Lecture: Mon 8/29/05

1. $\mathbb{N} := \{0, 1, 2, \dots\}$ natural numbers (whole numbers)

   - "God made the whole numbers; all the rest is the work of man."
   - operations $\implies$ solving equations $\implies$ inverse operations $\implies$ new number systems
   - accounting $\implies$ algebra:
     8 sheep, 3 born, how many?
     addition operation: $x = 8 + 3 = 11$
   - 11 sheep, 5 male, how many female?
     $y + 5 = 11$, $y = 11 - 5 = 6$ (inverse to + op)
   - 11 sheep, king wants 15 for taxes, how many left?
     $z + 15 = 11$, $z = 11 - 15 = -4$, debt of 4 sheep
     new type of number, has meaning in original context
   - $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ integers (from German *Zahl*)

2. $\mathbb{Q}$ rational numbers

   - 300 peasants, 15 sheep each in taxes, how much revenue?
     multiplication operation: $u = 300 \times 15 = 4500$
   - 4500 revenue, 160 soldiers, how much for each?
     $4500/60 = 225/8 = 28 + \frac{1}{8}$ fraction
   - $\mathbb{Q} = \{\, a/b \text{ with } a, b, \in \mathbb{Z}\,,\ b \neq 0 \,\}$ rational numbers (fractions)

   - make definitions for $\mathbb{Q}$ in terms of known terms for $\mathbb{Z}$
     equality of fractions: $a/b = c/d \iff ad = bc$
     addition of fractions: $a/b + c/d := (ad + bc)/bd$

3. $\mathbb{R}$ real numbers

   - square field has area, 200 yd^2, side is how long?
     $s^2 = 200$, $s = \sqrt{200} = 10\sqrt{2}$.
   - Proposition: $\sqrt{2} \notin \mathbb{Q}$: that is, $(a/b)^2 \neq 2$ for all $a/b \in \mathbb{Q}$
   - Lemma: a^2 even $\implies$ a even
     Proof of Lemma: if even $a = 2n$, then $a^2 = 4n^2$ even; if odd $a = 2n+1$, then $a^2 = 4n^2+4n+1 = 2(2n^2+2n)+1$ odd.
   - Proof of Proposition: Suppose $a/b \in \mathbb{Q}$ in lowest terms, so a, b are not both even. Suppose $(a/b)^2 = 2$, so that $a^2 = 2b^2$ is even. By the Lemma, $a = 2n$ is even, so $2b^2 = (2n)^2 = 4n^2$ and $b^2 = 2n^2$ is even. By the Lemma, b is also even, so we could not have *any* solution a/b in lowest terms.

- solve $x^2 = c \quad \Longrightarrow \quad$ solve $ax^2 + bx + c = 0$
  Complete-the-square trick: Rewrite eqn as $x^2+(b/a)x+(c/a) = 0$. If $2d = b/a$ then:

$$(x+d)^2 - d^2 + \frac{c}{a} = x^2 + \frac{b}{a}x + \frac{c}{a} = 0$$

  Now we can solve $(x+d)^2 = d^2 - c/a$, so $x = -d \pm \sqrt{d^2 - c/a}$ for $d = b/2a$. Work out the usual quadratic formula.

4. $\mathbb{C} = \{\, a + ib \;\text{ for }\; a, b \in \mathbb{R}\,\}$, complex numbers

   - solve $x^2 + 1 = 0$ gives new number $i = \sqrt{-1}$
   - can define operations on numbers $a + bi$ for $a, b \in \mathbb{R}$ in terms of known operations on $\mathbb{R}$.
     $(a + bi)(c + di) = ac + i^2bd + iad + ibc = (ac - bd) + i(ad + bc)$
   - can now solve $x^2 = -a$: $\;x = \sqrt{-a} = i\sqrt{a}$ for $a \geq 0$.
   - can now solve $ax^2 + bx + c = 0$ for *any* $a, b, c \in \mathbb{R}$ (even if no real solution): quadratic formula
   - Fundamental Theorem of Algebra: Any polynomial equation

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$$

     with coefficients $a_0, a_1, \ldots, a_n \in \mathbb{C}$ has at least one solution $x = a + bi \in \mathbb{C}$.
   - Thus, the process of finding more general number systems to solve equations ends with $\mathbb{C}$.

Lecture: Mon 8/31/05

1. Pythagorean triples

   - Number theory: properties of integers $\mathbb{Z}$
     finding integer solutions to equations
   - Example: Pythagorean triples
     all 3 sides of a right triangle are whole numbers
     solve $a^2 + b^2 = c^2$ for integers $a, b, c > 0$.
   - Let $x = a/c$, $y = b/c$, then solve:
     $x^2 + y^2 = 1$ for rational numbers $x, y \in \mathbb{Q}$.
     find rational points (x, y) on unit circle
   - Projection of circle from $(-1, 0)$ to line $x = 1$:
     miraculously, rational points $(1, t)$ on line
     correspond one-to-one with rational points (x, y) on circle
   - E.g. $t = \frac{3}{2}$, line between $(1, t)$ and $(-1, 0)$ is $y = \frac{3}{4}(x+1)$
     intersect with $x^2 + y^2 = 1 \implies 1 - x^2 = \frac{9}{16}(x+1)^2$
     $\implies 1 - x = \frac{9}{16}(x+1) \implies (x, y) = (\frac{7}{25}, \frac{24}{25})$
     $\implies (a, b, c) = (7, 24, 25)$.

2. Prime factorization of integers

   - divisibility: $a|b \iff b = ac$ for some $c \in \mathbb{Z}$
     a is a factor of b , a divides b , b is divisible by a
   - prime p means only possible factors $d|p$ are $d = 1, p$
     convention: 1 is *not* a prime
   - Fundamental Theorem of Arithmetic (Unique Factorization):
     Any positive integer n can be factored into primes: $n = p_1 p_2 \cdots p_r$.
     This can be done in only one way (except for the order of the factors).

3. Greatest common divisor

   - $\gcd(a, b) = \max\{\, d$ such that $d|a$ and $d|b \,\}$
   - Euclidean algorithm to find $\gcd(a, b)$
     Example: $(a, b) = (36, 15)$
     repeat division with remainder until remainder is 0:

$(36, 15)$	$36 = 2(15) + 6$	$3 \mid 36$
$(15, 6)$	$15 = 2(6) + 3$	$3 \mid 15$
$(6, 3)$	$6 = 2(3) + 0$	$3 \mid 6$

- Claim: (i) $3|36$ and $3|15$ (ii) $d|36$ and $d|15 \implies d|3$
  Proof of (i): clear from above.
  Proof of (ii): $3 = 2(6) - 15$, $6 = 2(15) - 36$
  so back-substitute: $3 = 2(2(15) - 36) - 15 = -36 + 3(15)$
  Since $3 = \ell(36) + m(15)$, if $d|36$ and $d|15$, then $d|3$.

4. General Euclidean Algorithm to find $\gcd(a, b)$

   - $x_0 := a$, $x_1 = b$, repeat division with remainder:
     $x_0 = q_1x_1 + x_2$, $x_1 = q_2x_2 + x_3$, $\cdots$, $x_{n-1} = q_nx_n + 0$
   - Proposition: $x_n = \gcd(a, b)$.
   - Claim: (i) $x_n|a$ and $x_n|b$ (ii) $x_n = \ell a + mb$ for $\ell, m \in \mathbb{Z}$
   - Prove Claims just as in above example, and prove Proposition using Claims.

5. Lemma: For p a prime: $p|ab \implies p|a$ or $p|b$.

   - Proof: Let $d = \gcd(p, a)$. Since $d|p$, we have $d = p$ or $d = 1$. If $d = p$, then $p|a$, OK. If $d = 1$, then $1 = d = \ell p + ma$, so $b = \ell pa + mab$. Since $p|\ell pa$ and $p|abm$, we have $p|b$, OK.

