Notes for 7 March (Thursday)

1 The road so far...

1. Proved and stated the Chinese remainder theorem in a different way by defining products of rings (and groups).
2. Defined the ring of polynomials $R[x]$.

2 Polynomials

Note that R is itself a subring of $R[x]$ by $a \to (a, 0, 0, \ldots)$.By convention, the zero polynomial is taken to have degree $-\infty$. The ring of polynomials in k variables $x_1, \ldots, x_k$ with coefficients in R is recursively defined as $R[x_1, \ldots, x_k] = R[x_1, \ldots, x_{k-1}][x_k]$. Here is our first lemma. Its proof is straightforward.

Lemma 2.1. *Let R be a commutative ring. For every non-zero polynomials p and q, if the leading coefficient of p (or q) is a non zero-divisor in R then $deg(pq) = deg(p) + deg(q)$.*

Two polynomials are equal iff their coefficients are equal. Here is a subtle definition in this regard : Given $p(x) = (a_0, a_1, \ldots, a_d, 0, 0 \ldots) \in R[x]$, consider the function $f : R \to R$ given by $f(a) = p(a) = a_0 + a_1 a + a_2 a^2 + \ldots a_d a^d$. The subtle point is that f does NOT always determine p, i.e., if $f_1 = f_2$, this does not mean that $p_1 = p_2$! Indeed, consider $p(x) \in \mathbb{F}_2[x]$ given by $p(x) = x + x^2$. Now $f(0) = 0, f(1) = 0$. So $f \equiv 0$ as a function on $\mathbb{F}_2$!

Now we try develop some number-theory-esque results about polynomials. It is useful to call polynomials of the form $p(x) = x^n + a_{n-1}x^{n-1} \ldots$ as monic polynomials.

Theorem 1. *Let R be a commutative ring. Let f, g be two polynomials in $R[x]$ with $f \neq 0$ and suppose the leading coefficient of f is a unit in R. Then there are polynomials q, r with $deg(r) < deg(f)$ such that $g = fq + r$. These q, r are unique.*

Proof. Let $f = a_n x^n + \ldots + a_0$. If $deg(g) < deg(f)$, then $q = f$. If $g = b_n x^n + \ldots + b_0$, then $g - b_n a_n^{-1} f(x)$ has degree $< f$ and hence $g = b_n a_n^{-1} f(x) + r(x)$. If $deg(g) = deg(f) + s$, then we induct on s. For $s = 0$ we are done. Assuming truth for $0, 1, 2 \ldots, s-1$, note that $g - b_{n+s} a_n^{-1} x^s f(x)$ has smaller degree and hence equals (by the induction hypothesis) $q_1(x) f(x) + r(x)$. Thus, $g = (q_1(x) + b_{n+s} a_n^{-1} x^s) f(x) + r(x)$.
Uniqueness : If $fq_1 + r_1 = fq_2 + r_2$, then $f(q_1 - q_2) = r_2 - r_1$. If $q_1 - q_2 = c_d x^d + \ldots + c_0$ where $c_d \neq 0$, then comparing coefficients we see that $c_d a_n \neq 0$ is the coefficient of x^{d+n} in $r_2 - r_1$, a contradiction. □

As a corollary, the division algorithm holds for $\mathbb{F}[x]$ where $\mathbb{F}$ is a field. Now we state a high-school theorem (whose proof is trivial).

Theorem 2. *If $f(x)$ is a polynomial with coefficients in a field $\mathbb{F}$, and $a \in \mathbb{F}$, then $f(a)$ is the remainder when dividing $f(x)$ by $x - a$.*

As a special case, if $f(x) \in \mathbb{F}[x]$, then $f(a) = 0$ iff $f(x)$ is divisible by $x - a$. A simple induction argument on the degree shows D'Alembert's theorem that a nonzero degree n polynomial $f(x) \in \mathbb{F}[x]$ has at most n distinct roots in $\mathbb{F}$. This simple observation can be used to prove the following theorem.

Theorem 3. *If $\mathbb{F}$ is a field with infinitely many elements, and $f(x), g(x) \in \mathbb{F}[x]$, then $f(x) = g(x)$ iff $f(a) = g(a)$ $\forall$ $a \in \mathbb{F}$.*

Now we can implement Euclid's algorithm for polynomials. Before doing so, we define a gcd of $f, g \in \mathbb{F}[x]$ as a polynomial $p(x)$ that divides f, g and has the largest degree among such divisors.

Theorem 4. *Consider the recursive algorithm $r_i = r_{i+1}q_{i+2} + r_{i+2}$ where $g = fq_1 + r_1$, $f = r_1 q_2 + r_2$. It terminates after a finite number (say $n+1$) steps such that $r_{n-1} = r_n q_{n+1} + 0$. Also, r_n is a gcd(f, g).*

Proof. Indeed, in each step the degree of the remainder decreases by at least 1. By the well ordering principle of the naturals, in a finite number (n) of steps the degree reaches 0. Then $r_{n-2} = r_{n-1}q_n + r_n$ where $r_n \in \mathbb{F}$. Hence, $r_{n-1} = r_n r_n^{-1} + 0$. Now, if $g = fq + r$, then p divides g and f iff it divides f and r. Hence if p is a gcd of f, g then it is one of f, r. Thus, a gcd of r_{n-1}, r_n is r_n itself which is a gcd of (f, g). □

It is important to say "a gcd" because there surely is more than one. Indeed, $p(x)a$ where $a \neq 0 \in \mathbb{F}$ is a gcd. The following lemma helps us pick a standard one.

Lemma 2.2. *If p, q are gcds of $f, g \in \mathbb{F}[x]$, then $p = qr$ where $r \in \mathbb{F}$. Hence, normalising a gcd to be monic fixes it uniquely.*

Proof. Firstly, every common divisor of f, g divides a gcd of f, g obtained by the Euclidean algorithm (HW). So if p, q are gcds then $p = qr$ where $deg(r) = 0$ by definition. Hence $r \in \mathbb{F}$. □

Just as in the case of the integers and Gaussian integers, following the Euclidean algorithm backwards and solving for the remainders yields the Bezout identity : Every gcd d of $f, g \in \mathbb{F}[x]$ can be written as $d = rf + sg$. As before, g, f are said to be coprime if $gcd(g, f) = 1$.

Here is another useful little lemma.

Theorem 5. *If R is an integral domain, i.e., it has no zero divisors, then so is $R[x]$.*

Proof. Suppose not, i.e., there exist non-zero $f(x) = a_n x^n + \ldots + a_0$ and $g(x) = b_d x^d + b_{d-1}x^{d-1} + \ldots$ such that $f(x)g(x) = 0$. Comparing the leading coefficients we see that $a_n b_d = 0$ and hence a_n is a zero-divisor thus contradicting the assumption that R has none. □