Tying up detail from last time:

Defs: ① If R is an ID then a non-zero element $a \in R \setminus R^\times$ <u>irreducible</u> if a is not a product of non-units. Otherwise a is called <u>reducible</u>.

② A nonzero element $a \in R$ is <u>prime</u> if (a) is a prime ideal.

Note: A prime element is always irreducible, but the converse is not true in eneral. (exercise)

Lem: If $a \in R$ (ID) is prime then it is irreducible.

Pf: Suppose a is prime and $a = bc$. Then $bc \in (a) \Rightarrow b \in (a)$ or $c \in (a)$. W.L.O.G. suppose $b \in (a)$. Then $b = ad$ for some $d \in R$. Then $a = bc = adc \Rightarrow dc = 1 \Rightarrow c$ is a unit. So a irreducible. $\blacksquare$

Ex to show that irreducible $\not\Rightarrow$ prime in general:

Let $R = \mathbb{Z}[\sqrt{-5}]$. Then $3 = (2+\sqrt{-5})(2-\sqrt{-5})$.

All of 3, $2+\sqrt{-5}$, $2+\sqrt{-5}$ are irreducible, but (use norm map like last time)

$(2+\sqrt{-5})$, $2-\sqrt{-5} \notin (3) \Rightarrow (3)$ is not prime

However, in a PID, irreducible $\Leftrightarrow$ prime.

Thm: If R is a PID then $a \in R$ is irreducible if and only if it is prime.

Pf: Already know that prime $\Rightarrow$ irred. So suppose a is irreducible, let M be a maximal ideal containing (a). Since R is a PID, $M = (m)$.

Then $a \in (m) \Rightarrow a = mb$ for some $b \in R$.

Since a is irred., b is a unit. Then $(a) = M$.

So (a) is maximal $\Rightarrow (a)$ is prime. ∎

Thm (cor. of proof): In a PID, non-zero prime ideals are maximal.

Polynomials over commutative rings

Thm (Division algorithm): Suppose F is a field, $f, g \in F[x]$, and $g \neq 0$. Then $\exists$ unique polynomials $q, r \in F[x]$ s.t. $f = qg + r$ and $r = 0$ or $\deg r < \deg g$.

Cor: If F is a field then $F[x]$ is a UFD.

Theorem (Gauss's Lemma): Suppose that R is a UFD and F is its f.o.f. If f is irreducible in $R[x]$ then it is irreducible in $F[x]$.

Thm: A ring R is a UFD if and only if $R[x]$ is a UFD.

Useful results for factoring polynomials:

(1) Bezout's Thm: If F is a field and $f \in F[x]$ then an element $\alpha \in F$ is a root of f if and only if $(x-\alpha) \mid f(x)$.

Pf: If $(x-\alpha) \mid f(x)$ then $f(x) = (x-\alpha) g(x)$

$\Rightarrow f(\alpha) = (\alpha - \alpha) g(\alpha) = 0$.

(divn alg.)

If $f(\alpha) = 0$: write $f(x) = (x-\alpha) q(x) + r(x)$, with $r = 0$ or $\deg r < \deg (x-\alpha)$. Then $f(\alpha) = 0$

$\Rightarrow r(\alpha) = 0 \rightarrow r = 0 \Rightarrow (x-\alpha) \mid f(x)$. ∎

Cor: If is a field then any non-zero poly. $f \in F[x]$ has at most $\deg(f)$ roots.

(2) Abel's Thm: Suppose F is a field, $f, g \in F[x]$, and f is irreducible. Then either $f \mid g$ or $\gcd(f, g) = 1$.

Cor: F is a field, $f, g \in F[x]$ are both monic (leading coeff $= 1$) and irred. Then either $f = g$ or $\gcd(f, g) = 1$.

(3) Lemma: If f is a poly. with coeffs. in a field F and if $\deg(f) = 2$ or 3 then f is irred. over F if and only if f has no roots in F.

Lemma: Suppose $f \in \mathbb{Z}[x]$ is given by

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad a_i \in \mathbb{Z}, \; a_n \neq 0.$$

If $f(p/q) = 0$ for some $p/q \in \mathbb{Q}$ with $(p, q) = 1$ then $p \mid a_0$ and $q \mid a_n$.

Lemma: If F is a field, $f, g \in F[x]$, $\deg f, \deg g \geq 1$, and $f(x) = g(x + \lambda)$ for some $\lambda \in F$, then f is irred. if and only if g is.

(4) Reduction test: Suppose that R is an ID and that $I \subseteq R$ is a proper ideal, and that $f \in R[x]$ is a non-constant monic polynomial. If the image of $f(x)$ in $(R/I)[x]$ is irred. then f is irred. in $R[x]$.

Eisenstein's criterion over $\mathbb{Z}$: Suppose $f \in \mathbb{Z}[x]$,

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad \gcd(a_0, \dots, a_n) = 1,$$

that p is a prime number, $p \mid a_i$ $0 \leq i < n$, $p \nmid a_n$, and $p^2 \nmid a_0$. Then f is irred. over $\mathbb{Z}$ (and therefore over $\mathbb{Q}$ by Gauss's lemma).