7.2: Polynomial Rings, Matrix Rings, and Group Rings

Alex L.

December 14, 2024

1 Motivation

We want to introduce three useful types of rings: Polynomial Rings, Matrix Rings, and Group Rings.

2 Content

2.1 Polynomial Rings

Definition: (Polynomial Rings) A polynomial ring $R[x]$ is a ring with members r of the form

$$r = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0$$

where $a_0, a_1, ..., a_n$ are real numbers with standard addition of like terms and multiplication of polynomials. Its pretty easy to see that this is a ring.

Notice that the ring of real numbers R is a subring of $R[x]$, when the highest degree is degree zero.

We can use different coefficients for the polynomial ring. For example, we could have

$$\mathbb{Z}[x]$$

the polynomial ring with integer coefficients, or even

$$\mathbb{Z}/3\mathbb{Z}[x]$$

the polynomial ring with coefficients mod 3.

The behaviour and properties of polynomials depends on which coefficient ring you pick. For example, $x^2 + 1$ is not a perfect square under real coefficients, but it is under coefficients $\mathbb{Z}/2\mathbb{Z}$.

Proposition: Let $\mathbb{R}$ be an integral domain (no zero divisors) and let $p(x)$ $q(x)$ be nonzero elements of $\mathbb{R}[x]$. Then:

1. The degree of $p(x)q(x)$ is the degree of $p(x)$ plus the degree of $q(x)$.
2. The units of $\mathbb{R}[x]$ are the units of $\mathbb{R}$
3. $\mathbb{R}[x]$ is an integral domain.

Proof:

1. The degree of a polynomial is the highest power term. Lets just examine these terms. Let $a_p x^p$ be the highest power term in $p(x)$ and $a_q x^q$ be the highest power term in $q(x)$. Then, when multiplied, these two will combine to form the term $a_p a_q x^{p+q}$. Since there are no zero divisors, this term will always exist if a_p and a_q are nonzero, and it is the highest power term in $p(x)q(x)$, since it is the product of the two highest power terms of $p(x)$ and $q(x)$. Therefore, the degree of the polynomial is $p + q$.
2. Remember that the units of $\mathbb{R}[x]$ are the elements that multiply to make the identity, 1. Multiplying elements of $\mathbb{R}[x]$ never decreases their degree, so in order to have $p(x)q(x) = 1$, both $p(x)$ and $q(x)$ nessecarily must be of degree zero. The degree zero elements of $\mathbb{R}[x]$ forms the ring $\mathbb{R}$, and as such, the units of $\mathbb{R}[x]$ are just the units of $\mathbb{R}$.
3. We see clearly that the additive identities and multiplicative identities are not equal. In addition, for there to be zero divisors, we must have a way of multiplying two nonzero polynomials to get all terms to be zero. However, there is never a way to get these terms to be zero. The coefficeints are never zero since the cefficient ring is never zero. In addition, since the degree of all terms is always positive, and multiplying terms adds their degrees, the

degree can never be zero (not that that would matter anyways). Therefore, there are no zero divisors and it is an integral domain.

2.2 Matrix Rings

Definition: (Matrix Rings) A **matrix ring** $M_n(R)$ is the ring of all $n \times n$ square matrices with entries from the ring R.

Note that when R is nontrivial, $M_n(R)$ is not commutative.

Every ring of the type $M_n(R)$ has zero divisors. Suppose we have a matrix A with at least one entry that is zero. Then, lets construct its zero divisor pair: first, transpose A, and then replace all nonzero elements with zeros, and all zero elements with any element of R. You will have constructed a nontrivial matrix, that when multiplied with A, yields a zero matrix.

An element m of $M_n(R)$ is a scalar matrix if the entries on the diagonal are all some element a, and zero elsewhere. The scalar matrices form a subring of $M_n(R)$ and this subring is isomorphic to R.

If S is a subring of R then $M_n(S)$ is a subring of $M_n(R)$.

2.3 Group Rings

Definition: (Group Rings) Let R be a commutative ring with $1 \neq 0$. Then, pick any finite group G. The ring RG is the **group ring** and has elements $a_1g_1 + a_2g_2 + a_3g_3 + ... + a_ng_n$, where $g_1, g_2, ...$ are elements in G and $a_1, a_2, ...$ are elements in R. We define addition componentwise, and multiplication as distribution (like multiplying polynomials), and defining $(a_ig_i)(a_jg_j) = (a_ia_j)(g_ig_j)$. RG is only commutative iff G is commutative.