Introduction to Rings and Modules

Lecture 11, Wednesday May 24 2023

Ari Feiglin

For the sake of this lecture, the ring R will always be an integral domain. Recall then that if $f, g \in R[x]$ then $\deg(fg) = \deg f + \deg g$, and $R[x]^\times = R^\times$.

Example 11.0.1:

Notice that for example $2x + 2 = 2(x + 1)$ is not a factorization in $\mathbb{Q}[x]$ since 2 is invertible, but it is a factorization in $\mathbb{Z}[x]$.

Definition 11.0.2:

A polynomial $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ is called **primitive** if $(a_0, \dots, a_n)$ is equal to R.

Proposition 11.0.3:

If f is primitive then for every factorization $f = gh$, $\deg g, \deg h \geq 1$.

Proof:

Suppose not. Then without loss of generality, $\deg h = 0$ and so h is simply a constant. Suppose $g = b_n x^n + \cdots + b_0$ then

$$f = hb_n x^n + \cdots + hb_0$$

Since $(hb_0, \dots, hb_n) \subseteq (h)$, and since this is a factorization, h is not invertible and therefore $(h) \neq R$. But this contradicts f being primitive. ■

Definition 11.0.4:

If $f \in R[x]$, then $\alpha \in R$ is called a **root** of f if $f(\alpha) = 0$. Or more formally, if $f = a_n x^n + \cdots + a_0$ then $f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0$.

Proposition 11.0.5:

If F is a field and $f \in F[x]$ is a polynomial where $\deg f \geq 1$. Then f has a linear component (meaning $\deg f = 1$ or f has a factorization where one of the components has degree one) if and only if f has a root.

Proof:

Suppose f has a linear component, then $f = (a_1 x + a_0)g$. Take $\alpha = -\frac{a_0}{a_1}$, then $f(\alpha) = (-a_0 + a_0)g(\alpha) = 0$, so f has a root.
Suppose f has a root α. Recall that $F[x]$ is a Euclidean domain whose norm is the degree of the polynomial, and so there exists $g, r \in F[x]$ such that

$$f = (x - \alpha)g + r$$

such that $\deg r < \deg(x - \alpha) = 1$, so $\deg r = 0$ meaning r is constant. But since α is a root,

$$0 = f(\alpha) = (\alpha - \alpha)g + r \implies r = 0$$

So $f = (x - \alpha)g$ as required (note that g may be constant as well). ■

The requirement for $\deg f \geq 1$ is more to ignore edge cases which arise when $f = 0$. The above proposition is technically true for every $f \in R[x]$, but if $f = 0$ the concept of a root and a linear component are meaningless.

Lemma 11.0.6 (Gauss's Lemma):

Let R be a UFD, and $F = \operatorname{Frac} R$ (where $\operatorname{Frac} R = S^{-1}R$ where $S = R \setminus \{0\}$, this is a field since R is an integral domain). Let $f \in R[x]$ primitive, then f is irreducible over $R[x]$ if and only if it is irreducible over $F[x]$.

We will prove this next lecture.

Corollary 11.0.7:

Let R be a UFD and $f \in R[x]$ be a primitive polynomial of degree 2 or 3. Then f is reducible over R if and only if it has a root in F.

Proof:

Let $F = \operatorname{Frac} R$. We will show f is reducible over $F[x]$, and by **Gauss's Lemma**, this implies f is reducible over R. This is equivalent to finding g, h non-invertible (and non-trivial since f isn't trivial) such that $f = gh$. But $\deg f = \deg g + \deg h$ and since $\deg f$ is 2 or 3, either g or h must have degree 1, which is simply saying that f has a linear component. So f is reducible if and only if it has a linear component, which is equivalent to saying that f has a root in F. ■

One direction of this is true in general, if f is non-linear and has a root in F then f by definition has a linear component and is therefore reducible in F and therefore R. But the converse is not true, suppose $\deg f = 4$ then f may be able to factorize into the product of two two-degree polynomials which have no roots (for example $(x^2+2)(x^2+1)$ in $\mathbb{R}$).

Lemma 11.0.8:

If R is a UFD and the greatest common divisor of a and b is 1, then if $a|bc$ then $a|c$.

Proof:

Suppose $a = p_1^{a_1} \cdots p_n^{a_n}$, $b = p_1^{b_1} \cdots p_n^{b_n}$, and $c = p_1^{c_1} \cdots p_n^{c_n}$. We showed that if $m_k = \min\{a_k, b_k\}$ then $d = p_1^{m_k} \cdots p_n^{m_k}$ is a gcd of a and b. Since 1 is a gcd, this means that d must be invertible by the definition of a gcd. But the product of irreducible elements cannot be invertible (if $p_1 \cdots p_n = u$ then $p_1 = p_1 \cdot p_1 \cdots p_n \cdot u^{-1}$ are two factorizations) so $p_k^{m_k}$ must be equal to 1. This means that $m_k = 0$ since $p_k^{a_k - m_k} = p_k^{a_k - m_k} p_k^{m_k} = p_k^{a_k}$ so otherwise we can find another factorization of a using $a_k' = a_k - m_k$.
So for every k, either a_k or b_k is 0. Since $a|bc$ this means that $bc = xa$ and since a and b share no common irreducible factors, a must share all its factors with c (since this is a UFD), meaning $a|c$. ■

Notice that we showed if a and b are coprime, they share no irreducible factors.