6. Proof of Fundamental Theorem of Arithmetic

   - Obviously there is some factorization of n into primes: keep factoring until factors are prime. But why unique (except for rearrangement)?
   - Suppose $p_1 \cdots p_r = q_1 \cdots q_s$. Then $p_1|q_1(q_2 \cdots q_s)$. Use Lemma: if $p_1|q_1$, then $p_1 = q_1$. If $p_1|q_2 \cdots q_s$, repeat to get $p_1 = q_2$ or $p_1|q_3 \cdots q_s$. In the end, we find $p_1 = q_i$ for some i.
   - Removing $p_1 = q_i$ from both sides of the product, get: $p_2 \cdots p_r = q_1 \cdots q_{i-1}q_{i+1} \cdots q_s$.
     Now repeat to find $p_2 = q_j$, and remove this factor from both sides, etc.
   - This process ends when there are no more primes on right or left side, leaving 1. But this means the product of remaining primes on the other side is 1, so the other side must have no primes left either. Thus $r = s$.
   - In the end, we find the list $p_1, \ldots, p_r$ is a rearrangement of the list $q_1, \ldots, q_s$, so factorization is unique.

Math 418H **Fall 2005**

Lecture: Wed 9/7/05

1. Fundamental Theorem of Arithmetic (Unique Factorization)

    - Any positive integer n can be expressed *in only one way* as:

    $$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

    for some primes $p_1, \ldots, p_r$ and integers $k_1, \ldots, k_n \geq 0$. That is, n can be uniquely identified by how many powers of each prime divide it.

    - Proof: Division algorithm $\implies$ Euclidean algorithm for gcd $\implies$ Key property of primes (if $p|ab$ then $p|a$ or $p|b$) $\implies$ Fundamental Theorem

    - Proposition: If $m/n \in \mathbb{Q}$ is in lowest terms, and $\sqrt{m/n} \in \mathbb{Q}$, then $\sqrt{m}, \sqrt{n} \in \mathbb{Z}$.
    Proof: Suppose a/b in lowest terms with $\sqrt{m/n} = a/b$. Let $p_1, \ldots, p_r$ be all the primes which divide any one of a, b, m, n, and write: $a = p_1^{a_1} \cdots p_r^{a_r}$, $b = p_1^{b_1} \cdots p_r^{b_r}$, etc. Now write out $a^2\, n = b^2\, m$ in terms of prime products, and show that $m = a^2$ and $n = b^2$.

2. Sieve of Eratosthenes to list primes

    - Make list of numbers 1,2, ... ,n. Cross out 1 (not a prime). Circle first uncrossed number 2, cross out all multiples of 2. Again circle first uncrossed number 3, cross out all multiples of 3. Repeat until all numbers are circled or crossed out: circled ones are the primes.

    - In fact, after you circle a given prime p, the first new number you cross out will be p^2. Thus, you can stop crossing out when $p^2 > n$, and just circle all remaining numbers. (Thanks to Benjamin Osborn & Alan Kish for the explanation.)

3. The sequence of primes

    - p = 2, 3, 5, 7,, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

    - Theorem: There exist infinitely many primes.
    Proof (Euclid): Consider any list of primes: $p_1, p_2, \ldots, p_r$, and let $n := p_1 p_2 \cdots p_r + 1$. Now if $p_i | n$, then $p_i | (n - p_1 \cdots p_r) = 1$, but no prime divides 1, so this is impossible. Thus the prime factors of n are different from $p_1, \ldots, p_r$, and we can extend our list with new primes. Repeating, we can extend the list indefinitely.

- Example: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$, so the new primes are 59 and 509. We skip over many primes this way, but we do get an infinite list.
- Fermat's formula: $F(n) = 2^{2^n} + 1$ takes values: $F(0) = 3$, $F(1) = 5$, $F(2) = 17$, $F(3) = 257$, which are all prime. Fermat conjectured $F(n)$ is always prime, but this is false. Primes $p = F(n)$ are called Fermat primes, but only 5 such p are known! (What are they?)
- Is there any formula $f(n)$ giving only primes? None is known.

4. Prime Number Theorem

- Let $p_n =$ the n^{th}-largest prime; and $\pi(n) :=$ the number of primes $\leq n$.
- For two sequences $f(n), g(n)$, we write $f(n) \approx g(n)$ to mean that the percentage difference between the two sides approaches zero for large n:

$$\lim_{n \to \infty} \frac{f(n)}{g(n)} = 1 .$$

- Theorem:

$$p_n \approx n \log(n) \qquad \text{and} \qquad \pi(n) \approx \frac{n}{\log(n)} ,$$

  where log means natural logarithm (base e).
- Proof uses sophisticated complex analysis, encoding the sequence of primes in terms of the Riemann zeta function

$$\zeta(s) := \prod_{p \text{ prime}} \frac{1}{1 - p^s} .$$

5. Twin Primes

- Pairs of primes (p, q) with $q = p + 2$. E.g. (11,13) and $(71, 73)$.
- Conjecture: There are infinitely many pairs of twin primes. If you prove it, you'll be famous!

Math 418H **Fall 2005**

Lecture: Fri 9/9/05

1. Prop: If $m/n \in \mathbb{Q}$ in lowest terms, and $\sqrt{m/n} \in \mathbb{Q}$, then $\sqrt{m}$, $\sqrt{n} \in \mathbb{Z}$.

   - First Proof (based on Fund Thm of Arithmetic). Assume a/b in lowest terms with $(a/b)^2 = m/n$, so that $a^2 n = b^2 m$. Let $p_1, \ldots, p_r$ be all primes dividing a, b, n, m, and let $a = p_1^{a_1} \cdots p_r^{a_r}$, $b = p_1^{b_1} \cdots p_r^{b_r}$, etc., with integers $a_i, b_i, m_i, n_i \geq 0$. Then $a^2 = b^2 m$ is equivalent (by the Fund Thm) to $2a_i + n_i = 2b_i + m_i$.

     We have $\gcd(a, b) = \gcd(m, n) = 1$. We will show $2a_i = m_i$ and $2b_i = n_i$ for all i, so $a^2 = m$, $b^2 = n$.

     - Suppose $p_i | a$. We have: $p_i \not| b$. Also $p_i | a^2 n = b^2 m$, so $p_i | m$ and $p_i \not| n$. Thus: $a_i, m_i > 0$ and $b_i = n_i = 0$. Thus $2a_i + n_i = 2b_i + m_i$ means $2a_i = m_i$ and $2b_i = n_i = 0$.
     - Suppose $p_i | b$. Similarly we get $a_i = m_i = 0$ and $b_i, n_i > 0$ and $2a_i = m_i = 0$, $2b_i = n_i$.
     - Suppose $p_i \not| a, b$. If $p_i | m$ then $p_i | b^2 m$ and $p_i | b^2$ and $p_i | b$. But then $\gcd(a, b) > 1$, so this cannot happen. Similarly $p_i | n$ cannot happen. Thus $p_i \not| a, b, m, n$, so forget about p_i.

     First Proof is done.

   - Lemma on Uniqueness of Fractions. If $a/b = c/d$ are both positive fractions in lowest terms, then $a = c$ and $b = d$.

     Proof of Lemma: We have $\gcd(a, b) = 1$, so we can write $1 = ma + nb$, so $c = mac + nbc = mac + nad = a(mc + nd)$, so $a | c$. Also $d = mad + nbd = mbc + nbd = b(mc + nd)$ so $b | d$. Similarly use $1 = pc + qd$ to get $c | a$ and $d | b$. Conclude $a = c$ and $b = d$.

