2.3 Lecture 8: Reducible and Irreducible Polynomials

Theorem 21. *(The Factor Theorem) Let* $f(X)$ *be a polynomial of degree* $n \geqslant 1$ *in* $\mathbb{F}[X]$ *and let* $\alpha \in \mathbb{F}$*. Then* α *is a root of* $f(X)$ *if and only if* $X - \alpha$ *divides* $f(X)$ *in* $\mathbb{F}[X]$*.*

Proof: By the division algorithm (Theorem 18), we can write

$$f(X) = q(X)(X - \alpha) + r(X),$$

where $q(X) \in \mathbb{F}[X]$ and either $r(X) = 0$ or $r(X)$ has degree zero and is thus a non-zero element of $\mathbb{F}$. So $r(X) \in \mathbb{F}$; we can write $r(X) = \beta$. Now

$$\begin{aligned} f(\alpha) &= q(\alpha)(\alpha - \alpha) + \beta \\ &= 0 + \beta \\ &= \beta. \end{aligned}$$

Thus $f(\alpha) = 0$ if and only if $\beta = 0$, i.e. if and only if $r(X) = 0$ and $f(X) = q(X)(X - \alpha)$ which means $X - \alpha$ divides $f(X)$. □

Remark This proves more than the statement of the theorem - it shows that $f(\alpha)$ is the remainder on dividing $f(X)$ by $X - \alpha$.

Now that we have some language for discussing divisibility in polynomial rings, we can also think about factorization. In $\mathbb{Z}$, we are used to calling an integer *prime* if it does not have any interesting factorizations. In polynomial rings, we call a polynomial *irreducible* if it does not have any interesting factorizations.

Definition 22. *Let* $\mathbb{F}$ *be a field and let* $f(X)$ *be a non-constant polynomial in* $\mathbb{F}[X]$*. Then* $f(X)$ *is* irreducible *in* $\mathbb{F}[X]$ *(or irreducible over* $\mathbb{F}$*) if* $f(X)$ *cannot be expressed as the product of two factors both of degree at least 1 in* $\mathbb{F}[X]$*. Otherwise* $f(X)$ *is* reducible *over* $\mathbb{F}$*.*

NOTES:

1. Any polynomial $f(X) \in \mathbb{F}[X]$ can be factorized (in an uninteresting way) by choosing $a \in \mathbb{F}^\times$ and writing
$$f(X) = a(a^{-1}f(X).$$
This is not considered to be a proper factorization of $f(X)$.

2. Every polynomial of degree 1 is irreducible.

3. It is possible for a polynomial that is irreducible over a particular field to be reducible over a larger field. For example $X^2 - 2$ is irreducible in $\mathbb{Q}[X]$. However it is not irreducible in $\mathbb{R}[X]$, since here $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$. Therefore when discussing irreducibility, it is important to specify what field we are talking about (sometimes this is clear from the context).

4. The only irreducible polynomials in $\mathbb{C}[X]$ are the linear (i.e. degree 1) polynomials. This is basically the Fundamental Theorem of Algebra, which states that every non-constant polynomial with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$.

Let $f(X)$ be a polynomial of degree $\geqslant 2$ in $\mathbb{F}[X]$. If $f(X)$ has a root α in $\mathbb{F}$ then $f(X)$ is not irreducible in $\mathbb{F}[X]$ since it has $X - \alpha$ as a proper factor. This statement has a partial converse.

Theorem 23. *Let* $f(X)$ *be a quadratic or cubic polynomial in* $f(X)$*. Then* $f(X)$ *is irreducible in* $\mathbb{F}[X]$ *if and only if* $f(X)$ *has no root in* $\mathbb{F}$*.*

Proof: Since $f(X)$ is quadratic or cubic any proper factorization of $f(X)$ in $\mathbb{F}[X]$ involves at least one linear (i.e. degree 1) factor. Suppose that $r(X) = aX + b$ is a linear factor of $f(X)$ in $\mathbb{F}[X]$. Then we have $f(X) = r(X)g(X)$ for some $g(X)$ in $\mathbb{F}[X]$. Since $\mathbb{F}$ is a field we can rewrite this as

$$f(X) = (X + b/a)(ag(X)).$$

Thus $X - (-b/a)$ divides $f(X)$ in $\mathbb{F}[X]$ and by Theorem 21 $-b/a$ is a root of $f(X)$ in $\mathbb{F}$. □

Theorem 23 certainly does not hold for polynomials of degree 4 or higher. That is, for a polynomial of degree 4 or more, having no roots in a particular field does not mean being irreducible over that field. Give an example to demonstrate this.

