Polynomials over **F**

Professor K. A. Ribet

October 10, 2025

Office hours

My office hours are Mondays 1:30–3 PM and Thursday 10:30 AM–noon in 732 Evans.

Week of October 20

- Math Monday talk on Fermat's Last Theorem, 5–6 PM, 1015 Evans
- Academic Empowerment Series event on office hours, 8–10 PM, Anchor House
- I'm teaching Math 113, TuTh, 2:10–3:30 PM, 155 Dwinelle

Factorization of integers

After a discussion about the analogy between integers and polynomials, this is the last thing that we saw on the screen on Wednesday:

Theorem (Fundamental theorem of arithmetic)

Every integer $\neq 0, 1, -1$ *is* $\pm$ *the product of prime numbers. The factorization of an integer into such a product in unique, up to permutation of the prime factors.*

This theorem is proved in Math 55. The same proof yields a unique factorization theorem for polynomials.

Integers $\longleftrightarrow$ polynomials

On Wednesday, I explained the analogy between (the ring of) integers and (the ring of) polynomials. Recall:

An *irreducible polynomial* is a nonconstant polynomial that does not factor into a product of two nonconstant polynomials. Irreducible polynomials are like the prime numbers, except that usually we insist that prime numbers be *positive*. In analogy, we insist that irreducible polynomials be *monic*. The monic irreducible polynomials over **F** are then like the prime numbers. Among the polynomials, the *units* are the nonzero constants. These are the polynomials that have polynomial inverses.

Factorization of polynomials

Theorem

Each polynomial $\neq 0$ or a unit is a unit times some product of monic irreducible polynomials. Factorizations of such polynomials are unique up to the order of the factors.

The proof is the same as for integers $\neq 0, 1, -1$. It's all the Euclidean algorithm, as seen in Math 55.

Roots and divisors

Imagine division of polynomials by a polynomial $z - \lambda$, of degree 1. If p is a polynomial, then $p = q(z - \lambda) + r$, where the remainder r is a "polynomial" of degree ≤ 0 and thus a constant. Make the substitution $z = \lambda$ to obtain $p(\lambda) = r$.

This thought experiment shows that the value of a polynomial at a number λ is the remainder when the polynomial is divided by $z - \lambda$. Thus the value is 0 when the division is exact.

Proposition (4.6)

The linear factor $z - \lambda$ divides a polynomial if and only if λ is a root of the polynomial.

Polynomials

Proposition (4.6)

The linear factor $z - \lambda$ divides a polynomial if and only if λ is a root of the polynomial.

Corollary (4.8)

A polynomial of degree m has at most m roots.

A polynomial with distinct roots $\lambda_1, \ldots, \lambda_d$ is divisible by $(z - \lambda_1) \cdots (z - \lambda_d)$ and thus has degree $\geq d$ if it's nonzero.

Consequence: polynomial that's identically 0 as a function is the 0 polynomial. Indeed, a nonzero polynomial some degree m and then cannot have more than m roots. A polynomial that's identically zero has infinitely many roots!

Fundamental theorem of algebra

Theorem

A nonconstant polynomial over **C** *has at least one root.*

A telegraphic proof of this theorem is on page 125 of LADR. Last semester, I wrote a more detailed version of the proof. You'll find it in `Files` on `bCourses`.

A restatement:

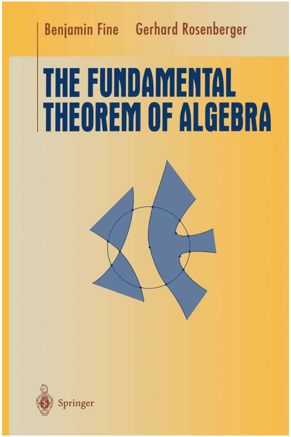
Theorem

The irreducible polynomials over **C** *have degree 1. The monic irreducible polynomials over* **C** *are of the form* $z - \lambda$*, with* λ *in* **C**.

Fundamental theorem of algebra

You can grab this book for free if you're in `berkeley.edu`. Just click on the image to get to the right web page.

Proofs of the Fundamental Theorem are usually given in Math 185. Axler's proof uses "only" Math 104.


Benjamin Fine Gerhard Rosenberger
THE FUNDAMENTAL THEOREM OF ALGEBRA
Springer

Summary of Axler's proof

Lemma

All complex numbers have complex kth roots for all $k \geq 1$.

Proof: Since 0 has the kth root 0, we can consider only nonzero complex numbers. If $z \neq 0$, $z \in \mathbf{C}$, then $z = |z| \cdot \dfrac{z}{|z|}$. The first factor is a positive real number and thus has a kth root. The second factor has absolute value 1. Thus it suffices to find kth roots of complex numbers of absolute value 1. These numbers lie on the unit circle in the complex plane and are of the form $e^{i\theta}$. A kth root of $e^{i\theta}$ is $e^{i\theta/k}$.

Summary of Axler's proof

Axler's proof starts with a nonconstant polynomial f. We want to prove that f has a root. We can divide f by its top coefficient without changing anything of significance. Then $f = z^n +$ lower-degree terms for some $n \geq 1$. It should be clear to all that $|f(z)| \to \infty$ as $|z| \to \infty$.

Choose a (random) complex number a and let $M = |f(a)|$. If $M = 0$, a is a root of f and we're done.

Suppose that M is positive. Then we can find some radius $R > 0$ so that $|z| \geq R$ implies $|f(z)| \geq 2M$. A consequence is that all values of $|f|$ less than or equal to M occur on the disc $D = \{\, z \in \mathbf{Z} \mid |z| \leq R \,\}$. The aim is to show that 0 is one of those values.