Proposition 11.0.9:

Suppose R is a UFD and $f = a_n x^n + \cdots + a_0 \in R[x]$. Suppose $\alpha = \frac{r}{s} \in F = \operatorname{Frac} R$ is a root of f. Further suppose $\frac{r}{s}$ is reduced (meaning $\gcd(r, s) = 1$, which makes sense since R is a UFD, but perhaps it makes even more sense to say $1 \in \gcd(r, s)$). Then $s|a_n$ and $r|a_0$.

Proof:

Notice that

$$0 = f(\alpha) = \sum_{k=0}^{n} a_k \frac{r^k}{s^k}$$

Multiplying both sides by s^n gives

$$0 = \sum_{k=0}^{n} a_k r^k s^{n-k} \implies -a_n r^n = \sum_{k=0}^{n-1} a_k r^k s^{n-k} = s\left(\sum_{k=0}^{n} a_k r^k s^{n-1-k}\right)$$

This means that s divides $a_n r^n$, but since s and r are coprime (and therefore s and r^n are coprime since they share no factors), this means by our lemma above that s divides a_n. Similarly we get

$$-a_0 s^n = r\left(\sum_{k=1}^{n} a_k r^{k-1} s^{n-k}\right)$$

and so r divides $a_0 s^n$ and since r and s are coprime, r divides a_0 as required. ■

Notice that this can help us limit the number of possible roots to look for in certain rings and specific polynomials.

Proposition 11.0.10 (Eisenstein's Criterion):

Let R be an integral domain, and $P \triangleleft R$ be a prime ideal. Let $f = x^n + \cdots + a_0 \in R[x]$ and suppose $a_0, \ldots, a_{n-1} \in P$, but $a_0 \notin P^2 = P \cdot P$, then f is irreducible over R.

Proof:

Suppose that there is a factorization $f = gh$, where the coefficients of g are b_k and h's are c_k. The free coefficient of f is a_0 and the free coefficient of gh is $b_0 c_0$, so $b_0 c_0 = a_0 \in P$. Since P is prime, this means that $b_0 \in P$ or $c_0 \in P$. But since $a_0 \notin P^2$, they cannot both be in P. Without loss of generality suppose $b_0 \in P$ and $c_0 \notin P$.
Inductively we can see that $b_k \in P$ for every k:

$$a_k = \sum_{i=0}^{k} b_i c_{k-i}$$

for $i < k$, $b_i \in P$ and so $b_i c_{k-i} \in P$. So

$$b_k c_0 = a_k - \sum_{i=0}^{k-1} b_i c_{k-i} \in P$$

and since $c_0 \notin P$ this means that $b_k \in P$. There is an issue when $k = n$ since $a_n = 1 \notin P$, but since this is a factorization if $n = k$ then h is a non-invertible constant. But the leading coefficient of g times h must be equal to $a_n = 1$, so h would then be invertible. So $k < n$.
Suppose $\deg g = k < n$ then $\deg h = n - k$. Then comparing the leading coefficients we have

$$a_n = 1 = b_k c_{n-k}$$

But since $b_k \in P$ this means that $1 \in P$ which is a contradiction (P is prime, so $P \neq R$). ■

This argument works if the leading coefficient of f is invertible. But otherwise, it may fail.

Proposition 11.0.11:

If $I \triangleleft R$, and we take the canonical homomorphism

$$\varphi\colon R \longrightarrow {}^{R}\!/_{I}, \quad x \mapsto x + I = \overline{x}$$

then this defines a homomorphism

$$\varphi\colon R[x] \longrightarrow \left({}^{R}\!/_{I}\right)[x], \quad f = \sum_{k=0}^{n} a_k x^k \mapsto \overline{f} = \sum_{k=0}^{n} \overline{a_k} x^k$$

Suppose f is a monic polynomial (its leading coefficient is 1), then if $\overline{f}$ is irreducible, so is f (and so if f is reducible, so is $\overline{f}$).

Proof:

Suppose there exists a factorization of f, $f = gh$. Then $\overline{f} = \overline{g} \cdot \overline{h}$, so $\overline{g}$ or $\overline{h}$ must be invertible. Without loss of generality, $\overline{h}$ is invertible. Therefore $\overline{h}$ is constant, so if $h = h_k x^k + \cdots + h_0$ then $\overline{h} = \overline{h_k} x^k + \cdots + \overline{h_0}$, so $\overline{h_i} = 0$ for

every $i > 0$.
If $\deg h = t$ and $\deg g = \ell$ then

$$a_n = 1 = g_\ell h_t$$

So g_ℓ and h_ℓ are invertible, and therefore are not in I. But then $\overline{h_t} \neq 0$, so $t = 0$, meaning h is constant. But $h_0 = h_t$ is invertible, and therefore h is invertible, so gh is not a factorization in contradiction. ■

Example 11.0.12:

The converse is not true: if $\overline{f}$ is reducible, f may not be. Take for example $x^2 + 1 \in \mathbb{Z}[x]$ which is irreducible, but if $I = 5\mathbb{Z}$ then $x^2 + [1] = (x - [2])(x + [2])$ so $x^2 + [1]$ is reducible.