FIELDS AND POLYNOMIAL RINGS

MATH 435 SPRING 2012
NOTES FROM APRIL 6TH, 2012

1. Irreducible polynomials

Throughout this section, k denotes a field. Before really starting, I'd like to point out a couple lemmas. The first ties together the notions of ideal containment and elements dividing each other.

Lemma 1.1. *Given any elements f, g in an integral domain with unity R, we have that $f|g$ if and only if $\langle g \rangle \subseteq \langle f \rangle$.*

Proof. if $f|g$, then $g = uf$ for some $u \in R$. But then $rg = (ru)f \in \langle f \rangle$ for any $r \in R$. Thus $\langle g \rangle \subseteq \langle f \rangle$. Conversely, if $\langle g \rangle \subseteq \langle f \rangle$ then $g \in \langle f \rangle$ and thus $g = uf$ for some $u \in R$. Thus $f|g$ as desired. □

The next lemma explains when principal ideals are equal to the whole ring.

Lemma 1.2. *Suppose that R is a commutative ring with unity and $f \in R$. Then $\langle f \rangle = R$ if and only if f is invertible.*

Proof. If $\langle f \rangle = R$, then $1 \in \langle f \rangle$ since $1 \in R$. Thus there exists $r \in R$ such that $rf = 1$, but this implies that f is invertible.

Conversely, if f is invertible with inverse f^{-1}, then $1 = f{-}1f \in \langle f \rangle$. But then for any element $r \in R$,

$$r = r \cdot 1 \in \langle f \rangle$$

which implies that $R = \langle f \rangle$ as well. □

We begin with a definition of an irreducible element.

Definition 1.3. Suppose that $f \in k[x]$ is a non-zero non-invertible element. Then we say that f *is irreducible* if any of the following equivalent conditions hold (note that if one of them hold, then all of them hold).

1. For every element $v \in k[x]$, either $\gcd(f, v) = 1$ or $f|v$.
2. If $f|(ab)$ for some elements $a, b \in k[x]$, then either $f|a$ or $f|b$.
3. If $f = gh$ for some elements $g, h \in k[x]$, then either g or h invertible.
4. The ideal $\langle f \rangle$ is maximal.
5. The quotient ring $k[x]/\langle f \rangle$ is a field.

Proof that the definitions above are equivalent. Certainly conditions 4. and 5. are equivalent.

First we show that 1. $\Rightarrow$ 2. Suppose then that $f|(ab)$ and f does not divide a and f does not divide b. We write $ab = fu$ for some $u \in k[x]$. Since f does not divide a, we must have $\gcd(f, a) = 1$. Thus there exists $s, t \in k[x]$ such that $sf + ta = 1$. Multiplying through by b, we get

$$sfb + tab = b$$

and so $sfb + tfu = b$. Factoring out an f, we get that $f(sb + tu) = b$ and so f divides b, a contradiction.

Now we show that 2. $\Rightarrow$ 3. Indeed, suppose now that $f = gh$. Then since $f|(gh)$, we have that $f|g$ or $f|h$. In other words, either $g = sf$ or $h = tf$ for some s or $t \in R$. In the first case, we obtain

$$f = gh = (sf)h$$

which implies that $1 = sh$ which proves that h is invertible. In the second case, we obtain

$$f = gh = g(tf)$$

which implies that $1 = gt$ which proves that g is invertible. Thus either g or h is invertible, as desired.

Next we show that 3. $\Rightarrow$ 1. which will prove the equivalence of 1., 2., and 3. Thus choose $v \in k[x]$ and suppose that $1 \neq d = \gcd(f, v)$ and that f does not divide v. But since $d|f$, we have that $f = du$ for some $u \in k[x]$. Thus either d or u is invertible. We will obtain a contradiction in either case.