Summary of Axler's proof

The big gun here is Math 104, which will imply that the set of values $|f(D)|$ is a closed interval $[A, B]$ with $A \leq B$ and A, B nonnegative real numbers. Once again, the aim is to show that $A = 0$.

The proof is by contradiction: Assuming that A is positive, we make estimates to show that there is some value of $|f|$ that's less than A. In this final step, we use the lemma about kth roots.

Irreducible polynomials over **R**

What are the monic irreducible polynomials over **R**?

The degree 1 polynomials $z - \lambda$ with $\lambda \in \mathbf{R}$ are irreducible.

By the quadratic formula (or completing the square), a quadratic polynomial $z^2 + bx + c$ factors into two linear factors if $b^2 - 4c$ is nonnegative. If instead $b^2 - 4c$ is *negative*, then the polynomial has two complex (non-real) roots and thus is not the product of two degree 1 factors over **R**.

Thus the real quadratic polynomials with negative discriminants are irreducible polynomials over **R**.

Proposition (4.16)

The monic irreducible polynomials over **R** are the $z - \lambda$ wth $\lambda \in \mathbf{R}$ and the $z^2 + bz + c$ with $b, c \in \mathbf{R}$ and $b^2 - 4c < 0$.

Linear, irreducible quadratic — we've seen all the irreducibles.

How come?

Odd degree real polynomials have roots

This is a digression:

Suppose that $p(z) = z^n + a_{n-1}z^n + \cdots + a_0$ is a monic real polynomial with n odd. In calculus, we learn that $p(z) \to +\infty$ as $z \to +\infty$ and $p(z) \to -\infty$ as $z \to -\infty$. Graphing p, we see that it crosses the z-axis. In other words, it has a root.

Only in Math 104 do we prove the Intermediate Value Theorem, which guarantees that p has a root. Let's stipulate that we have taken or will take Math 104.

Because p has a root, it has a linear factor. Thus it is reducible (i.e., not irreducible) if its degree is bigger than 1.

Conclusion: Odd degree real polynomials are irreducible only when they have degree 1. This is consonant with the claim on a previous slide.

Even degree polynomials?

Proposition (4.16)

The monic irreducible polynomials over **R** are the $z - \lambda$ wth $\lambda \in$ **R** and the $z^2 + bz + c$ with $b, c \in$ **R** and $b^2 - 4c < 0$.

To prove the proposition, we need to show that polynomials of degrees > 2 are reducible even if the degrees are even. For example, how do we know that there are no irreducible quartic polynomials over **R**?

A quick discussion

Let p be a real polynmial of degree > 1. If it has a root, then it's divisible by some $z - \lambda$ and is therefore reducible. So let's assume that it has no real root.

By the Fundamental Theorem of algebra, p has a *complex* (but non-real) root λ. Thus $p(\lambda) = 0$. Use $\overline{\quad}$ for complex conjugation and note that conjugation respects addition and multiplication. We discover that

$$0 = \overline{p(\lambda)} = p(\overline{\lambda})$$

because the coefficients of p are real. Since $\overline{\lambda} \neq \lambda$, p is divisible by the quadratic polynomial $(z - \lambda)(z - \overline{\lambda})$, which is a real polynomial!

If p has degree > 2, it has a degree 2 factor, which makes it reducible. As I'll explain in class, the polynomial $p[(z - \lambda)(z - \overline{\lambda})]^{-1}$ is actually a real polynomial (whereas you might worry that it has complex coefficients).

Hurray, we’re done chatting about polynomials.

Let’s move to Chapter 5!

Eigenvalues and eigenvectors

To be faithful to LADR, I'll repeat some terminology at the start of Chapter 5:

A linear map $T : V \to V$ is called an *operator* on V. We've already used the term.

If $U \subseteq V$ is a subspace and T is an operator on V, one can ask whether $T(U) \subseteq U$, which means "$Tu \in U$ for all $u \in U$." A subspace with this property is said to be *invariant* under T.

Examples: The null space of an operator T is T-invariant, and so is the range of T. The subspace $\{0\}$ and the full space V are also invariant under T.

Cyclic subspaces

If v is an element of V, there is a smallest T-invariant subspace of V that contains v: it's the intersection of all such subspaces.

We'll study it next week, but here's a brief description: it's the span of v, Tv T^2v,$\ldots$, T^nv, where $n = \dim V$.

Here, $T^2 = T \circ T$, $T^3 = T \circ T \circ T$, etc. More generally, if p is a polynomial, we can form $p(T)$:

$$p(z) = a_0 + a_1 z + \cdots + a_d z^d \quad \rightsquigarrow \quad p(T) = a_0 I + a_1 T + \cdots + a_d T^d.$$

One-dimensional invariant subspaces?

Suppose that T is an operator on V and that $U \subseteq V$ is a 1-dimensional subspace of V. Then $U = \mathbf{F} \cdot v$ for some nonzero $v \in V$. If U is T-invariant, then $Tv \in U$, so that $Tv = \lambda v$ for some scalar λ.

Conversely, it $Tv = \lambda v$ for some $\lambda \in \mathbf{F}$, then the line $\mathbf{F} \cdot v$ is T-invariant.

A *nonzero* vector v is an *eigenvector* for T if $Tv = \lambda v$ for some scalar λ.

The scalar λ is unique if it exists — it's the *eigenvalue* for the eigenvector v.

Eigenvalues, eigenvectors

We say that λ is an eigenvalue for T if there is some nonzero $v \in V$ such that $Tv = \lambda v$. Thus λ is an eigenvalue for T if the operator $T - \lambda I$ has a nonzero null space. (Here, I is the identity map $V \to V$.)

If V is finite-dimensional (as it is most of the time), $T - \lambda I$ has a nonzero null space $\iff$ $T - \lambda I$ is not invertible.