   - Second Proof of Prop (based on Uniqueness of Fractions). Suppose a/b in lowest terms with $(a/b)^2 = m/n$. Then $a^2/b^2 = m/n$ with both sides in lowest terms (prove!), $a^2 = m$ and $b^2 = n$.

   - Both proofs ultitmately rest on the key lemma resulting from the Euclidean algortitihm: we can always write $\gcd(a, b) = ma + nb$ for some $m, n \in \mathbb{Z}$.

2. Fermat's Little Theorem: If p is prime, then $p \mid n^p - n$ for any $n \in \mathbb{Z}$.

   - Proof (David Krcatovic): Use induction on n. For $n = 1$, the statement is obvious. Now assume $p \mid n^p - n$. By the Binomial Theorem:

$$\begin{aligned}(n{+}1)^p - (n{+}1) &= n^p + pn^{p-1} + \tfrac{1}{2}p(p{-}1)n^{p-2} + \cdots + pn + 1 - (n{+}1) \\ &= (n^p - n) + \textstyle\sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!}\, n^{p-k} \,.\end{aligned}$$

     In the last expression, p divides the first term by the inductive hypothesis, and p divides each term in the summation because the numerator contains the prime p, and every term in the denominator is less than p. Conclusion: $p \mid (n{+}1)^p - (n{+}1)$, so the induction proceeds, and the Theorem is true for every positive integer n.

Lecture Mon 9/12/05

Algebra Definitions 1

We define some terms concerning generalized number systems.

- A **ring** is a set R along with operations of addition $+ : R \times R \to R$ and multiplication $\bullet : R \times R \to R$, satisfying the following properties:

  (i) $+$ associativity: $(a+b)+c = a+(b+c)$ for all $a, b, c \in R$.

  (ii) $+$ identity: there exists $0 \in R$ such that $0 + a = a + 0 = a$ for all $a \in R$.

  (iii) $+$ inverse: for any $a \in R$, there is a $b \in R$ with $a + b = b + a = 0$: we denote b by $-a$.

  (iv) $+$ commutativity: $a + b = b + a$ for all $a, b \in R$.

  (i′) $\bullet$ associativity: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ for all $a, b, c \in R$.

  (ii′) $\bullet$ identity: there exists $1 \in R$ such that $1 \bullet a = a \bullet 1 = a$ for all $a \in R$.

  (v) distributivity: $a \bullet (b + c) = a \bullet b + a \bullet c$ and $(a + b) \bullet c = a \bullet c + b \bullet c$.

- A **division ring** is a ring satisfying:

  (iii′) $\bullet$ inverse: for any non-zero $a \in R$, there is a $b \in R$ with $a \bullet b = b \bullet a = 0$: we denote b by a^{-1} or $1/a$.

- A **commutative ring** is a ring satisfying:

  (iv′) $\bullet$ commutativity: $a \bullet b = b \bullet a$ for all $a, b \in R$.

- A **field** is a ring satisfying both (iii′) and (iv′).

- A **unit** in ring R is an element a which has a mulitiplicative inverse $a^{-1} \in R$. The set of units is denoted $R^\times$. Thus, a field F is a ring in which every non-zero element is a unit: $F^\times = F \setminus \{0\}$. Elements of a ring are **associates** if they differ by a unit factor: $a, b \in R$ such that $a = ub$ for $u \in R^\times$.

- A **zero-divisor** in a ring R is an element $a \neq 0$ such that $a \bullet b = 0$ for some $b \in R$. A **domain** is a commutative ring with no zero-divisors.

- A **Euclidean ring** is a domain R along with a function

  $$\text{size} : R \setminus \{0\} \to \mathbb{N}$$

  (where $\mathbb{N} = \{0, 1, 2, \cdots\}$) such that for any $a, b \in R$, there are $q, r \in R$ with $a = qb + r$ and $r = 0$ or $\text{size}(r) < \text{size}(b)$. The elements q, r are not necessarily unique.

Examples

- $\mathbb{Z}$, the integers, is commutative ring, a Euclidean domain, but not a field. The units are: $\mathbb{Z}^\times = \{\pm 1\}$.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, the rational, real and complex numbers, are all fields.
- $\mathbb{Z}_n$, clock arithmetic mod n, is a commutative ring for any n. It is a field for $n = 2$. For which n is it a field? What are the units and zero-divisors?
- $M_n(\mathbb{Q})$, the $n \times n$ matrices with entries in $\mathbb{Q}$ under matrix addition and multiplication, is a ring, but not commutative, and without division. The units are the nonsingular matrices, the zero-divisors are the singular matrices (prove!).
- $\mathbb{Q}[x]$, the polynomial functions:

  $$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \,,$$

  with $a_0, \ldots, a_n \in \mathbb{Q}$, under the pointwise addition and multiplication, is a commutative ring and a domain. The units are the non-zero contstant functions $f(x) = c$. It is also a Euclidean domain under the polynomial division algorithm, with size function $\operatorname{size} f(x) = \deg f(x) = n$, the degree of the highest non-zero term $a_n x^n$.

  All of these features make the polynomial ring $\mathbb{Q}[x]$ analogous to the integer ring $\mathbb{Z}$.
- $\mathbb{Q}(x)$, the rational functions, is the set of quotients of two polynomial functions: $f(x)/g(x)$ with $g(x) \neq 0$. This is a field, analogous to $\mathbb{Q}$.

Lecture: Wed 9/14/05

1. $\mathbb{Q}[x]$ polynomial ring

- $\mathbb{Q}[x]$ is the set of all polynomial functions

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n ,$$

where the coefficients $a_i \in \mathbb{Q}$ for all i.

- Degree: If $a_n \neq 0$, we say $n = \deg f(x)$, the degree of the polynomial. A constant function $f(x) = c \neq 0$ has degree 0, and the zero function $f(x) = 0$ has no degree (or degree $-\infty$).
- Monic polynomial: $a_n = 1$.
- Addition:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i := \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i$$

Thus, $\deg(f(x) + g(x)) = \max(\deg f(x) , \deg g(x))$.

- Multiplication:

$$\left(\sum_{i=0}^{n} a_i x^i\right) \bullet \left(\sum_{i=0}^{m} b_i x^i\right) := \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k$$

Thus $\deg(f(x) \bullet g(x)) = \deg f(x) + \deg g(x)$.

- We can think of $f(x) \in \mathbb{Q}[x]$ as a function $f : \mathbb{Q} \to \mathbb{Q}$ with the usual addition and multiplication of functions. From this, it is clear that $\mathbb{Q}[x]$ is a commutative ring and a domain, because $\mathbb{Q}$ is so.
- Arithmetic in $\mathbb{Q}[x]$ is analogous to $\mathbb{Z}$, with x taking the role of base 10:

$$\begin{aligned} (3x^2{+}5x) + (2x{+}3) &= 3x^2{+}7x{+}3 \\ 350 + 23 = (3{\cdot}10^2{+}5{\cdot}10) + (2{\cdot}10{+}3) &= 3{\cdot}10^2{+}7{\cdot}10{+}3 = 373 \end{aligned}$$

- The key algorithm for $\mathbb{Q}[x]$, as for $\mathbb{Z}$, is long division. For any $f(x), g(x) \in \mathbb{Q}[x]$, there exist $q(x), r(x) \in \mathbb{Q}[x]$ with:

$$f(x) = q(x)g(x) + r(x) \quad \text{and} \quad \deg r(x) {<} \deg g(x) \;\; \text{or} \;\; r(x){=}0 .$$

- Units: $\mathbb{Q}[x]^\times = \{f(x) = c \neq 0\}$, the non-zero constant functions (the polynomials of degree 0).

