Math 494

Yiwei Fu

Feb 01, 2022

Last time:

Theorem (Bezout's theorem)**.** *If $f(x,y)$ and $g(x,y)$ are polynomials in $\mathbb{C}[x,y]$ with no (non-constant) common factor. Then they only have finitely many common zeros in $\mathbb{C}\times\mathbb{C}$.*

In fact

$$\#\textit{of zeros} \leq (\textit{total deg of } f(x,y)) \cdot (\textit{total deg of } g(x,y)).$$

Note: every nonzero element of $(\mathbb{C}(y))[x]$ can be written as $\frac{a(y)}{b(y)} \cdot H(x,y)$ where $a,b \in \mathbb{C}[y]\setminus\{0\}$ and $H(x,y) \in \mathbb{C}[x,y]$ is note divisible by any nonconstant polynomial in $\mathbb{C}[Y]$.

Proof. In $(\mathbb{C}(y))[x]$, $(f,g) = (h)$ with $h \in \mathbb{C}[x,y], h$ not divisible by any nonconstant polynomial in $\mathbb{C}[y]$.

$\implies rf + sg = h, r, s \in (\mathbb{C}(y))[x] \implies r_1 f + s_1 g = hv$, we may assume $u, r_1, s_1 \in \mathbb{C}[x,y]$ have no common factor.

If $h = 1$ then $r_1 f + s_1 g = u$. So any common root (x_0, y_0) of f and g would have $u(y_0) = 0$. $(u \neq 0)$ So there are finitely many possibilities for y_0. Look at x_0, if they sample process also result in $h = 1$, there are finitely many possibilities for x_0.

Now show $h = 1$. Otherwise $h \mid f$ in $(\mathbb{C}(y))[x]$.

$$h\frac{a(y)}{b(y)}H(x,y) = f \implies h(x,y)a(y)H(x,y) = f(x,y)b(y)$$

where $a,b \in \mathbb{C}[y]$ coprime, $b \neq 0$. $H \in \mathbb{C}[x,y]$ not divisible by any nonconstant polynomial in $\mathbb{C}[y]$.

If $b(y)$ is nonconstant then it has a root $\beta \in \mathbb{C}$. Evaluate at $y = \beta$ gives

$$h(x,\beta)\alpha(\beta)H(x,\beta) = 0$$

while all three are nonzero by assumption, which is a contradiction.

Therefore $b(y)$ is constant $\implies h \mid f$ in $\mathbb{C}[x,y]$. Similarly $h \mid g$ in $\mathbb{C}[x,y]$, a contradiction.

■

Factorization (in an Integral Domain)

Suppose R an integral domain.

$$u \in R^* \iff (u) = (1),\ u = 0 \iff (u) = (0).$$

u is irreducible (u is nonzero, not a unit, not a product of two nonzero non-units) $\iff$ $(0) \subsetneq (u) \subsetneq (1)$ (there is no principal ideal strictly between (u) and (1).)

u is reducible $\iff (0) \subsetneq (u) \subsetneq (a) \subsetneq (1)$ for some $a \in R$.

Definition. A "PID" (principle integral domain) is an integral domain in which all ideals are principal

Definition. u is prime $\iff u \notin R^*, [u \mid ab \implies u \mid a$ or $u \mid b]$.

Lemma. *If R is an integral domain and $u \in R$ is a non-zero prime then u is irreducible.*

Proof. Otherwise u is reducible $\implies u = ab$, $a, b \neq 0$, $a, b \in R^*$. u is prime $\implies u \mid a$ or $u \mid b$. Assume $u \mid a \implies uv = a \implies u = ab = uvb \implies vb = 1 \implies b$ is a unit, a contradiction. ■

Lemma. *If R is PID and $u \in R$ is irreducible then u is prime.*

Proof. Suppose $u \mid ab$. Then $(u, a) = (h)$. So $h \mid u$. If $h \notin R^*$ then $u = h \cdot \text{unit} \implies u \mid h$, but $h \mid a \implies u \mid a$.

If $h \in R^*$ then $\exists x, y \in R\ s.t.\ ux + ay = 1$. Multiply by b we have $uxb + aby = b$. $u \mid uxb, u \mid aby \implies u \mid b$. ■

Note: If $u \in R$ is prime then $u \mid a_1 a_2 \ldots a_k \implies u \mid a_i$ for some i (by induction). If in addition all a_i's are irreducible then $u = a_i{\cdot}$unit for some i.

Lemma. *If R is an integral domain where all irreducible elements are prime, then any nonzero element of R has at most one prime factorization. (up to equivalence i.e. if $p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_\ell$ with p_i, q_j irreducible in R then $k = \ell$ and $\exists \sigma$ a permutation, $p_i = q_{\sigma(i)} \cdot$ unit, $\forall i$.)*

Proof. If $p_1 \ldots p_k = q_1 \ldots q_\ell, p_i, q_j$ irreducible. Then $p_1 \mid q_1 \ldots q_\ell \implies p_1 = q_j \cdot$ unit for some j.

Hence

$$p_2 p_3 \dots p_k = \text{unit} \cdot \prod_{r \neq j} q_r.$$

Then induct. ∎

Next time: If R is PID (or more generally, every ideal in R is finitely generated), then every nonzero non-unit in R is a product of primes. ($\implies$ PID's are UFD's)

Definition. An integral domain R is Euclidean if $\exists \phi : R \to \{-\infty\} \cup \mathbb{Z}_{\geq 0}$ $s.t.$ $\forall a, b \in R$ with $b \neq 0$, $\exists q, r \in R$ $s.t.$ $a = bq + r$ and $\phi(r) < \phi(b)$.

Example. $R = \mathbb{Z}$, $\phi(n) = |n|$. $R = k[x]$, $\phi(f) = \deg(f)$.

Lemma. *$\mathbb{Z}[i]$ is Euclidean with $\phi(x) = |x|^2, a + bi \mapsto a^2 + b^2$.*

Here ϕ is multiplicative.

Proof. Given $a, b \in \mathbb{Z}[i], b \neq 0$, want $q, r \in \mathbb{Z}[i]$ $s.t.$ $a = bq + r, |r| < |b|$. Equivalently:

$$\frac{a}{b} = q + \frac{r}{b}, \ \left|\frac{r}{b}\right| < 1.$$

Clearly $\forall \alpha \in \mathbb{C}, \exists q \in \mathbb{Z}[i]$ $s.t.$ $\alpha - q = u + vi$ ($u, v \in \mathbb{R}, |u|, |v| \leq \frac{1}{2} \implies |u + vi| < 1$).

If $\alpha \in \mathbb{Q}[i]$ then $u, v = \mathbb{Q}$. So write $u + vi = \frac{r}{b}$ then $|r| < |b|$ and $a = bq + r$. ∎

Fun fact: $x^2 + x + 41$ is prime for $x = 0, 1, \dots, 39$ and this statement is equivalent to $\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$ being a unique factorization domain.