Math 403 Chapter 17: Factorization of Polynomials

1. **Introduction:** The notion of factorization of polynomials depends heavily on the ring in question. For example consider $p(x) = 2x + 2$. In $\mathbb{Z}[x]$ we can factor this as $2x + 2 = 2(x + 1)$ but in $2\mathbb{Z}[x]$ we cannot factor it. What we do in this section is work out some specifics.

2. **Reducibility**

   (a) **Definition:** Let D be an integral domain and let $f(x)$ be a non-zero non-unit in $D[x]$, we say that $f(x)$ is *reducible over* D if we can factor $f(x) = g(x)h(x)$ where both $g(x)$ and $h(x)$ are non-units. Otherwise we say that $f(x)$ is irreducible over D.

   Note: The phrase "reducible/irreducible over D" can be best interpreted as "factorable/ nonfactorable into non-units in $D[x]$".

   Note: This is basically an generalization of the notion of primality. For example in $\mathbb{Z}$ we say that 6 is composite (think reducible) because we may write $6 = (2)(3)$ and neither is a unit (the units are ± 1). On the other hand we cannot do this with 5, which is prime (think irreducible). The integers $0, -1, 1$ are considered neither.

   Example: The polynomial $2x+2$ is reducible over $\mathbb{Z}$ since we can write $2x+2 = 2(x+1)$ and neither 2 nor $x + 1$ is a unit in $\mathbb{Z}[x]$.

   Example: The polynomial $2x + 2$ is irreducible over $\mathbb{R}$ since any factorization results in at least one unit, for example $2x + 2 = 2(x + 1)$ doesn't count since 2 is a unit.

   Example: The polynomial $x^2 - 5$ is reducible over $\mathbb{R}$ since we can write $x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$ and neither is a unit in $\mathbb{R}[x]$.

   Example: The polynomial $x^2 - 5$ is irreducible over $\mathbb{Q}$ since we cannot factor it into non-units in $\mathbb{Q}[x]$.

   (b) **Theorem (Reducibility for Degrees 2 and 3):** Let F be a field. If $f(x) \in F[x]$ has degree 2 or 3 then $f(x)$ is reducible over F iff $f(x)$ has a zero/root in F.

   Note: This is a generalization of a well-known fact in $\mathbb{R}[x]$. For example if $f(x) = x^3 + x^2 - x - 10$ then knowing that $f(2) = 0$ is equivalent to knowing that $x - 2$ is a factor and in fact $x^3 + x^2 - x - 10 = (x - 2)(x^2 + 3x + 5)$. This doesn't work in degree 4 or higher, for example $x^4 + 2x^2 + 1$ factors as $(x^2 + 1)(x^2 + 1)$ but has no zeros/roots in $\mathbb{R}$.

   Note: Since $\mathbb{Z}_p$ (with p a prime) is a field, in $\mathbb{Z}_p[x]$ we can check for reducibility in the degree 2/3 case by simply checking all roots. For example consider $f(x) = x^4 + 2x^2 + x + 1 \in \mathbb{Z}_3[x]$. We check $f(0) = 1$, $f(1) = 2$, and $f(2) = 0$. Since $f(2) = 0$ we know that $(x - 2)$ is a factor and $f(x)$ is reducible over $\mathbb{Z}_3$. On the other hand consider $f(x) = x^3 + x^2 + x + 2 \in \mathbb{Z}_3[x]$. We check $f(0) = 2$, $f(1) = 2$ and $f(2) = 1$. Since there are no zeros/roots we know $f(x)$ is irreducible over $\mathbb{Z}_3$.

   Proof:
   $\Longrightarrow$: Suppose $f(x)$ is reducible, then $f(x) = g(x)h(x)$ and since neither is a unit, both have positive degree, and then since the degrees add to 3, one of them must have degree 1 and the other degree 2. The one degree 1 factor yields a zero/root.
   $\Longleftarrow$: Suppose $f(x)$ has a zero/root. Then by the Factor Theorem $f(x) = (x - a)g(x)$ and so $f(x)$ is reducible. $\mathcal{QED}$

   (c) **Theorem (Reducibility over $\mathbb{Q}$ implies over $\mathbb{Z}$):** If $f(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$ then it is reducible over $\mathbb{Z}$.
   Proof: Omit. $\mathcal{QED}$

   Note: Essentially this states that if we have a polynomial with coefficients in $\mathbb{Z}$ that if we can factor it into non-units in $\mathbb{Q}[x]$ then we can factor it into non-units in $\mathbb{Z}[x]$.