2. Factorization in $\mathbb{Q}[x]$

   - Divisibility: $g(x)$ divides $f(x)$, written $g(x) \,|\, f(x)$, means $f(x) = g(x)h(x)$ for some $h(x) \in \mathbb{Q}[x]$. Note that the units $c \neq 0$ divide every polynomial $f(x)$, since $f(x) = c \bullet \frac{1}{c} f(x)$.
   - Irreducible polynomials: The analog of primes are the polynomials $p(x)$ whose only divisors are 1 and $p(x)$ (times units).
   - Polynomial greatest common divisor: $d(x) = \gcd(f(x)\,,\, g(x))$ is the highest degree polynomial with $d(x) \,|\, f(x)$ and $d(x) \,|\, g(x)$. Note that $d(x)$ is not unique, but can be multiplied by any unit. We usually normalize $d(x)$ to be monic.
   - Euclidean Algorithm: Works exactly as for $\mathbb{Z}$. Shows that

     $$\gcd(f(x)\,,\, g(x)) = n(x)f(x) + m(x)g(x)$$

     for some $n(x), m(x) \in \mathbb{Q}[x]$.
   - *Key Property of Primes:* If an irreducible $p(x) \,|\, a(x)b(x)$, then $p(x) \,|\, a(x)$ or $p(x) \,|\, b(x)$.

     Proof. If $\gcd(a(x)\,,\, p(x)) = p(x)$, then $p(x) \,|\, a(x)$. Otherwise, $\gcd(a(x)\,,\, p(x)) = 1$, so by the Euclidean Algorithm $1 = m(x)a(x) + n(x)p(x)$ and:

     $$b(x) = m(x)a(x)b(x) + n(x)p(x)b(x)\,.$$

     Since $p(x)$ divides both terms on the righthand side, it also divides the lefthand side: $p(x) \,|\, b(x)$.
   - *Unique Factorization:* In $\mathbb{Q}[x]$, any polynomial factors into a product of irreducibles in a unique way, except for rearranging the factors, and multiplying by units. If we specify that all polynomials are monic, we can forget about multiplying by units.

     Proof. Same as for $\mathbb{Z}$.

3. $R[x]$, general polynomial ring.

   - We can define polynomials $R[x]$ with coefficients in any commutative ring R.
   - All results above hold whenever $R = F$, any field. For example $R = \mathbb{R}$ the reals, or $\mathbb{C}$ the complex numbers, or $\mathbb{Z}_2$ the clock arithmetic modulo 2.
   - If R is not a field, the division algorithm for $R[x]$ does not work, and $R[x]$ is *not* Euclidean.
     Example: $\mathbb{Z}[x]$ has no possible division algorithm.

Lecture: Wed 9/14/05

1. $\mathbb{Q}[x]$ polynomial ring

   - $\mathbb{Q}[x]$ is the set of all polynomial functions

     $$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \,,$$

     where the coefficients $a_i \in \mathbb{Q}$ for all i.
   - Degree: If $a_n \neq 0$, we say $n = \deg f(x)$, the degree of the polynomial. A constant function $f(x) = c \neq 0$ has degree 0, and the zero function $f(x) = 0$ has no degree (or degree $-\infty$).
   - Monic polynomial: $a_n = 1$.
   - Addition:

     $$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i := \sum_{i=0}^{\max(m,n)} (a_i{+}b_i) x^i$$

     Thus, $\deg(f(x) + g(x)) = \max(\deg f(x) \,, \deg g(x))$.
   - Multiplication:

     $$\left(\sum_{i=0}^{n} a_i x^i\right) \bullet \left(\sum_{i=0}^{m} b_i x^i\right) := \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k$$

     Thus $\deg(f(x) \bullet g(x)) = \deg f(x) + \deg g(x)$.
   - We can think of $f(x) \in \mathbb{Q}[x]$ as a function $f : \mathbb{Q} \to \mathbb{Q}$ with the usual addition and multiplication of functions. From this, it is clear that $\mathbb{Q}[x]$ is a commutative ring and a domain, because $\mathbb{Q}$ is so.
   - Arithmetic in $\mathbb{Q}[x]$ is analogous to $\mathbb{Z}$, with x taking the role of base 10:

     $$\begin{aligned} (3x^2{+}5x) + (2x{+}3) &= 3x^2{+}7x{+}3 \\ 350 + 23 = (3{\cdot}10^2{+}5{\cdot}10) + (2{\cdot}10{+}3) &= 3{\cdot}10^2{+}7{\cdot}10{+}3 = 373 \end{aligned}$$

   - The key algorithm for $\mathbb{Q}[x]$, as for $\mathbb{Z}$, is long division. For any $f(x), g(x) \in \mathbb{Q}[x]$, there exist $q(x), r(x) \in \mathbb{Q}[x]$ with:

     $$f(x) = q(x)g(x) + r(x) \quad \text{and} \quad \deg r(x) {<} \deg g(x) \;\; \text{or} \;\; r(x){=}0 \,.$$

   - Units: $\mathbb{Q}[x]^\times = \{f(x) = c \neq 0\}$, the non-zero constant functions (the polynomials of degree 0).

2. Factorization in $\mathbb{Q}[x]$

   - Divisibility: $g(x)$ divides $f(x)$, written $g(x) \mid f(x)$, means $f(x) = g(x)h(x)$ for some $h(x) \in \mathbb{Q}[x]$. Note that the units $c \neq 0$ divide every polynomial $f(x)$, since $f(x) = c \bullet \frac{1}{c} f(x)$.
   - Irreducible polynomials: The analog of primes are the polynomials $p(x)$ whose only divisors are 1 and $p(x)$ (times units).
   - Polynomial greatest common divisor: $d(x) = \gcd(f(x), g(x))$ is the highest degree polynomial with $d(x) \mid f(x)$ and $d(x) \mid g(x)$. Note that $d(x)$ is not unique, but can be multiplied by any unit. We usually normalize $d(x)$ to be monic.
   - Euclidean Algorithm: Works exactly as for $\mathbb{Z}$. Shows that

     $$\gcd(f(x), g(x)) = n(x)f(x) + m(x)g(x)$$

     for some $n(x), m(x) \in \mathbb{Q}[x]$.
   - *Key Property of Primes:* If an irreducible $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

     Proof. If $\gcd(a(x), p(x)) = p(x)$, then $p(x) \mid a(x)$. Otherwise, $\gcd(a(x), p(x)) = 1$, so by the Euclidean Algorithm $1 = m(x)a(x) + n(x)p(x)$ and:

     $$b(x) = m(x)a(x)b(x) + n(x)p(x)b(x).$$

     Since $p(x)$ divides both terms on the righthand side, it also divides the lefthand side: $p(x) \mid b(x)$.
   - *Unique Factorization:* In $\mathbb{Q}[x]$, any polynomial factors into a product of irreducibles in a unique way, except for rearranging the factors, and multiplying by units. If we specify that all polynomials are monic, we can forget about multiplying by units.

     Proof. Same as for $\mathbb{Z}$.

3. $R[x]$, general polynomial ring.

   - We can define polynomials $R[x]$ with coefficients in any commutative ring R.
   - All results above hold whenever $R = F$, any field. For example $R = \mathbb{R}$ the reals, or $\mathbb{C}$ the complex numbers, or $\mathbb{Z}_2$ the clock arithmetic modulo 2.
   - If R is not a field, the division algorithm for $R[x]$ does not work, and $R[x]$ is *not* Euclidean.
     Example: $\mathbb{Z}[x]$ has no possible division algorithm.

Lecture: Mon 9/19/05

1. Factoring polys and finding roots

   - Root of a polynomial $f(x)$ means a value c with $f(c) = 0$.
   - *Prop:* For $f(x) \in \mathbb{Q}[x]$, have: $f(c) = 0$ for $c \in \mathbb{Q} \implies (x-c) \mid f(x)$.

