claim that the $f(x)$ clock is a vector space with basis $1, x, x^2, ..., x^{d-1}$. To see this, we just have to remember what this clock is(!) Namely, the elements of the $f(x)$-clock are the remainders when polynomials are divided by $f(x)$. That is, they are all the polynomials of degree $d-1$ or less. But of course these polynomials form a vector space, with basis $1, x, x^2, ..., x^{d-1}$, since addition of the remainder polynomials in the $f(x)$-clock is just ordinary addition!

This means that we can write down multiplication tables for our clocks, even over infinite fields by simply multiplying the basis elements.

Example: $x^3 - 2$-clock over $\mathbf{Q}$:

$\times$	1	x	x^2
1	1	x	x^2
x	x	x^2	-2
x^2	x^2	-2	$-2x$

Example: $x^2 + 1$-clock over $\mathbf{R}$:

$\times$	1	x
1	1	x
x	x	-1

Does this look familiar? It ought to. It is the multiplication table for $\mathbf{C}$!

Step 3: The only finite dimensional vector space over $\mathbf{C}$ which is also a field is $\mathbf{C}$ itself.

Proof: Suppose V is a finite dimensional vector space over $\mathbf{C}$ and a field. Choose a vector $v \in V$. Then we know that the set of vectors:

$$\{1, v, v^2, v^3, ...\}$$

eventually becomes linearly dependent, because V is finite dimensional. Let v^d be a power so that the sequence is linearly dependent. Recall that linear dependence means there are complex numbers $a_0, a_1, a_2, ..., a_d$ so that:

$$f(v) = a_d v^d + a_{d-1} v^{d-1} + ... + a_0 = 0$$

In other words, v is a root of $f(v)$. But $f(v)$ factors completely, telling us that:

$$0 = a_d(v - r_1)(v - r_2)...(v - r_d)$$

for complex numbers $a_d, r_1, ..., r_d$. But V is a field! So the only way we could have $v - r_1$ as a divisor of zero would be if $v - r_1 = 0$. In other words, $v = r_1$. But then all vectors are complex multiples of 1, which is to say that $V = \mathbf{C}$.

Step 4: $\mathbf{C}$ is the only 2-dimensional vector space over $\mathbf{R}$ which is also a field.

Proof: Suppose V is a 2-dimensional vector space over $\mathbf{R}$ which is also a field. Choose a vector $v \in V$ which is not a multiple of 1. Then $1, v, v^2$ must be dependent, satisfying:

$$0 = f(v) = av^2 + bv + c$$

for coefficients $a, b, c \in \mathbf{R}$. Of course, this polynomial cannot factor over $\mathbf{R}$ because if it did, we'd have $v = r$, violating the choice of v. So $f(x)$ is prime in $\mathbf{R}[x]$, and in fact V **is** the $f(x)$-clock, with multiplication table:

$\times$	1	x
1	1	x
x	x	$-\frac{b}{a}x - \frac{c}{a}$

In this case, it is not clear at all that this clock is actually $\mathbf{C}$ in disguise, but it is. And we see this by **changing basis**. Namely, instead of v, choose the vector:

$$w = \frac{2a}{\sqrt{4ac - b^2}} \left(v + \frac{b}{2a} \right)$$

(since $f(v)$ has no real roots, $4ac - b^2$ is positive!)

Then $w^2 = -1$, as the reader is invited to check, and with this choice of w, we get:

$$0 = g(w) = w^2 + 1$$

showing that V **is** the $g(w)$-clock, which **is** $\mathbf{C}$!

Last Step: Proof of the End-of-the-Line Theorem.

Suppose now that V is a finite-dimensional vector space over $\mathbf{R}$ which is also a field. If $V = \mathbf{R}$, there is nothing to show. Otherwise, there is a $v \in V$ which is independent of 1. Take the **smallest** power d so that:

$$\{1, v, v^2, ..., v^d\}$$

is linearly dependent. Then v satisfies a polynomial:

$$0 = f(v) = a_d v^d + a_{d-1} v^{d-1} + ... + a_0$$

and I claim that $f(x)$ is prime! If it were not, then $f(x) = p(x)q(x)$ would give us $p(v) = 0$ or $q(v) = 0$ and linear dependence for a smaller power of v.

But the only prime polynomials (other than the linear ones) in $\mathbf{R}[x]$ are quadratic, by Step 1. So $f(x)$ has degree 2. Now the $f(x)$-clock is a vector space over $\mathbf{R}$ of dimension 2 by Step 2. It is $\mathbf{C}$ by Step 4. This means that the subspace spanned by 1 and v in V is the field $\mathbf{C}$. But this also means that V itself is a vector space over $\mathbf{C}$. By Step 3, this means that V must be **equal** to $\mathbf{C}$, and we are done! Whew!

Exercises.

1. (a) If V is a vector space of dimension n over field with k elements, then how many elements are there in V?

(b) Suppose F is a finite field and $1 + 1 = 0$ in F. Conclude that the number of elements in F is 2^n for some n.

(c) Suppose F is any field with 9 elements. Show that $1+1+1 = 0$ in F.

(d) Suppose F is any field with 16 elements. Show that $1 + 1 = 0$ in F

(e) Show that there is no field with 6 elements.

2. Show that $x^2 - 2$ still does not have a root in the $x^2 + 1$-clock over $\mathbf{Q}$. Hence this clock is **not** algebraically closed. (Unlike the same clock over $\mathbf{R}$.)

3. Suppose $f(x)$ is a polynomial in $\mathbf{R}[x]$ and r is a (real) root.

(a) Show that $f'(r) = 0$ if and only if $(x - r)^2$ divides $f(x)$

(Hint: Use Leibniz's rule on $f(x) = (x - r)q(x)$)

(b) Show that if $f'(r) \neq 0$ and $f(x)$ has even degree, then $f(x)$ must have another real root different from r.

4. (a) Factor $x^4 - 2$ completely in $\mathbf{R}[x]$.

(b) Prove that $x^4 - 2$ is prime in $\mathbf{Q}[x]$.

(c) Write out the multiplication table for the $x^4 - 2$-clock, which is a field and a vector space of dimension 4 over $\mathbf{Q}$.