   Example: As an example consider $f(x) = 10x^2 - 11x - 35$. Observe that $f(x) = \left(5x - \frac{25}{2}\right)\left(2x + \frac{14}{5}\right)$ so we can factor it in $\mathbb{Q}[x]$. But in fact $f(x) = (2x - 5)(5x + 7)$ as well, so we can factor it in $\mathbb{Z}[x]$. The theorem states that this can always be done.

(d) **Theorem (Mod p Irreducibility Test):** Let p be a prime and let $f(x) \in \mathbb{Z}[x]$ with degree 1 or greater. Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained by reducing all of $f(x)$'s coefficients mod p. Then if $\deg(\bar{f}(x)) = \deg(f(x))$ and if $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ then $f(x)$ is irreducible over $\mathbb{Q}$.

Note: Be careful of how this is used. Basically we can pick a prime p and if the degree of $\bar{f}(x)$ is unchanged and if $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ (which can be easily tested in the cases of degrees 2 and 3) then we gain irreducibility over $\mathbb{Z}$. However if the degree drops then nothing can be concluded and if $\bar{f}(x)$ is reducible over $\mathbb{Z}_p$ then nothing is concluded. When nothing is concluded we can of course try other p but we could continue to gain no new knowledge each time.

Example: Consider $f(x) = x^3 + 7x^2 + 13x - 4$. Using $p = 2$ we have $\bar{f}(x) = x^3 + x^2 + x$. This is reducible over $\mathbb{Z}_p$ and nothing is gained.

Using $p = 3$ we have $\bar{f}(x) = x^3 + x^2 + x + 2$. Using the deg2/3 test we check: $\bar{f}(0) = 2$, $\bar{f}(1) = 5 = 2$ and $\bar{f}(2) = 16 = 1$. Since there are no zeros/roots we know that $\bar{f}(x)$ is irreducible over $\mathbb{Z}_3$ and then by the mod p test $f(x)$ is irreducible over $\mathbb{Z}$.

Proof: Suppose $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$ and so $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$ both having degree less than $\deg(f(x))$. If we reduce the coefficents of all three mod p to get $\bar{f}$, $\bar{g}$ and $\bar{h}$ then we have $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ and $\deg(\bar{g}(x)) \leq \deg(g(x)) < \deg(f(x)) = \deg(\bar{f}(x))$ and similarly for $h(x)$. Of course since which contradicts the fact that $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$. $\mathcal{QED}$

(e) **Theorem (Eisenstein's Criterion):** Suppose we have:

$$f(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x]$$

If we can find a prime p such that $p \nmid a_n$, $p \mid a_{n-1}$, ...,$p \mid a_0$, $p^2 \nmid a_0$ then $f(x)$ is irreducible over $\mathbb{Q}$.

Example: The polyomial $6x^5 + 5x^4 - 25x^3 + 15x + 10$ is irreducible over $\mathbb{Q}$ using the prime $p = 5$.

Proof: Suppose such a p exists but $f(x)$ is reducible over $\mathbb{Q}$. We know then that it is reducible over $\mathbb{Z}$ and so $f(x) = g(x)h(x)$ with $g(x) = b_i x^i + ... + b_1 x + b_0$ and $g(x) = c_j x^j + ... + c_1 x + c_0$ with $1 \leq i < n$ and $1 \leq j < n$. Since $a_0 = b_0 c_0$ and since $p \mid a_0$ but $p_0^2 \nmid a_0$ we have either $p \mid b_0$ or $p \mid c_0$ but not both. Without loss of generality assume $p \mid b_0$ and $p \nmid c_0$. Since $a_n = b_i c_j$ and since $p \nmid a_n$ we know $p \nmid b_i$ and so there is a smallest index $m \leq i < n$ with $p \nmid b_m$. Consider that:

$$a_m = b_0 c_m + b_1 c_{m-1} + ... + b_{m-1} c_1 + b_m c_0$$

Since $p \mid a_m$ and $p \mid b_0$, ... $p \mid b_{m-1}$ we must have $p \mid b_m c_0$ which contradicts the fact that $p \nmid b_m$ and $p \nmid c_0$. $\mathcal{QED}$

