Abstract Algebra I - Lecture 23

Adam Chapman

Department of Mathematics, Michigan State University, East Lansing, MI 48824

---

Note on divisibility of polynomials.
If \( f(x) | g(x) \) and \( g(x) | f(x) \) then \( f(x) = c \cdot g(x) \) for some scalar \( c \in F^\times = F \setminus \{0\} \).

Proof.
From \( f(x) | g(x) \) we obtain \( \deg(f) \leq \deg(g) \) and from \( g(x) | f(x) \) we obtain \( \deg(g) \leq \deg(f) \), so \( \deg(g) = \deg(f) \). Now, divide \( f(x) \) by \( g(x) \): \( f(x) = q(x)g(x) \). The degree of \( q(x) \) must be 0, so \( q(x) \) is a scalar \( c \in F^\times \).

Congruence classes of polynomials.
Let \( F \) be a field. Consider the ring of polynomials \( F[x] \). Given a polynomial \( f(x) \), we can consider the equivalence relation \( g(x) \equiv h(x) \pmod{f(x)} \iff f(x)|(g(x) - h(x)) \). The set of congruence classes is denoted by \( F[x]/f(x) \).

Example.
Take \( F = \mathbb{R} \) and \( f(x) = x \). Two polynomials \( g(x) = a_0 + a_1x + \ldots \) and \( h(x) = b_0 + b_1x + \ldots \) are congruent modulo \( f(x) \) if and only if \( a_0 = b_0 \). Therefore the classes in \( \mathbb{R}[x]/x \) are parameterized by the free coefficients: \( \mathbb{R}[x]/x = \{[a_0] : a_0 \in \mathbb{R}\} \).

Ring structure.
\( F[x]/f(x) \) has a ring structure with addition and multiplication defined in the usual sense:

\[
[g(x)] + [h(x)] = [g(x) + h(x)]
\]

\[
[g(x)] \cdot [h(x)] = [g(x)h(x)]
\]

Example.
In \( \mathbb{Z}_2[x]/(x^2 + x + 1) \) we have: \( [x^2] \cdot [x + 1] = [x^3 + x^2] = [x(x + 1) + x^2] = [x] \).

Terminology.
When talking about polynomials in \( F[x] \), a scalar means an element in \( F \setminus \{0\} \). This set is exactly the set of polynomials of degree 0, and also the set of units in \( F \), and also the set of units in \( F[x] \).

---

Email address: adam1chapman@yahoo.com (Adam Chapman)

Preprint submitted to Elsevier October 28, 2015
Irreducible Polynomials.
A polynomial $f(x) \in F[x]$ of degree $\geq 1$ is irreducible if for any $f(x) = g(x)h(x)$, either $g(x)$ is a scalar or $h(x)$ is a scalar.

Examples.

- A polynomial of degree 1 is always irreducible.
- Every irreducible polynomial in $\mathbb{C}[x]$ is of degree 1.
- A polynomial in $\mathbb{R}[x]$ is irreducible if and only if it is either of degree 1 or if it is of degree $2 - ax^2 + bx + c$ and $b^2 - 4ac < 0$.

Remark.
The only divisors of an irreducible polynomial are scalar multiples of itself and scalars. Therefore, if $f(x) = c_kx^k + \cdots + c_0$ is irreducible then $\gcd(f(x), h(x))$ can be either $\frac{1}{c_k}f(x)$ or 1.

Definition.
Two polynomials $f(x), g(x)$ are relatively prime if $\gcd(f(x), g(x)) = 1$.

Proposition.
$f(x)$ is invertible in $F[x]/g(x)$ if and only if $\gcd(f(x), g(x)) = 1$.

Proof.
$\gcd(f(x), g(x)) = 1 \iff \varphi(x)f(x) + \psi(x)g(x) = 1$ for some $\varphi(x), \psi(x) \in F[x] \iff \varphi f(x) \equiv 1 \pmod{g(x)}$ for some $\varphi(x) \in F[x] \iff f(x)$ is invertible in $F[x]/g(x)$.

Proposition.
A polynomial $f(x) \in F[x]$ is irreducible if and only if whenever $f(x)|g(x)h(x)$, either $f(x)|g(x)$ or $f(x)|h(x)$.

Proof.

$\Rightarrow$
Assume $f(x)$ is irreducible. Assume $g(x)$ and $h(x)$ are not multiples of $f(x)$. Then they are prime to $f(x)$. Therefore $g(x)$ and $h(x)$ are invertible in $F[x]/f(x)$. Hence $g(x)h(x)$ is invertible in $F[x]/f(x)$. Consequently $g(x)h(x)$ is prime to $f(x)$ and so not a multiple of $f(x)$.

$\Leftarrow$
Assume that for any $g(x)$ and $h(x)$, if $f(x)|g(x)h(x)$ then either $f(x)|g(x)$ or $f(x)|h(x)$. Assume that $f(x) = \varphi(x)\psi(x)$. Then $f(x)|\varphi(x)$ or $f(x)|\psi(x)$. If $f(x)|\varphi(x)$ then
\[ \varphi(x) = c \cdot f(x) \] and since \( f(x) = \varphi(x)\psi(x) \), \( \psi(x) \) must be a scalar. Similarly, if \( f(x)|\psi(x) \) then \( \varphi(x) \) must be a scalar. Therefore \( f(x) \) is irreducible.

**Notes on the general case of integral domains.**

In general, in an integral domain \( R \), a noninvertible element \( f \) is irreducible if whenever \( f = gh \), either \( g \) is invertible or \( h \) is invertible. In case of polynomials over fields, \( g \) is invertible if and only if it is of degree 0. This way this definition boils down to the definition above of irreducible elements in \( F[x] \).

In integral domains it is not true in general that \( f \) is irreducible if and only if whenever \( f|gh \) either \( f|g \) or \( f|h \). For example, in the integral domain \( \mathbb{Z}[\sqrt{-6}] \) (i.e. the set of all numbers that can be obtained by addition and multiplication of integers and the square root of \(-6\)) we have \((2 + \sqrt{-6}) \cdot (2 - \sqrt{-6}) = 10\), so \(2|(2 + \sqrt{-6}) \cdot (2 - \sqrt{-6})\) even though neither \(2 + \sqrt{-6}\) is a multiple of \(2\) nor \(2 - \sqrt{-6}\).

**Exercise.**

Say if \( f(x) \) is irreducible in \( \mathbb{R}[x] \) in the following cases:

- \( f(x) = x^2 + 1 \).
- \( f(x) = x^2 - 1 \).
- \( f(x) = x - 15 \).
- \( f(x) = x^{123} - 3x^{77} + 6 \).