     Proof of $\Rightarrow$: Divide: $f(x) = q(x)\,(x-c) + r(x)$ with $\deg r(x) < deg(x-c) = 1$. Thus $r(x) = a$, a constant (possibly zero). Now: $0 = f(c) = q(c)\,(c-c) + a = a$, i.e. $f(x) = q(x)\,(x-c)$.
   - *Prop:* The number of distinct roots of a polynomial is always less than its degree.

     Proof: Let $f(x) = a_0 + \cdots + a_n x^n$ with $\deg f(x) = n$. Let $c_1, \ldots, c_k$ be its distinct roots. Then $f(x) = (x-c_1)\, f_1(x)$ by the previous proposition. Further $0 = f(c_2) = (c_2 - c_1)\, f_1(c_2)$, and $c_2 - c_1 \neq 0$, so $f_1(c_2) = 0$, and similarly $c_2, \ldots, c_k$ are roots of $f_1(x)$. Repeating, get:
     $$f(x) = (x-c_1)\cdots(x-c_k)\, f_k(x)$$
     for some poly $f_k(x)$ of degree $d \geq 0$. Taking degrees of both sides, $n = k + d$, so $k \leq n$.

2. Rational Root Test

   - *Theorem:* If $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ (i.e., $a_i \in \mathbb{Z}$), and $f(c/d) = 0$ for $c/d \in \mathbb{Q}$ in lowest terms, then $c \mid a_0$ and $d \mid a_n$ in $\mathbb{Z}$.
   - Example: Find all complex roots of
     $$g(x) = x^3 - \frac{13}{3}x^2 - \frac{1}{3}x + 2 = 0\,.$$
     Clear denominators to get $f(x) = 3x^3 - 13x^2 - x + 6 = 0$. Any rational root c/d must satisfy $c \mid 6$ and $d \mid 3$, so candidates are:
     $$\frac{c}{d} = \pm 6\,,\ \pm 2\,,\ \pm 1\,,\ \pm\frac{2}{3}\,,\ \pm\frac{1}{3}\,.$$
     Plugging in $f(c/d)$, find the only rat root is $f(-2/3) = 0$. Factoring, get $h(x) = g(x)/(x+2/3) = x^2 - 5x + 3$. Now apply quadratic formula to find the remaining 2 roots of $h(x)$.

3. Factorization in $R[x]$

   - For any commutative ring R, we can define $R[x]$, the ring of polynomials with coefficients in R. The unit polynomials are just the unit constant functions: $R[x]^\times = R^\times$.
   - Irreducible polynomial $p(x) \in R[x]$ means: the only divisors of $p(x)$ in $R[x]$ are $p(x)$ and 1 (times a unit $c \in R^\times$).
   - For general R, if $p(x)$ is irreducible, then it is impossible to factor $p(x) = f(x)g(x)$ with $g(x), g(x) \in R[x]$ and $\deg g(x)\,, \deg g(x) < \deg p(x)$.

     But if R is not a field, we can have irreducible constants $c \notin R^\times$, so $p(x)$ could be reducible even if there is no factorization $p(x) = f(x)g(x)$ as above.
   - Example: Consider $p(x) = 2x^2 - 4$.

– In $\mathbb{R}[x]$ with real number coefficients, we can factor:

$$p(x) = x^2 - 2 = 2(x - \sqrt{2})(x + \sqrt{2}) \in \mathbb{R}[x]\,.$$

So $p(x)$ is reducible in $\mathbb{R}[x]$.

– In $\mathbb{Q}[x]$ with rational coefficients, any non-trivial factors $p(x) = f(x)g(x)$ would have to be linear: $f(x) = x{-}a$ for some $a \in \mathbb{Q}$ with $f(a) = 0$, but the roots $a = \pm\sqrt{2}$ are irrational. So $p(x)$ is irreducible in $\mathbb{Q}[x]$.

– In $\mathbb{Z}[x]$, where the coefficients are not a field, we can factor $p(x) = 2\,(x^2{-}2)$, where 2 and $(x^2{-}2)$ are both irreducible in $\mathbb{Z}[x]$. So $p(x)$ is reducible in $\mathbb{Z}[x]$.

4. Factorization in $\mathbb{Z}[x]$ vs $\mathbb{Q}[x]$

- Units: $\mathbb{Z}[x]^\times = \{\pm 1\}$, but general $f(x) = c$ is *not* invertible in $\mathbb{Z}[x]$. $\mathbb{Q}[x]^\times = \mathbb{Q}^\times$, the non-zero constant polynomials
- Two types of primes in $\mathbb{Z}[x]$. First, any prime integer $p \in \mathbb{Z}$ is also a prime in $\mathbb{Z}[x]$. Second, for any irreducible $f(x) \in \mathbb{Q}[x]$, we can clear denominators and get an irreducible in $\mathbb{Z}[x]$. Example: $x^2{-}x{-}\frac{1}{2}$ in $\mathbb{Q}[x]$ corresponds to the irreducible $2x^2{-}2x{-}1$ in $\mathbb{Z}[x]$. However, $4x^2{-}4x{-}2 = 2\,(2x^2{-}2x{-}1)$ is reducible in $\mathbb{Z}[x]$, but irreducible in $\mathbb{Q}[x]$, since the constant 2 is a unit in $\mathbb{Q}[x]$.
- *Gauss Lemma:* If an integer polynomial $f(x)$ is irreducible in $\mathbb{Z}[x]$, then $f(x)$ is also irreducible in the larger ring $\mathbb{Q}[x]$.

  Equivalently, if an integer polynomial $f(x)$ is reducible in $\mathbb{Q}[x]$, then $f(x)$ is also reducible in the smaller ring $\mathbb{Z}[x]$.

5. Proof of the Rational Root Test

- *Idea of Proof:* If $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with $f(c/d) = 0$, then $f(x) = (x - c/d)\,g(x)$ for some $g(x) \in \mathbb{Q}[x]$ with $\deg g(x) = n{-}1$. We can factor in $\mathbb{Z}[x]$ by clearing denominators:

$$\begin{aligned} f(x) &= (dx - c)\,(b_{n-1}x^{n-1} + \cdots + b_1 x + b_0) \\ &= db_{n-1}x^n + \cdots + (db_0{-}cb_1)x - cb_0 \end{aligned}$$

  with $b_i \in \mathbb{Z}$. Thus $a_0 = -cb_0$ and $a_n = db_{n-1}$, so $c \,|\, a_0$ and $d \,|\, a_n$.
- *Why this proof is incomplete:* The dubious phrase is "clearing denominators." If we multiply $(x - c/d)$ by d, we have to divide $g(x)$ by d, and it is not at all clear that the resulting factor $b_{n-1}z^{n-1} + \cdots + b_0$ will be in $\mathbb{Z}[x]$. Also, notice that we never used the hypothesis $\gcd(c, d) = 1$, so we have actually "proved" RRT without assuming c/d is in lowest terms, which is FALSE!
- *Proof (assuming Gauss Lemma):* Induction on $n = \deg f(x)$.

  If $n = 1$, then ... *(Exercise)*

  If $n > 1$, we may assume RRT is true for polynomials of degree $k < n$. Since $f(c/d) = 0$, we known $f(x) = (x{-}c/d)\,g(x)$ for $g(x) \in \mathbb{Q}[x]$, so $f(x)$ is reducible in $\mathbb{Q}[x]$. Thus by the Gauss Lemma $f(x)$ is reducible in $\mathbb{Z}[x]$, meaning $f(x) = f_1(x)\,f_2(x)$ for $f_1(x), f_2(x) \in \mathbb{Z}[x]$ with $\deg f_1(x)\,, \deg f_2(x) < n$.