- u **is invertible:** In this case, $d = fu^{-1}$ and $f|d$. But note $d|v$ and so $f|v$ as well. But this is a contradiction.
- d **is invertible:** In this case, $\deg d = 0$ and so d is a monic polynomial of degree 0, in other words, $d = 1$, a contradiction.

Now we prove that 4. (or 5.) are equivalent to 1., 2. and 3. Suppose that 5. holds, thus $\langle f \rangle$ is in particular a prime ideal. We will show that 2. holds. Indeed, suppose that $f|(ab)$ for some $a, b \in k[x]$. Then $ab \in \langle f \rangle$ which implies that either $a \in \langle f \rangle$ or $b \in \langle f \rangle$, since $\langle f \rangle$ is a prime ideal by assumption. In the first case, $f|a$ and in the second, $f|b$. But this proves that f satisfies condition 2.

Finally, we assume that condition 3. holds but that $\langle f \rangle$ is not maximal. Thus there exists an ideal $J \subseteq k[x]$ such that

$$\langle f \rangle \subsetneq J \subsetneq k[x]$$

But since $k[x]$ is a PID, $J = \langle g \rangle$ for some $g \in k[x]$ and so $f \in \langle g \rangle$. Thus there exists $h \in k[x]$ such that $f = gh$. But then either g or h is invertible. Again we consider two cases:

- g **is invertible:** In this case, $J = k[x]$ which is impossible.
- h **is invertible:** In this case, $h^{-1}f = g$ and so $f|g$ and thus $J = \langle g \rangle \subseteq \langle f \rangle$ which is also impossible.

Since both possibilities lead to contradiction, we have completed the proof. ☐

Remark 1.4. The condition 2. above is usually described as f *is prime* whereas the condition in 1. is usually described as f *is irreducible*. As we have seen, in $k[x]$ these conditions are equivalent, but for a more general integral domain with unity, they are distinct. However, the proof 2. $\Rightarrow$ 3. always holds (we didn't use any special properties of $k[x]$). In other words, every prime element is irreducible.

2. Testing for irreducibility

In this section, develop some tests to discern whether a given element is irreducible.

Proposition 2.1. *Suppose that k is a field and that $f \in k[x]$, then f has a degree 1 factor (in other words $(bx - a)|f$ for some $0 \neq b \in k$ and $a \in k$) if and only if f has a root in k.*

Proof. Indeed, suppose first that $(bx - a)|f$ for some nonzero $b \in k$ and $a \in k$. By replacing a by a/b, we may assume that $b = 1$ and thus that $(x - a)|f$. Thus $f(x) = (x - a)g(x)$ which implies that

$$f(a) = (a - a)g(a) = 0g(a) = 0$$

and thus f has a root in k.

Conversely, suppose that f has a root $a \in k$. Consider then $f(x) = (x-a)q(x) + r(x)$ for some $q(x), r(x) \in k[x]$ where $\deg r < \deg(x-a) = 1$. But then $\deg r = 0$ (or $r = 0$ itself). Thus $r(x) = r$ is a constant. Plugging in a we get

$$0 = f(a) = (a-a)q(a) + r(a) = 0 + r = r$$

Thus $r = r(x) = 0$ and so $(x-a)|f$ as desired. □

Here is an important corollary.

Corollary 2.2. *A polynomial $f(x) \in k[x]$ of degree 2 or 3 is irreducible if and only if $f(a) \neq 0$ for every $a \in k$.*

Proof. Certainly if $f(a) = 0$ then $(x-a)|f(x)$ and so f is not irreducible since then $f(x) = (x-a)g(x)$ for some $g(x)$ of degree 1 or 2 (in other words, g is not invertible).

Conversely, if $f = gh$ where neither g or h is invertible, then by degree considerations, either g or h is degree 1. Thus either g or h must be of the form $bx - c$ for some $0 \neq b, c \in k$. Thus $x - \frac{c}{b}$ also divides $f(x)$ and so $f(c/b) = 0$. This completes the proof. □