Lecture: Wed 9/14/05

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

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

     $$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\,,$$

     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.