Math 418H **Fall 2005**

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.