Math 521A

4.3 – Irreducibles and Unique Factorization

Theorem

Let R be an integral domain. Then $f(x) \in R[x]$ is a unit if and only if $f(x)$ is a constant polynomial that is a unit in R.

The proof is on the board.

Corollary

Let F be a field. Then $f(x) \in R[x]$ is a unit if and only if $f(x) = c$ where $c \in F$ is nonzero.

Example

$$\{\text{units of } \mathbb{Z}[x]\} = \{-1, 1\};$$
$$\{\text{the units of } \mathbb{Q}[x]\} = \mathbb{Q} \setminus \{0\}.$$

Remark: The above theorem is not true if R is not an integral domain: For example, $1 + 3x$ is a unit in $\mathbb{Z}_9[x]$ because

$$(1 + 3x)(1 + 6x) = 1 \text{ in } \mathbb{Z}_9[x].$$

Definition (Associate Elements in a Ring)

Let R be a commutative ring with identity. Elements a and b in R are said to be associates if there exists a unit $u \in R$ such that $a = bu$. For example, in $\mathbb{Z}_{10}$, 4 and 6 are associates because $6 = 4 \cdot 9$ and 9 is a unit in $\mathbb{Z}_{10}$.

Now let F be a field. In view of the above definition, $f(x), g(x) \in F[x]$ are associates if $f(x) = cg(x)$ for some $c \neq 0$ in F. From the previous slide, note that the only units in $F[x]$ are the nonzero constant polynomials.

Definition (Reducible and Irreducible Polynomials)

A nonconstant polynomial $p(x) \in F[x]$ is said to be irreducible if its only divisors are its associates and the nonzero constant polynomials (the units of $F[x]$). A nonconstant polynomial that is not irreducible is said to be reducible.

- Equivalently, $f(x) \neq 0$ in $F[x]$ is reducible if and only if $f(x) = f_1(x) \cdot f_2(x)$ where
$$0 < \deg f_1(x) \leq \deg f_2(x) < \deg f(x).$$
- In view of the latter observation, the polynomial $f(x) = ax + b$ with $a \neq 0$ is always irreducible in $F[x]$.
- When talking about irreducibility, one must specify "where": For example, $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$ and in $\mathbb{R}[x]$, but it is reducible in $\mathbb{C}[x]$ because $x^2 + 1 = (x + i)(x - i)$ where $i = \sqrt{-1}$. Also, $x^2 + 1 = (x + 1)(x + 1) = (x + 1)^2$ in $\mathbb{Z}_2[x]$, hence $x^2 + 1$ is reducible in $\mathbb{Z}_2[x]$.

Theorem

Let F be a field and $p(x) \in F[x]$ a non-constant polynomial. The following are equivalent:

(1) *$p(x)$ is irreducible.*

(2) *$p(x)|b(x)c(x) \Rightarrow p(x)|b(x)$ or $p(x)|c(x)$.*

(3) *$p(x) = r(x)s(x) \Rightarrow r(x)$ or $s(x)$ equals a nonzero constant.*

Corollary

Let $p(x)$ be an irreducible polynomial in $F[x]$ and suppose $p(x)|a_1(x)\cdots a_n(x)$. Then $p(x)|a_i(x)$ for some i, $1 \leq i \leq n$.

Theorem

Let F be a field. Every nonconstant polynomial $f(x) \in F[x]$ is a product of irreducible polynomials in $F[x]$. This factorization is unique in the following sense: If

$$f(x) = p_1(x)p_2(x)\cdots p_r(x) \text{ and } f(x) = q_1(x)q_2(x)\cdots q_s(x)$$

with each $p_i(x)$ and $q_j(x)$ irreducible, then $r = s$, and after reordering, $p_i(x) =$ associate of $q_i(x)$, $i = 1, \ldots, r$.