Math 371 Lecture #18
§5.2: Congruence Class Arithmetic

Congruence in $F[x]$ leads to new rings and fields of the form $F[x]/(p(x))$, in a way that is richer than congruence in $\mathbb{Z}$ leads to the rings and fields $\mathbb{Z}_n$.

Congruence modulo $p(x)$ preserves the congruence classes under addition and multiplication.

**Theorem 5.6.** Let $F$ be a field and $p(x)$ a nonconstant polynomial in $F[x]$. If $[f(x)] = [g(x)]$ and $[h(x)] = [k(x)]$ in $F[x]/(p(x))$, then

$$[f(x) + h(x)] = [g(x) + k(x)]$$

and

$$[f(x)h(x)] = [g(x)k(x)].$$

**Proof.** With $f(x) \equiv g(x) \pmod{p(x)}$ and $h(x) \equiv k(x) \pmod{p(x)}$, we have by Theorem 5.2 that $f(x) + h(x) \equiv g(x) + k(x) \pmod{p(x)}$.

By Theorem 5.3, we then have $[f(x) + h(x)] = [g(x) + k(x)]$.

We also have that $f(x)h(x) \equiv g(x)k(x) \pmod{p(x)}$, and so again by Theorem 5.3, we have that $[f(x)g(x)] = [h(x)k(x)]$. □

We can now define addition and multiplication in $F[x]/(p(x))$ that are independent of the representatives of the classes.

**Definition.** For a field $F$, let $p(x) \in F[x]$ be a nonconstant polynomial. Addition and multiplication in $F[x]/(p(x))$ are defined by

$$[f(x)] + [g(x)] = [f(x) + g(x)]$$

and

$$[f(x)][g(x)] = [f(x)g(x)].$$

**Example.** Consider the set of congruence classes $Q[x]/(x^2 - x - 1)$.

We know that every nonzero congruence class has a representative of degree less than 2. So the addition and multiplication of $[4x - 3]$ and $[-2x + 4]$ in $Q[x]/(x^2 - x - 1)$ are

$$[(4x - 3) + (-2x + 4)] = [2x + 1]$$

and

$$[(4x - 3)(-2x + 4)] = [-8x^2 + 22x - 12].$$

We can represent the class of $-8x^2 + 22x - 12$ by its remainder when divided by $x^2 - x - 1$. Since

$$-8x^2 + 22x - 12 = (x^2 - x - 1)(-8) + (14x - 20),$$

then

$$[-8x^2 + 22x - 12] = [14x - 20].$$

Is $Q[x]/(x^2 - x - 1)$ a ring? a commutative ring? a commutative ring with identity? an integral domain? a field?

If so to any of these, does $Q[x]/(x^2 - x - 1)$ contain a subring isomorphic to $Q$?

**Theorem 5.7.** For a field $F$, let $p(x) \in F[x]$ be a nonconstant polynomial. Then $F[x]/(p(x))$ is a commutative ring with identity. Furthermore, $F[x]/(p(x))$ contains a subring $F^*$ that is isomorphic to $F$. 

Proof. The eight axioms for a ring are easily verified for $F[x]/(p(x))$ because $F[x]$ is a ring.

The ring $F[x]/(p(x))$ is a commutative ring because $F[x]$ is a commutative ring.

The commutative ring $F[x]/(p(x))$ has an identity $z(x) = 1_F$ because the field $F$ has an identity $1_F$.

Now let $F^*$ be the subset of $F[x]/(p(x))$ consist of all the congruence classes of the constant polynomials;

$$F^* = \{ [a] : a \in F \}.$$

One easily verifies that $F^*$ is a subring of $F[x]/(p(x))$.

The proposed isomorphism $\varphi : F \to F^*$ is the map defined by $\varphi(a) = [a]$.

This definition gives a surjective map.

From the definitions of addition and multiplication on $F[x]/(p(x))$ we have

$$\varphi(a + b) = [a + b] = [a] + [b] = \varphi(a) + \varphi(b),$$

and

$$\varphi(ab) = [ab] = [a] [b] = \varphi(a) \varphi(b).$$

Thus $\varphi$ is a surjective homomorphism.

To show injectivity of $\varphi$, we suppose that $\varphi(a) = \varphi(b)$.

Then $[a] = [b]$, which means that $a - b$ is divisible by $p(x)$.

Since $\deg p(x) \geq 1$, this can only happen if $a - b = 0$.

