Math 332 Tuesday April 13

* Return HW * discuss – don't forget splitting problem from previous HW.
* Quiz: see homepage

Last time Division algorithm: given $f, g \in k[x]$, $g \neq 0$, $\exists! q, r \in k[x]$ s.t.

$$f = qg + r \quad \text{with} \quad \deg r < \deg g.$$

Outline of the rest of the semester
- primes, irreducibles, factoring, UFDs
- Gröbner bases
- field theory? Factoring over finite fields? Sandpiles?

Cor. $k[x]$ is a PID.

Pf/ Let $I \subseteq k[x]$ be an ideal. If $I = (0)$, it's principal. If $I \neq (0)$, take a polynomial $g \in I \setminus \{0\}$ of least degree. Claim: $I = (g)$. Let $f \in I$.

By the division algorithm, $\exists q, r \in k[x]$ such that $f = qg + r$ with $\deg r < \deg g$.

Then $r = f - qg \in I$. By minimality of $\deg g$, we need $r = 0$. Hence, $f = qg \in (g)$. □

Cor. If $f \in k[x]$ and $a \in k$, then $f(a) = 0 \iff x - a$ divides f.

Pf/ ($\Leftarrow$) If $x - a$ divides f, then $f(x) = (x-a)q(x)$ for some $q \in k[x]$. Then

$$f(a) = (a-a)q(a) = 0.$$

($\Rightarrow$) Use the division algorithm to write $f(x) \overset{\star}{=} (x-a)\,q(x) + r(x)$ with $\deg r < 1$.
Thus, r is a constant. If $f(a) = 0$, then $\star \Rightarrow r(a) = 0 \Rightarrow r(x) = 0$

$\Rightarrow f(x) = (x-a)\,q(x)$. $\square$

Cor. If $f(x) \in k[x]$, $f \neq 0$, then $Z(f)$ is finite.

Pf/ We prove this by induction. If f is constant, then since $f \neq 0$, it has no zeros. Now suppose $\deg f = d > 0$. If $a \in k$ is a zero of f, we can write $f = (x-a)q$ where $\deg q = d-1$. For $b \in k$, $b \neq a$, we have $f(b) = 0$ iff $q(b) = 0$, i.e. $Z(f) = Z(x-a) \cup Z(q) = \{a\} \cup Z(q)$
By induction q has a finite number of zeros. $\square$

Irreducibles, Primes, UFDs

Let R be a commutative ring with 1.

Def. $r \in R$ is **irreducible** if it is nonzero, not a unit, and whenever $r = st$ with $s, t \in R$, then s or t is a unit.

(So an irreducible element cannot be factored non-trivially).

Examples

* The irreducible elements of $\mathbb{Z}$ are the primes.
* $2x+6$ is reducible as an element of $\mathbb{Z}[x]$ but not as an element of $\mathbb{Q}[x]$.

Def. If $a, b \in R$, then a **divides** b, denoted $a \mid b$, if $\exists c \in R$ s.t. $b = ac$.

Def. A nonzero, non-unit element $p \in R$ is **prime** if $\forall a, b \in R$, $p \mid (ab) \Rightarrow p \mid a$ or $p \mid b$.

Example 2 is prime in $\mathbb{Z}$ but not in $\mathbb{Z}[i]$: $2 = (1+i)(1-i)$.

Prop. $p \in R$ is prime iff (p) is a prime ideal.

Pf/ Exercise. □

Prop. In a domain, prime $\Rightarrow$ irreducible.

Pf/ Let p be a prime in a domain R, and suppose $p = st$ with $s, t \in R$. Then, $p \mid (st)$. Since p is prime, we may assume $p \mid s$, i.e. $s = up$ for some $u \in R$. But then $s = up = ust \Rightarrow s(1-ut) = 0 \Rightarrow 1 - ut = 0 \Rightarrow ut = 1 \Rightarrow t$ is a unit. $\square$

Example In general, irreducible $\not\Rightarrow$ prime. For example, $2 \in \mathbb{Z}[-5] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is irreducible not prime

Pf/ To see 2 is irreducible, suppose $2 = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Then, multiplying by conjugates gives $4 = \alpha\bar{\alpha}\beta\bar{\beta}$. If $\alpha\bar{\alpha} = 1$ or $\beta\bar{\beta} = 1$, then α or β is a unit. Otherwise, $\alpha\bar{\alpha} = \beta\bar{\beta} = 2$. Say $\alpha = a + b\sqrt{-5}$. Then $2 = \alpha\bar{\alpha} = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 - 5b^2$. Working modulo 5, we get

$$2 = a^2 - 5b^2 = a^2 \mod 5.$$

But 2 is not a square mod 5.

To see 2 is not prime, note that that $(1-\sqrt{-5})(1+\sqrt{-5}) = 6$, so $2 \mid (1-\sqrt{-5})(1+\sqrt{-5})$. But 2 does not divide $1 \pm \sqrt{-5}$:

$$(1 \pm \sqrt{-5}) = 2(a+b\sqrt{-5}) \Rightarrow 1 \pm \sqrt{-5} = 2a + 2b\sqrt{-5} \Rightarrow 2a = 1 \Rightarrow a = \tfrac{1}{2} \notin \mathbb{Z}. \square$$

Thm. Let R be a PID, and let $r \in R \setminus \{0\}$. Then r is irreducible iff r is prime.

Pf/ We've already seen that prime $\Rightarrow$ irreducible. Conversely, suppose r is irreducible and suppose $r \mid ab$ for some $a, b \in R$ with $r \nmid a$. Consider the ideal $I = (a, r)$. Since $r \nmid a$, we have $a \notin (r)$, hence, $I \supsetneq (r)$. Since R is a PID, $\exists\, c \in R$ s.t. $I = (c)$. So $(c) \supsetneq (r) \Rightarrow r = cd$ for some d where d is not a unit (otherwise, $(c) = (cd) = (r)$). Since r is irreducible, c is a unit, and hence $(a, r) = (c) = R$. So we can write $1 = ua + vr$. It follows that $b = uab + vrb$, and since $r \mid uab$ and $r \mid vrb$, $r \mid b$, as required. $\square$