In general, deciding whether a given polynomial is reducible over a field is a difficult problem. We will look at this problem in the case where the field of coefficients is $\mathbb{Q}$. The problem of deciding reducibility in $\mathbb{Q}[X]$ is basically the same as that of deciding reducibility in $\mathbb{Z}[X]$, as the following discussion will show.

Lemma 24. *For a field $\mathbb{F}$, let $a \in \mathbb{F}^\times$ and let $f(X) \in \mathbb{F}[X]$. Then $f(X)$ is reducible in $\mathbb{F}[X]$ if and only if $af(X)$ is reducible in $\mathbb{F}[X]$.*

Proof: Any factorization of $f(X)$ immediately implies a factorization of $af(X)$, and vice versa.

Note that any polynomial in $\mathbb{Q}[X]$ can be multiplied by a non-zero integer to produce a polynomial in $\mathbb{Z}[X]$. Then by Lemma 24 the problem of deciding reducibility in $\mathbb{Q}[X]$ is the same as that of deciding reducibility over $\mathbb{Q}$ for polynomials in $\mathbb{Z}[X]$.

Suppose that $f(X)$ is a polynomial with coefficients in $\mathbb{Z}$. Surprisingly, $f(X)$ has a proper factorization with factors in $\mathbb{Q}[X]$ if and only if $f(X)$ has a proper factorization with factors (of the same degree) that belong to $\mathbb{Z}[X]$. This fact is a consequence of Gauss's lemma which is discussed below. It means that a polynomial with integer coefficients is irreducible over $\mathbb{Q}$ provided that it is irreducible over $\mathbb{Z}$. This is good news because irreducibility over $\mathbb{Z}$ should be easier to decide in principle (why is this?).

Definition 25. *A polynomial in $\mathbb{Z}[X]$ is called* primitive *if the greatest common divisor of all its coefficients is 1.*

EXAMPLE
$3X^4 + 6X^2 - 2X - 2$ is primitive.
$3X^4 + 6X^2 = 18X$ is not primitive, since 3 divides each of the coefficients.

The following statement is one of many unrelated things called "Gauss's Lemma".

Theorem 26. *(Gauss's Lemma) Let $f(X)$ and $g(X)$ be primitive polynomials in $\mathbb{Z}[X]$. Then their product is again primitive.*

Proof: We need to show that no prime divides all the coefficients of $f(X)g(X)$. We can write

$$\begin{aligned} f(X) &= a_sX^s + a_{s-1}X^{s-1} + \cdots + a_1X + a_0,\ a_s \neq 0, \\ f(X) &= b_tX^t + b_{t-1}X^{t-1} + \cdots + b_1X + b_0,\ b_t \neq 0. \end{aligned}$$

Let p be a prime. Since $f(X)$ and $g(X)$ are primitive we can choose k and m to be the least integers for which p does not divide a_k and p does not divide b_m. Now look at the coefficient of X^{k+m} in $f(X)g(X)$. This is

$$a_{k+m}b_0 + \cdots + a_{k+1}b_{m-1} + a_kb_m + a_{k-1}b_{m+1} + \cdots + a_0b_{k+m}.$$

Since $p|b_i$ for $i < m$ and $p|a_i$ for $i < k$, every term in the above expression is a multiple of p except for a_kb_m which is definitely not. Thus p does not divide the coefficient of X^{k+m} in $f(X)g(X)$, p does not divide all the coefficients in $f(X)g(X)$ and $f(X)g(X)$ is primitive. □