  Now $0 = f(c/d) = f_1(c/d)\,f_2(c/d)$, so c/d is a root of $f_1(x)$ or $f_2(x)$ (say $f_1(x)$). By induction, RRT applies to $f_1(x)$ having degree $k < n$, so $f_1(x) = b_k x^k + \cdots + b_0$ for $b_i \in \mathbb{Z}$ with $c \,|\, b_0$ and $d \,|\, b_k$. Writing out the coefficients of $f(x) = f_1(x)\,f_2(x)$ gives the divisibility $c \,|\, a_0$ and $d \,|\, a_n$, so RRT holds for $f(x)$ of degree n.

Math 418H **Fall 2005**

Lecture: Wed 9/21/05

1. Gauss Lemma for primitive polynomials in $\mathbb{Z}[x]$

   - Divisibility: $g(x) \mid f(x)$ in $\mathbb{Z}[x]$ means $f(x) = g(x)\,h(x)$ for some $h(x) \in \mathbb{Z}[x]$. We say $p(x)$ is *irreducible* in $\mathbb{Z}[x]$ if its only divisors are 1 and $p(x)$ (times ± 1).
   - A constant $n \in \mathbb{Z}$ divides $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ whenever $n \mid a_0, \ldots, a_n$. A constant $p \in \mathbb{Z}$ is irreducible in $\mathbb{Z}[x]$ whenever it is prime in $\mathbb{Z}$.
     These just restate the above in the case of constant polynomials.
   - Primitive polynomial: $f(x) \in \mathbb{Z}[x]$ with $\gcd(a_0, a_1, \ldots, a_n) = 1$. That is, no integer n divides $f(x)$ (except units ± 1).
   - *Lemma:* If $f(x), g(x) \in \mathbb{Z}[x]$ are primitive, then the product $f(x)\,g(x)$ is also primitive.
   - Equivalently: If $f(x)\,g(x)$ is not primitive, then $f(x)$ or $g(x)$ is not primitive. That is, if a prime $p \in \mathbb{Z}$ divides $f(x)\,g(x)$ in $\mathbb{Z}[x]$, then p divides $f(x)$ or $g(x)$.
   - *Proof:* Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$, and suppose p divides the product:

     $$f(x)\,g(x) = \sum_{k=0}^{n+m} c_k x^k = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k .$$

     Assume we have: $p \mid a_0, a_1, \ldots, a_k$ and $p \mid b_0, b_1, \ldots, b_\ell$ for some $k < n$ and $\ell < m$. Either or both lists are allowed to be empty, containing no elements, in which case we have assumed *nothing*. Now we have:

     $$c_{k+\ell+2} \;=\; \begin{matrix} a_0 b_{k+\ell+2} + a_1 b_{k+\ell+1} + \cdots + a_k b_{\ell+2} \\ a_{k+\ell+2} b_0 + a_{k+\ell+1} b_1 + \cdots + a_{k+2} b_\ell \end{matrix} \; + \; a_{k+1} b_{\ell+1} \quad .$$

     By assumption, p divides the lefthand side $c_{k+\ell+2}$, and p divides all the terms on the righthand side except possibly $a_{k+1} b_{\ell+1}$. But then p *must* divide the last term, and $p \mid a_{k+1}$ or $p \mid b_{\ell+1}$.

     Hence we can add one item (a_{k+1} or $b_{\ell+1}$) to our list of coefficients divisible by p. We can keep repeating this argument and enlarging our list: the process will only end when $k = n$ or $\ell = m$, which means $p \mid f(x)$ or $p \mid g(x)$.

2. Factorization in $\mathbb{Z}[x]$ versus $\mathbb{Q}[x]$

   - *Gauss Lemma:* If a non-constant $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.
   - Equivalently: If $f(x) \in \mathbb{Z}[x]$ has non-trivial factors in $\mathbb{Q}[x]$, then it has non-trivial factors in $\mathbb{Z}[x]$.
   - *Proof:* Suppose $f(x) = g(x)h(x)$ with $f(x) \in \mathbb{Z}[x]$ and $g(x), h(x) \in \mathbb{Q}[x]$. We must find factors of $f(x)$ in $\mathbb{Z}[x]$. Let $f(x) = af_0(x)$, $g(x) = bg_0(x)$, $h(x) = ch_0(x)$, where $f_0, g_0, h_0 \in \mathbb{Z}[x]$ are primitive polynomials, and $a \in \mathbb{Z}$, $b, c \in \mathbb{Q}$.

     Then $\frac{a}{bc} f_0(x) = g_0(x)h_0(x)$, which is a primitive polynomial by Gauss' Lemma above. Thus both $f_0(x)$ and $\frac{a}{bc} f_0(x)$ are primitive integer polynomials, so we must have $a/bc = 1$ and $a = bc$. Thus $f(x) = bcg_0(x)h_0(x) = ag_0(x)h_0(x)$, with all factors in $\mathbb{Z}[x]$.

3. Unique factorization for $\mathbb{Z}[x]$

   - $\mathbb{Z}[x]$ has no possible division algorithm because $\gcd(2, x) = 1$, but $2n(x) + xm(x) \neq 1$ for any $n(x), m(x) \in \mathbb{Z}[x]$.
   - *Proposition:* Any integer polynomial factors into a product of irreducibles in $\mathbb{Z}[x]$, namely into prime constants and irreducible primititve polynomials, and this factorization is unique except for re-ordering and $\pm$ signs.
   - *Proof:* Suppose

     $$p_1 \cdots p_r \, f_1(x) \cdots f_u(x) = q_1 \cdots q_s \, g_1(x) \cdots g_v(x)\,,$$

     where $p_i, q_i \in \mathbb{Z}$ are prime constants and $f_i(x), g_i(x) \in \mathbb{Z}[x]$ are primitive irreducibles. Thus $f_i(x), g_i(x)$ are also irreducibles in $\mathbb{Q}[x]$ by the above Gauss Lemma on Factorization. By the Unique Factorization for $\mathbb{Q}[x]$ we may assume $f_i(x) = c_i g_i(x)$ for constants $c_i \in \mathbb{Q}^\times$. But since both $f_i(x)$ and $g_i(x)$ are primitive integer polynomials, we must have $c_i = \pm 1$. Factoring $f_i(x) = g_i(x)$ from both sides, we have $p_1 \cdots p_r = q_1 \cdots q_s$. By Unique Factorization for $\mathbb{Z}$, we may assume $p_i = \pm q_i$, so we are done.

Math 418H **Fall 2005**

Lecture: Wed 9/28/05

1. Why define abstract structures like a field or a Euclidean ring, rather than just prove things for $\mathbb{Q}$ and $\mathbb{Z}$ directly?

   - The field axioms are the crucial properties of $\mathbb{Q}$, which give a foundation from which to rigorously prove most of the formulas of algebra. Similarly, the crucial properties of $\mathbb{Z}$ are captured in the definition of a Euclidean ring, giving us a foundation to prove non-obvious facts such as Unique Factorization.
   - Once we prove a formula using only the field axioms, we know it holds not only for $F = \mathbb{Q}$, but for *any* new field we may define, such as the clock arithmetic field $\mathbb{Z}_p$ (p prime) or the rational functions $\mathbb{Q}(x)$. Similarly,since Unique Factorization depends only on the division algorithm, we know it holds not only for $\mathbb{Z}$ but for $\mathbb{Q}[x]$ and any other Euclidean ring we find.

