Math 332 Thursday 4/16/09

Quiz Let R be a commutative ring with 1.

1. Show that an ideal $I \subsetneq R$ is maximal iff R/I is a field.
2. Show that if R is a domain and $p \in R$ is prime, then p is irreducible.

Thm. In a PID, an ideal is prime iff it's maximal.

Pf/ A maximal ideal is always prime: Let I be an ideal in any (commutative ring w/ 1) R. Then I is maximal iff R/I is a field. So I maximal $\Rightarrow$ R/I field $\Rightarrow$ R/I a domain $\Rightarrow$ I prime.

The converse does not hold in general: $(x) \subseteq k[x,y]$ is prime but not maximal since $k[x,y]/(x) \cong k[y]$ is a domain but not a field (or note $(x) \subsetneq (x,y) \subsetneq k[x,y]$).
Thus, the hypothesis the R is a PID is needed.

Suppose R is a PID and I is prime. Then $I = (r)$ where r is prime, hence, irreducible. Say J is an ideal with $J \supsetneq (r)$. Since R is a PID, $J = (s)$ for some $s \in R$. Then $(s) \supset (r) \Rightarrow r = st$ for some t. Since $(s) \neq (r)$, the element t is a non-unit. It follows that s is a unit, since r is irreducible. Thus, $J = R$. We've shown $I = (r)$ is maximal. $\square$

Summary Let R be a commutative ring w/ 1, and let $r \in R$.

* r prime $\Leftrightarrow$ (r) prime
* r prime $\Rightarrow$ r irreducible
* r irreducible $\Rightarrow$ r prime if R is a PID, but not in general.
* If $I \subseteq R$ is an ideal, then I maximal $\Rightarrow$ I prime.
  If R is a PID, then I prime $\Rightarrow$ I maximal.

First tricks for factoring Polynomials

Thm. (Gauss' lemma) If $f \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.

Pf/ See Thm. 35.7 in our text. □

Thm. (Dedekind?) Let $f \in \mathbb{Z}[x]$ with $\deg f \geq 1$, and let $p \in \mathbb{Z}$ be prime. Let $\bar{f} \in \mathbb{Z}_p[x]$ be the polynomial obtained by reducing the coefficients of f modulo p. Then if $\deg f = \deg \bar{f}$, we have $\bar{f}$ irred in $\mathbb{Z}_p[x] \Rightarrow f$ irred. in $\mathbb{Q}[x]$.

Pf/ Suppose f reducible in $\mathbb{Q}[x]$. Then by Gauss' lemma, it reducible in $\mathbb{Z}[x]$, so $\exists$ nonconstant g, h with integer coefficients s.t. $f = gh$. But then $\bar{f} = \bar{g}\bar{h}$ in $\mathbb{Z}[x]$ and $\deg f = \deg g + \deg h = \deg \bar{f} = \deg \bar{g} + \deg \bar{h} \Rightarrow$ $\bar{g}, \bar{h}$ non-constant. □

Example x^3+x+1 is irreducible / $\mathbb{Q}$ since it's irreducible mod 2:

If it factored in $\mathbb{Z}_2$, it would need to have a linear factor, hence a zero.

But $0^3+0+1=1$ and $1^3+1+1=1$ mod 2.

Example By the same reasoning $x^3+(\text{even})x^2+\text{odd}(x)+\text{odd}$ is irreducible / $\mathbb{Q}$.

Example x^4+1 is irreducible over $\mathbb{Q}$ but reducible / $\mathbb{Z}_p$ $\forall$ primes p.

Pf/ HW. □

Thm. (Eisenstein's criterion, 1850) Let $f(x)=\sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. If there is a prime p such that $p \nmid a_n$, $p \mid a_i$ for $i=0,\dots,n-1$, and $p^2 \nmid a_0$, then f is irreducible over $\mathbb{Z}$ (hence, $\mathbb{Q}$).

Example $3x^5+25x^3+5x^2+10x+15$ is irreducible by Eisenstein's criterion with $p=5$.

Pf of Eisenstein's criterion / Say $f = (\underbrace{b_s x^s + \cdots + b_0}_{g})(\underbrace{c_t x^t + \cdots + c_0}_{h})$, and suppose we can find p as in the statement. Then $a_0 = b_0 c_0$, $p \mid a_0$, $p^2 \nmid a_0 \Rightarrow$ we may assume $p \mid b_0$, $p \nmid c_0$. On the other hand $a_n = b_s c_t$ and $p \nmid b_s c_t$ $\Rightarrow p \nmid b_s$. Let r be the least integer such to $p \nmid b_r$. So $n \geq r > b_0$.

We have $a_r = b_r c_0 + b_{r-1} c_1 + \cdots + b_0 c_r$. Now $p \mid b_i$ for $i < r$ and if $r < n$, $p \mid a_r$. So if $r < n$, we have $p \mid b_r c_0$, but $p \nmid c_0$. So $p \mid b_r$, a contradiction. So $r = n$. But then $s = n \Rightarrow \deg h = t = 0 \Rightarrow h$ is a unit. $\square$

Cor. (p^{th} cyclotomic polynomial) Let p be a prime. Then

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 \quad \text{is irreducible over } \mathbb{Q}.$$

Pf / This is a tricky application of Eisenstein's criterion. If $\Phi_p(x+1) = g(x)h(x)$, then $\Phi_p(x) = g(x-1)h(x-1)$. Thus, $\Phi_p(x)$ is irreducible iff $\Phi_p(x+1)$ is irreducible.

Now $\Phi_p(x+1) = \dfrac{(x+1)^p - 1}{(x+1) - 1} = \dfrac{x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \cdots + p + 1 - 1}{x} = x^{p-1} + px^{p-2} + \cdots + p.$

Easy fact: $p \mid \binom{p}{k}$ for $1 \leq k < p$. So we are done by Eisenstein. $\square$

UFD

Def. A domain R is a **unique factorization domain (UFD)** if every non-zero non-unit can be written uniquely as a product of irreducible elements (not counting the order of the factors and units).

Summary of results

* PID $\Rightarrow$ UFD (Hence, $k[x]$ is a UFD (for k a field). Also $\mathbb{Z}[x]$ is a UFD.)
* R a UFD $\Rightarrow$ $R[x]$ a UFD. (Hence, $k[x_1,\dots,x_n]$ is a UFD.)
* In a UFD, prime $\Leftrightarrow$ irreducible.

Pf/ prime $\Rightarrow$ irreducible in any domain. So we only need show the converse. Suppose R is a UFD and $r \in R$ is irreducible. Suppose $r \mid (ab)$. Then $ab = rs$. Factor a, b, s into irreducibles. By uniqueness of factorization, r must be a factor of a or b. $\square$

GRÖBNER BASES: See the Gröbner basis handout.