3. **Connection to Quotient Rings**

(a) **Theorem:** Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ iff $p(x)$ is irreducible over F.

Proof:

$\Longrightarrow$: Suppose $\langle p(x) \rangle$ is a maximal ideal in $F[x]$. We know that $p(x) \neq 0$ and $p(x)$ is not a unit since neither $\{0\}$ nor $\langle \text{unit} \rangle = F[x]$ is a maximal ideal in $F[x]$. Let $p(x) = g(x)h(x)$ be a factorization. Then $\langle p(x) \rangle \subseteq \langle g(x) \rangle \subseteq F[x]$ and since $\langle p(x) \rangle$ is maximal we either have $\langle g(x) \rangle = \langle p(x) \rangle$ or $\langle g(x) \rangle = F[x]$. In the first case we get $\deg(g(x)) = \deg(p(x))$ by a previous theorem (they both have minimal and therefore equal degree) and in the second case we get $\deg(g(x)) = 0$ and so $\deg(h(x)) = \deg(p(x))$. Thus $p(x)$ is irreducible.

$\Longleftarrow$: Suppose that $p(x)$ is irreducible over F. Let I be an ideal with $\langle p(x) \rangle \subseteq I \subseteq F[x]$. Because $F[x]$ is a PID we know that $I = \langle g(x) \rangle$ for some $g(x) \in F[x]$ and so $p(x) \in \langle g(x) \rangle$ and hence $p(x) = g(x)h(x)$ for some $h(x) \in F[x]$. Since $p(x)$ is irreducible either $g(x)$ or $h(x)$ is a constant. In the first case $I = F[x]$ and in the second case $I = \langle p(x) \rangle$. $\mathcal{QED}$

Note: This can be used to construct desired fields. If we want a field with 7 elements we can use $\mathbb{Z}_7$ but if we want a field with 27 elements we cannot use $\mathbb{Z}_{27}$ because it is not a field (why not?)

But we can construct one when this new theorem is coupled with a theorem from earlier in the class which stated:

$$\text{An ideal } I \text{ of a ring } R \text{ is maximal} \Leftrightarrow R/I \text{ is a field.}$$

It follows that we can say that given a field F:

$$p(x) \in F[x] \text{ is irreducible over } F \Leftrightarrow \langle p(x) \rangle \text{ is maximal} \Leftrightarrow F[x]/\langle p(x) \rangle \text{ is a field.}$$

Consider that we showed that $p(x) = x^3 + x^2 + x + 2$ is irreducible over $\mathbb{Z}_3$ and hence $\mathbb{Z}_3[x]/\left\langle x^3 + x^2 + x + 2 \right\rangle$ is a field. Elements in this field have the form $ax^2 + bx + c + \left\langle x^3 + x^2 + x + 2 \right\rangle$ with $a, b, c \in \mathbb{Z}_3$ (why?) and there are 27 such elements.

(b) **Corollary:** Let F be a field and let $p(x), a(x), b(x) \in F[x]$. If $p(x)$ is irreducible over F and if $p(x) \mid a(x)b(x)$ then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

Note: This is a generalization of the notion from number theory (that we've used) that if a prime $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof: Since $p(x)$ is irreducible $F[x]/\langle p(x) \rangle$ is a field and hence an integral domain. Then $\langle p(x) \rangle$ is a prime ideal and since $p(x) \mid a(x)b(x)$ we have $a(x)b(x) \in \langle p(x) \rangle$ and so one of them is in $\langle p(x) \rangle$. The result follows. $\mathcal{QED}$