Content:

Theorem	Division Algorithm in $\mathbb{Z}$ and $k[x]$
Definition	$(a_1, a_2, \ldots, a_n)$
Example	$(2, x) = \{f(x) \mid$ constant term is even$\}$ in $\mathbb{Z}[x]$; $(2, x) = \mathbb{Q}[x]$ in $\mathbb{Q}[x]$; $(x^2, x^3) = (x^2)$ in $\mathbb{Q}[x]$
Definition	irreducible, associate, prime elements
Proposition	If $p(x) \in k[x]$, then $p(x)$ is irreducible $\Leftrightarrow$ deg $(p(x)) = n \geq 1$ and there is no factorization in $k[x]$ of the form $p(x) = f(x)g(x)$ where deg $f < n$ and deg $g < n$.
Definition	gcd in a commutative ring
Theorem	If R is a PID, $a, b \in R$, then (1) a gcd of a and b exists, (2) If d is a gcd of a and b then $\exists\ x, y \in R$ such that $d = ax + by$.

Recall Division Algorithm for $\mathbb{Z}$.
If $a, b \in \mathbb{Z}$, then $\exists!\ q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$

Division Algorithm in $k[x]$
If $f(x), g(x) \in k[x]$, then $\exists!\ q(x), r(x) \in k[x]$ such that
$f(x) = g(x)q(x) + r(x)$ where $r(x) = 0$ or deg $r(x) <$ deg $g(x)$

We used this to show $k[x]$ is a PID. We noticed the elements of smallest degree generate principal ideals.

(a) is the ideal generated by a. So if $a \in I$ and I is an ideal in R, then $(a) \subseteq I$.

Definition $(a_1, a_2, \ldots, a_n)$ is the smallest ideal containing $a_1, a_2, \ldots, a_n$.

Example Consider (2, x) in $\mathbb{Z}[x]$.
Let $I = \{f(x) \mid$constant term is even$\}$
$(2, x) = I$? Yes.

Proof:
Recall that we showed I is an ideal last term (see p. 147) and that I is not principal, hence $\mathbb{Z}[x]$ is not a PID.
So, to get $(2, x) \subseteq I$, we need only show $2, x \in I$.
Since 2 and x are polynomials with even constant term, then $2, x \in I$.
To get $I \subseteq (2, x)$, we work with an arbitrary element in I.
Let $f(x) \in I$, then $f(x) = a_n x^n + \cdots + a_1 x + 2k$ for some $k \in \mathbb{Z}$.
$= x(a_n x^{n-1} + \cdots + a_1) + 2k$.
Since $x(a_n x^{n-1} + \cdots + a_1) \in (2, x)$ and $2k \in (2, x)$, then $f(x) \in (2, x)$.
$\therefore I \subseteq (2, x)$, hence $(2, x) = I$.

Example Consider (2, x) in $\mathbb{Q}[x]$.
$(2, x) = \mathbb{Q}[x]$? Yes.

Proof:
Since ½ (2) = 1 ∈ $(2, x)$, then we get the whole ring.
Or, alternatively, since 2 is a unit, we get the whole ring.

Example Consider (x^2, x^3) in $\mathbb{Q}[x]$.
Is $(x^2, x^3) = (x^2)$? Yes.

Proof:
Note that (x^2, x^3) is an ideal that contains x^2 (i.e. $x^2 \in (x^2, x^3)$)
and (x^2) is the smallest ideal in $k[x]$ that contains x^2.
Thus $(x^2) \subseteq (x^2, x^3)$.
To show the reverse containment,
note that $x^3 = x^2 \bullet x \in (x^2)$ as $x \in k[x]$.
Thus (x^2) is an ideal in $k[x]$ that contains x^2 and x^3.
And since (x^2, x^3) is the smallest ideal in $k[x]$ that
contains x^2 and x^3, we have $(x^2, x^3) \subseteq (x^2)$.
$\therefore$ $(x^2) = (x^2, x^3)$.

Example Consider $f(x) = x^2 - 4$, $g(x) = ½ (x^2 - 4)$, and $h(x) = x^2 + 4$ in $\mathbb{Q}[x]$.
f and g have the same degree and same roots, so they very much alike. The ½ is of little consequence. But h is different from f and g as it cannot be broken down.

Definition Let R be an integral domain.
(1) Let $r \in R$. r is *irreducible* if whenever $r = pq$ then $p \in U(R)$ or $q \in U(R)$. [Here assume $r \neq 0$ and $r \notin U(R)$.]
(2) Let $a, b \in R$. We say a and b are *associates* if $a = bu$ for some $u \in U(R)$.
(3) Let $p \in R$, $p \neq 0$ and $p \notin U(R)$. We say p is a *prime* element if whenever $p|ab$, then $p|a$ or $p|b$.