2. Basic formulas for any field F

   - We assume axioms (i)–(iv), (i')–(iv'), (v). In the proofs, we will use commutativity and associativity without comment.
   - *Lemma:* The elements 0, 1, $-a$, a^{-1} are unique.
     Proof: If we have two zero elements $0, 0'$ with $a + 0 = a + 0' = a$ for all a, then: $0 = 0 + 0' = 0'$. If we have two inverse elements $-a, -a'$ with $(-a) + a = (-a') + a = 0$, then:
     $$\begin{aligned} -a &= (-a) + 0 \\ &= (-a) + a + (-a') \\ &= 0 + (-a') = -a'. \end{aligned}$$
     Similarly for 1 and a^{-1}.
   - *Lemma:* $0 \bullet a = 0$
     Proof:
     $$\begin{aligned} 0 &= -(0 \bullet a) + 0 \bullet a \\ &= -(0 \bullet a) + (0{+}0) \bullet a \\ &= -(0 \bullet a) + 0 \bullet a + 0 \bullet a \\ &= 0 \bullet a. \end{aligned}$$
   - *Lemma:* $-(-a) = a$
     Proof:
     $$\begin{aligned} -(-a) &= -(-a) + 0 \\ &= -(-a) + (-a) + a \\ &= 0 + a = a. \end{aligned}$$

- *Lemma:* $(-a) \bullet b = -(a \bullet b)$
  Proof: By definition, $-(a \bullet b)$ is the unique element such that $-(a \bullet b) + a \bullet b = 0$. Now:
  $$\begin{aligned} (-a) \bullet b + a \bullet b &= ((-a) + a) \bullet b \\ &= 0 \bullet b \;=\; 0\,. \end{aligned}$$
- *Lemma:* $(-a) \bullet (-b) = a \bullet b$
  Proof: Using the previous lemma twice:
  $$\begin{aligned} (-a) \bullet (-b) &= -(a \bullet (-b)) \\ &= -(-(a \bullet b)) = a \bullet b\,. \end{aligned}$$

3. Advanced formulas for any field F

- Prove the following as exercises.
- Quadratic formula: The only roots of $ax^2 + bx + c \in F[x]$ are $x = (-b \pm d)/2a$, where $d \in F$ is an element with $d^2 = b^2 - 4ac$. If there is no such element $d \in F$, then the equation has no solution.
- FOIL: $(a + b)(c + d) = ac + ad + bc + bd\,.$
  This holds in any commutative ring, not necessarily a field.
- Binomial Theorem:
  $$\begin{aligned} (a+b)^2 &= a^2 + 2ab + b^2 \\ (a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3 \\ (a+b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\ (a+b)^n &= a^n + \tbinom{n}{1}a^{n-1}b + \tbinom{n}{2}a^{n-2}b^2 + \cdots + b^n\,, \end{aligned}$$
  where the binomial coefficients $\binom{n}{k}$ are defined recursively by:
  $$\tbinom{n}{0} = \tbinom{n}{n} = 1 \qquad \text{and} \qquad \tbinom{n+1}{k} = \tbinom{n}{k} + \tbinom{n}{k-1}\,.$$
  Again, this holds in any commutative ring.
- *Example:* In $F = \mathbb{Z}_2$, we have $2 = 0$, so $(a + b)^2 = a^2 + b^2$. This is not so remarkable, since $\mathbb{Z}_2$ has only two elements. But now consider $\mathbb{Z}_2[x]$, polynomials with coefficients in $\mathbb{Z}_2$. For example:
  $$f(x) = 0\,,\ 1\,,\ x\,,\ x{+}1\,,\ x^2\,,\ x^2{+}1\,,\ x^2{+}x\,,\ x^2{+}x{+}1\,,\ \ldots$$
  Then we once again have:
  $$(f(x) + g(x))^2 = f(x)^2 + g(x)^2$$
  for any polynomials $f(x), g(x) \in \mathbb{Z}_2[x]$.
- $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots ab^{n-2} + b^{n-1})$.

Lecture Mon 10/4/05

Algebra Definitions 2: Real Numbers

- There is not necessarily any natural order on a given commutative ring R: rather, we must define it. An **order relation** on R is a specification of when $a < b$ holds for elements $a, b \in R$. Once $<$ is defined, we let $a > b$ mean $b < a$, and we let $a \leq b$ mean $a < b$ or $a = b$. The defined relation must obey the following axioms:

  (i) Compatibility with $+$ and $\bullet$
  If $a < b$ and c is arbitrary, then $a + c < b + c$.
  If $0 < a < b$ and $0 < c$, then $a \bullet c < b \bullet c$.

  (ii) Trichotomy: For any $a \in R$, exactly one of the following holds: $a > 0$, $a = 0$ or $a < 0$.

  EXERCISES: These axioms imply all the usual algebraic properties of inequalities. Prove the follwing:

  - $a < b \iff b - a > 0$
  - If $a < b$ and $b < c$, then $a < c$.
  - If $a > 0$, then $-a < 0$.
  - If $a, b < 0$, then $ab > 0$.
  - If R contains an element with $a^2 = -1$, then there is no possible order relation on R. (Thus, there is no possible order on the complex numbers $R = \mathbb{C}$.)

- Consider an ordered ring R. An *upper bound* of a subset $A \subset R$ is an element $b \in R$ such that $b \geq a$ for all $a \in A$. A *least upper bound* of A is an upper bound b such that $b \leq b'$ for every upper bound b' of A.

  We say that R is **topologically complete** if it obeys the *least upper bound property*:
  If a set A has any upper bound in $r \in R$, then A has a least upper bound in $r' \in R$.

  EXERCISES:

  - The field of rational numbers $R = \mathbb{Q}$ is *not* topologically complete. Answer: The set $S = \{x \in \mathbb{Q} \mid x^2 < 2\}$ has upper bounds 1.5, 1.42, 1.415, etc., but does not have any least upper bound in $\mathbb{Q}$.
  - The ring of integers $R = \mathbb{Z}$ *is* topologically complete.

- We **construct the field of real numbers** $\mathbb{R}$ out of the rational numbers $\mathbb{Q}$ by defining a real number to be a *cutset*: i.e., a set of rational numbers $S \subset \mathbb{Q}$ such that:

  (i) S is a downset: $s \in S$ implies $t \in S$ for all $t < s$.

  (ii) S is non-trivial: $S \neq \emptyset, \mathbb{Q}$.

  (iii) S contains no maximal element: no element $s \in S$ is an upper bound of S.

  Defining $+$, $\bullet$, and $<$ appropriately, we show that $\mathbb{R}$ is a topologically complete, ordered field.

- Addition: $S+T := \{s+t \mid s \in S\,,\, t \in T\}$.
- Zero element: $S_0 = \mathbb{Q}_{<0} := \{s \in \mathbb{Q} \mid s < 0\}$.
- Negatives: $-S := \{-s \mid s \notin S\,, s \neq \mathrm{lub}(S)\}$.
- Order: $S < T$ means $S \subset T$
- Multiplication: For $S, T \geq S_0$, define:

$$S \bullet T := \{st \mid s \in S\,,\, t \in T\,,\, s, t \geq 0\} \,\cup\, S_0\,.$$

  For $S < 0 < T$, define $S \bullet T := -(-S \bullet T)$, and similarly for other cases.

We then proceed to prove that the above definition satisfies the properties of a field with order and topological completeness. This involves a lot of checking, but our definitions at least make the completeness easy: If $\mathcal{A} \subset \mathbb{R}$ is any collection of downsets $S \in \mathcal{A}$, then an upper bound is a cutset $B \subset \mathbb{Q}$ with $S \subset B$ for all $S \in \mathcal{A}$. Then we easily check that $B := \bigcup_{S \in \mathcal{A}} S$ is a cutset, and is the least upper bound of $\mathcal{A}$.

Our definition establishes the existence of $\mathbb{R}$, but once we have established it, we *never* use it in proofs. Rather, we rely on the *unique properties* of $\mathbb{R}$ stated in the following result.

- **Theorem** If R is any topologically complete ordered field, then R is naturally isomorphic to $\mathbb{R}$. That is, there is a unique map $\phi : R \to \mathbb{R}$ which is one-to-one and onto, and which respects addition and multiplication: $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ for all $a, b \in R$.

