Abstract Algebra
Lecture 10
Wednesday, 10/6/2010

1 Special Rings

1.1 Polynomial Rings

Defn: Let R be a commutative ring with identity. Then

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R\}$$

Addition and multiplication are the usual operations. Then $R[x]$ is a ring, called a **polynomial ring**.

Ex: How nice is $R[x]$? This depends on R. For example, $x^2 + 1$ is irreducible in $\mathbb{Z}[x]$, but it is factorable in $\mathbb{C}[x]$, and $x^2 + 1 = (x + 1)(x + 1)$ in $\mathbb{Z}_2[x]$. The "best case" is when R is an integral domain.

Theorem: Let R be an integral domain. Then

1. $\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x))$ for $f(x), g(x) \in R[x]$,
2. $R[x]$ is an integral domain,
3. The units in $R[x]$ are precisely the units in R (we consider $R \leq R[x]$ as the constant polynomials)

Proof:

1. Say $f = a_n x^n + \cdots$, $g = b_m x^m + \cdots$. Then $f \cdot g = a_n b_m x^{m+n} + \cdots$. Since R is an integral domain, $a_n b_m \neq 0$. Thus, $\deg(f \cdot g) = m + n$.
2. $R[x]$ is clearly commutative, since R was commutative. The identity of $R[x]$ is the identity of R. The fact that $R[x]$ has no zero-divisors follows from the first part.
3. Let $f \in R[x]$ be a unit. Then $f \cdot g = 1$ for some $g \in R[x]$. Then $0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$, so $\deg(f) = 0$.

■

Ex: What about when R is not an integral domain? $\mathbb{Z}_4[x]$ is a good example. $(2x + 1)(2x + 1) = 4x^2 + 4x + 1 = 1$, so we have a unit that is not a constant. $(2x)(2x) = 4x^2 = 0$, so we also have zero-divisors.

Ex: We can also throw on multiple indeterminants.

$$R[x,y] = \{\text{polynomials in } x \text{ and } y \text{ with coefficients in } R\}.$$

Note that $R[x,y] = (R[x])[y]$.

Defn: The **ring of formal power series** is defined by

$$R[[x]] = \{a_0 + a_1x + a_2x^2 + \cdots \mid a_i \in R\}.$$

Ex: The series $1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots$ and $\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots$ are both in this ring. This ring does also include finite polynomials.

1.2 Matrix Rings

Defn: Let R be a ring, $n \in \mathbb{N}$. Then

$$M_n(R) = \{m \times n \text{ matrices with entires in } R\}.$$

This is called a **matrix ring**. Note that, if R is a non-commutative ring, we need to be careful about our multiplication.

Note: Matrix rings are almost never commutative. There are two exceptions: when $n = 1$ (which is silly), and when everything in R is either 0 or a zero-divisor with every other element of R (which is even more silly). Matrix rings have zero divisors. Units in $M_n(R)$ are matrices whose determinants are units. We need the determinant of a matrix to be a unit so we can multiply by its inverse to calculate the inverse of the matrix. In general, Cramer's Rule gives the inverse. If R has an identity, then $M_n(R)$ has an identity.

1.3 Group Rings

Defn: Let R be a commutative rings with identity. Let G be a group (usually finite). Then

$$R[G] = \left\{ \sum_{g \in G} r_g f \mid r_g \in R \right\}.$$

This is known as a **group ring**.

Ex: Consider $\mathbb{Z}[S_3]$. Then an element of this ring is $3(12) + 5(132) - 6e$. Our operations work as

$$(3(12) + 5(132)) + (2(12) - (13)) = 5(12) + 5(132) - (13),$$
$$(3(12) + 5(132)) \cdot 2(12) = 6(12)(12) + 10(132)(12) = 6e + 10(23).$$

Theorem: The group $R[G]$ is commutative if and only if G is abelian.

2 Ring Homomorphisms

Defn: If R and S are rings, a **ring homomorphism** $f : R \to S$ is a function satisfying
1. $f(ab) = f(a)f(b)$
2. $f(a + b) = f(a) + f(b)$

Ex: Let $f_n : \mathbb{Z} \to \mathbb{Z}$ defined by $x \mapsto nx$ for some $n \in \mathbb{Z}$. Then $f(x + y) = n(x + y) = nx + ny = f(x) + f(y)$, but $f(xy) = nxy \neq nxny = f(x)f(y)$ so this is not a homomorphism (unless $n = 0, 1$).

Ex: Let $f : \mathbb{Z} \to Z_n$, $x \mapsto x \mod n$ for $n \geq 1 \in \mathbb{Z}$. This is a homomorphism.

Defn: A **ring isomorphism** is a bijective ring homomorphism.

Theorem: Let $\varphi : R \to S$ be a homomorphism of rings. Then
1. $\varphi(0_R) = 0_S$
2. $\varphi(na) = n\varphi(a)$
3. $\varphi(a^n) = \varphi(a)^n$
4. $\varphi(-a) = -\varphi(a)$
5. $\varphi(a + b + \cdots) = \varphi(a) + \varphi(b) + cdots$
6. $\varphi(abc \cdots) = \varphi(a)\varphi(b)\varphi(c) \cdots$

If R and S have identity elements, it is not necessarily the case that $\varphi(1_R) = 1_2$.