Note If $g(x) = ½ f(x)$ in an integral domain, then deg g = deg ½ + deg f.
Thus, we can see that the definition of irreducible will apply if g is irreducible.

Example 3 and –3 are irreducible, associate, and prime elements in $\mathbb{Z}$.

Note Some stuff you'll explore in the homework assignment:
prime element $\Rightarrow$ irreducible but not the reverse implication
For example, since 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, and
$3 | (2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$, but $3 \nmid (2 + \sqrt{-5})$ and $3 \nmid (2 - \sqrt{-5})$.

However, if R is a PID, then irreducible $\Leftrightarrow$ prime element.

Proposition Let $p(x) \in k[x]$ (k will always denote a field now).
Then $p(x)$ is irreducible $\Leftrightarrow$ deg $(p(x)) = n \geq 1$ and there is no factorization in $k[x]$ of the form $p(x) = f(x)g(x)$ where deg $f < n$ and deg $g < n$.

Proof:
Straightforward, you can read it in the book (p. 135)
We first show that $g(x) \in k[x]$ is a unit if and only if deg $g = 0$.
Assume $g(x)$ is a unit, then $g(x)u(x) = 1$, then deg g + deg u = deg 1 = 0; since degrees are nonnegative, we have deg $g(x) = 0$.
Conversely, if deg $g(x) = 0$, then $g(x)$ is a nonzero constant; that is, $g(x) \in k$. Since k is a field, $g(x)$ has an inverse, hence $g(x)$ is a unit.
Assume $p(x)$ is irreducible, then, by definition, it is not a unit or 0, hence it has degree $n \geq 1$. And its only factorizations are of the form $p(x) = f(x)g(x)$, where $f(x)$ or $g(x)$ is a unit; that is, where either deg $f(x) = 0$ or deg $g(x) = 0$.
$\therefore$ $p(x)$ has no factorization in which both factors have smaller degree.
Conversely, assume $p(x)$ has degree $n \geq 1$ and is not irreducible. Then it has a factorization $p(x) = f(x)g(x)$, in which neither $f(x)$ nor $g(x)$ is a unit; that is, neither $f(x)$ nor $g(x)$ has degree 0.
$\therefore$ $p(x)$ has a factorization as a product of polynomials of smaller degree.

Question If $f(x)$ has no roots is $f(x)$ irreducible?
Not necessarily.
$(x^2 + 4)^2$ in $\mathbb{Q}[x]$ is reducible but has no roots.

If $f(x)$ has a root is $f(x)$ irreducible?
Maybe.
$x - 2$ has a root and is irreducible.
$(x - 2)(x^2 + 1)$ has a root and is reducible.

If the degree of a polynomial is ≥ 2, then having a root implies reducible.

3.5 p. 147

Definition Le $a, b \in R$, R a commutative ring. $d \in R$ is a gcd of a and b if
(1) $d|a$ and $d|b$
(2) Whenever $c|a$ and $c|b$, then $c|d$.

Theorem Let R be a PID. Let $a, b \in R$.
(1) A gcd of a and b exists.
(2) If d is a gcd of a and b then $\exists\ x, y \in R$ such that $d = ax + by$.

Proof:
If $a = b = 0$, then $d = 0$. Assume a and b are not both 0.
Let $I = \{ar + bs |\ r, s \in R\}$. We first will show I is an ideal.
We have $a \bullet 0 + b \bullet 0 = 0 \in I$.
Let $ar + bs, ar' + bs' \in I$. Then since R is commutative, we have
$(ar + bs) - (ar' + bs') = a(r - r') + b(s - s') \in I$.
Let $m \in R$. Then $(ar + bs)m = a(rm) + b(sm) \in I$ as $rm, sm \in R$.
$\therefore$ I is an ideal.
Since R is a PID, then $\exists\ d \in R$ such that $I = (d)$. We will show d is a gcd of a and b.
Since $a \bullet 1 + b \bullet 0 = a \in$ I, then $a = dk$ for some $k \in R$. So $d|a$.
Similarly $d|b$.
Assume $c|a$ and $c|b$, then $a = cm$ and $b = cn$ for some $m, n \in R$.
And since $d \in I$, then $\exists\ x, y \in R$ such that
$d = ax + by = cmx + cny = c(mx + ny)$.
$\therefore$ $c|d$, hence d is a gcd of a and b.

Next Time For Wednesday, think about if p is irreducible, then what could gcd(p, a) be?