  That is, any topologically complete ordered field is just a "copy" of the real numbers, so that anything true about $\mathbb{R}$ also holds for any such field. Thus, in proving things about $\mathbb{R}$, we should only use the properties of a complete ordered field, never any specific construction of $\mathbb{R}$ such as the one above.

- A function $f : \mathbb{R} \to \mathbb{R}$ is **continuous** at $x = a$ if, for any y-tolerance $\epsilon > 0$, there is some sufficiently small x-tolerance $\delta > 0$ such that x being within distance δ of a guarantees that $f(x)$ is within distance ϵ of $f(a)$. That is:

$$\forall \epsilon{>}0 \; \exists \delta{>}0 \;:\; |x-a| < \delta \implies |f(x) - f(a)| < \epsilon\,.$$

  We have:

  - $f(x) = \text{const}$ and $f(x) = x$ are continuous at all $x = a$.
  - If $f(x), g(x)$ are continuous at $x = a$, then so are $f(x){+}g(x)$, $f(x){\cdot}g(x)$, and $f(x)/g(x)$ (the last provided $g(a) \neq 0$).
  - Any polynomial function $f(x) \in \mathbb{R}[x]$ is continuous at all $x = a$, and any rational function $f(x)/g(x) \in \mathbb{R}(x)$ is continuous at all $x = a$ with $g(a) \neq 0$.

- **Theorem** (Intermediate Value Theorem) If $f : [a, b] \to \mathbb{R}$ is a function continuous on an interval $[a, b]$, and $f(a) < v < f(b)$, then there is some value $c \in [a, b]$ such that $f(c) = v$.

  That is, $f(x)$ cannot go past the value v without hitting it. This implies that any odd-degree polynomial $f(x) \in \mathbb{R}[x]$ has a root $f(c) = 0$.

Lecture: Wed 10/10

1. Classifying real numbers

   - $\mathbb{R} \setminus \mathbb{Q}$ are the *irrational* numbers.
   - Let A be the set of *algebraic real numbers*, those reals which are roots of some polynomial $f(x) \in \mathbb{Q}[x]$.
   - We call $\mathbb{R} \setminus A$ the *transcendental* numbers. For example, $\pi = 3.14\cdots$ is transcendental, meaning that $a_0 + a_1\pi + \cdots + a_n\pi^n \neq 0$ for any $a_0, \ldots, a_n \in \mathbb{Q}$.

2. Degrees of infinity (Georg Cantor)

   - Cardinality: Two sets are said to have the same size or cardinality if there exists a one-to-one correspondence (bijection) between them.
   - Countable: a set whose elements can be put into a list; i.e., the set has the cardinality of the natural numbers $\mathbb{N}$.
   - $\mathbb{Z}$ is countable: $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$
   - $\mathbb{Q}$ is countable: $\mathbb{Q}_{>0} = \{\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \ldots\}$. In the list, skip over repeated rational numbers. Then alternate positive and negative to list all $\mathbb{Q}$.
   - A is countable by a similar argument.
   - $\mathbb{R}$ is *not* countable. Suppose we had a list $\{a_1, a_2, \ldots\}$ of *all* the real numbers in the interval $(0, 1)$. Write each number in decimal form: $a_i = 0.a_{i1}a_{i2}a_{i3}\cdots)$, where a_{ij} is a digit 0–9. Define a decimal number $b = 0.b_1b_2b_3\cdots$ by choosing the digits $b_1 \neq a_{11}$, $b_2 \neq a_{22}$, etc. Then clearly $b \neq a_i$ for any i, since they differ in the i^{th} digit, so b is a real number *not* on the list. Therefore, there can be no such complete list.
   - The irrational numbers, and even the transcendental numbers, are uncountable, so there are much, much more of them than of rationals or algebraic numbers.

3. Uniqueness of the real numbers

   - *Theorem:* The real numbers $\mathbb{R}$ are structurally defined by the properties of a topologically complete ordered field.

     That is, if $\mathcal{R}$ is any topologically complete ordered field, then there exists a unique one-to-one correspondence $\phi : \mathbb{R} \to \mathcal{R}$ which respects addition and multiplication:

$$\phi(a + b) = \phi(a) + \phi(b) \qquad \text{and} \qquad \phi(ab) = \phi(a)\,\phi(b)\,,$$

for every $a, b \in \mathbb{R}$ (so that $\phi(a), \phi(b) \in \mathcal{R}$). We say that ϕ is an *isomorphism* of fields. Furthermore, ϕ respects order: $a < b \iff \phi(a) < \phi(b)$.

- *Proof.* First $\mathcal{R}$, being a field, has unique additive and multiplicative identity elements $\tilde{0}, \tilde{1} \in \mathcal{R}$. Now define the counterpart of an integer

$$\tilde{n} := \underbrace{1 + \cdots + 1}_{n \text{ times}} \in \mathcal{R}\,.$$

Now $\tilde{1} = \tilde{1}^2 > \tilde{0}$ in the ordered field $\mathcal{R}$, so if $n < m \in \mathbb{Z}$, then in $\mathcal{R}$:

$$\tilde{n} < \tilde{n} + \tilde{1} + \cdots + \tilde{1} = \tilde{m}\,.$$

We can now make a copy of $\mathbb{Q}$ in $\mathcal{R}$ consisting of the quantities $\tilde{n}/\tilde{m}$, and these numbers behave the same as ordinary rationals. Finally, every real number $a \in \mathbb{R}$ is the least upper bound of a cutset $S \subset \mathbb{Q}$, so define its counterpart $\tilde{a} := \operatorname{lub}\{\tilde{s} \mid s \in S\} \in \mathcal{R}$, which exists since $\mathcal{R}$ is topologically complete. Now define $\phi : \mathbb{R} \to \mathcal{R}$ by $\phi(a) := \tilde{a}$. We may show this has the desired properties, and is unique.

4. Exercise: $\mathbb{Z}$ is topologically complete

- We check the least upper bound property. Let $A \subset \mathbb{Z}$ be a bounded, non-empty set of integers with upper bound $r \in \mathbb{Z}$. For $a \in A$, the subset $A \cap [a, r] = \{a_1, \ldots, a_n\}$ has at most $r - a$ elements. We clearly have $m = \max(a_1, \ldots, a_n) = \max A$, and this is the least upper bound of A in $\mathbb{Z}$.

5. Exercise: If $f(x), g(x)$ are continuous functions at $x = a$, then the product function $f(x)g(x)$ is likewise.

- We want to control the deviation $|f(x)g(x) - f(a)g(a)|$ in terms of $|f(x) - f(a)|$ and $|g(x) - g(a)|$. We have:

$$\begin{aligned} |f(x)g(x) - f(a)g(a)| &= |f(x)g(x) - f(x)g(a) + f(x)g(a) - f(a)g(a)| \\ &\leq |f(x)|\,|g(x){-}g(a)| + |f(x){-}f(a)|\,|g(a)| \end{aligned}$$

- Given $\epsilon > 0$, choose $\delta > 0$ small enough so that

$$|f(x) - f(a)| < \min\left(\frac{\epsilon}{2(|g(a)| + \epsilon)}\,, \epsilon\right),$$

$$|g(x) - g(a)| < \frac{\epsilon}{2(|f(a)| + \epsilon)}\,.$$

Then we have $|f(x)| \leq |f(a)| + \epsilon$, and:

$$\begin{aligned} |f(x)g(x) - f(a)g(a)| &< (|f(a)|{+}\epsilon)\,\frac{\epsilon}{2(|f(a)|{+}\epsilon)} + |g(a)|\frac{\epsilon}{2(|g(a)| + \epsilon)} \\ &< \epsilon/2 + \epsilon/2 = \epsilon\,. \end{aligned}$$