Thus $a = b$, and $\varphi$ is injective. \hfill \Box

Really IMPORTANT idea: It is general practice to identify $F^*$ inside $F[x]/(p(x))$ with $F$, which we can do because $F^*$ and $F$ are isomorphic. This is what Theorem 5.8 (in Ed.2 and Ed.3) states.

We can thus think of the commutative ring $F[x]/(p(x))$ with identity as containing the field $F$.

Example. Construct the addition and multiplication tables for the commutative ring $\mathbb{Z}_2[x]/(x^2 + x)$ with identity.

The elements of $\mathbb{Z}_2[x]/(x^2 + x)$ have the form $[ax + b]$ for $a, b \in \mathbb{Z}_2$.

By identifying the isomorphic copy of $\mathbb{Z}_2$ inside $\mathbb{Z}_2[x]/(x^2 + x)$, we write 0 instead of $[0]$, and 1 instead of $[1]$.

The addition and multiplication tables for $\mathbb{Z}_2[x]/(x^2 + x)$ are

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>[x]</th>
<th>[x + 1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>[x]</td>
<td>[x + 1]</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>[x + 1]</td>
<td>[x]</td>
</tr>
<tr>
<td>[x]</td>
<td>[x]</td>
<td>[x + 1]</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>[x + 1]</td>
<td>[x + 1]</td>
<td>[x]</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
The justification for the lower right $2 \times 2$ block in the multiplication table is: $[x][x] = [x^2]$ where $x^2 = (x^2 + x)(1) + x$ so that $[x^2] = [x]$; also $[x + 1][x] = [x^2 + x] = 0$; and $[x + 1][x + 1] = [x^2 + 1]$ where $x^2 + 1 = (x^2 + x)(1) + (x + 1)$ so that $[x + 1][x + 1] = [x + 1]$.

Are there any zero divisors in $\mathbb{Z}_2[x]/(x^2 + x)$? Yes, both $[x]$ and $[x + 1]$ are zero divisors, and so $\mathbb{Z}_2[x]/(x^2 + x)$ is not an integral domain.

Which of the elements of $\mathbb{Z}_2[x]/(x^2 + x)$ are units?

According to the multiplication table, there is only one unit in $\mathbb{Z}_2[x]/(x^2 + x)$, namely 1. The remaining nonzero elements $[x]$ and $[x + 1]$ are not units, and so $\mathbb{Z}_2[x]/(x^2 + x)$ is not a field.

Is $x^2 + x$ reducible in $\mathbb{Z}_2[x]$? Yes, $x^2 + x = x(x + 1)$.

**Theorem 5.9.** For a field $F$ and a nonconstant $p(x) \in F[x]$, if $f(x) \in F[x]$ and $p(x)$ are relatively prime, then $f(x)$ is a unit in $F[x]/(p(x))$.

**Proof.** With $f(x)$ and $p(x)$ relatively prime, there are polynomials $u(x), v(x) \in F[x]$ such that

$$1 = f(x)u(x) + p(x)v(x).$$

Hence we have

$$f(x)u(x) - 1 = -p(x)v(x) = p(x)(-v(x)).$$

Thus $[f(x)] [u(x)] = [f(x)u(x)] = 1$, meaning that $[f(x)]$ is a unit in $F[x]/(p(x))$. $\square$

**Example.** Is $[3x + 4]$ a unit in $\mathbb{Q}[x]/(x^2 - x - 1)$?

We apply the Euclidean Algorithm to $p(x) = x^2 - x - 1$ and $f(x) = 3x + 4$ to get

$$x^2 - x - 1 = (3x + 4) \left( \frac{x}{3} + \frac{7}{9} \right) + \frac{19}{9}.$$ 

Since the remainder is an associate of 1, the polynomials $p(x)$ and $f(x)$ are relatively prime.

We find $u(x)$ and $v(x) \in \mathbb{Q}[x]$ for which $1 = f(x)u(x) + p(x)v(x)$ by reversing the Euclidean Algorithm:

$$1 = (3x + 4) \left( -\frac{3x}{19} + \frac{7}{19} \right) + (x^2 - x - 1) \left( \frac{9}{19} \right).$$

Thus $[3x + 4]$ is a unit in $\mathbb{Q}[x]/(x^2 - x - 1)$ with inverse $-(3x/19) + (7/19)$.

Are there any zero divisors in $\mathbb{Q}[x]/(x^2 - x - 1)$? Is every nonzero $[ax + b]$ a unit in $\mathbb{Q}[x]/(x^2 - x - 1)$? Is $x^2 - x - 1$ irreducible in $\mathbb{Q}[x]$?