MATH H113: Honors Introduction to Abstract Algebra

2016-03-28

- Polynomial Rings (continued)
- Group rings
- Homomorphisms and kernels

Handout: Sample Second Midterm!!
Midterm (April 5) will cover all sections up to and including Sect. 7.2.

For Friday, read Sect. 7.3, especially the examples on p. 243-247.

Is $\mathbb{Z}/6\mathbb{Z}$ an integral domain?
No: $\bar{2} \cdot \bar{3} = \bar{0}$ so it has zero divisors.

Polynomials

Caution: Don't think of polynomials as functions. For example, $(\mathbb{Z}/2\mathbb{Z})[x]$ is infinite, but there are only finitely many functions from $\mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$
So, for example, let $p(x) = x^2 - x$.
Then $p(\bar{0}) = \bar{0}^2 - \bar{0} = \bar{0}$
$p(\bar{1}) = \bar{1}^2 - \bar{1} = \bar{0}$
Although p gives us the constant function 0 from $\mathbb{Z}/2\mathbb{Z}$ to itself, it is a nonzero element of $(\mathbb{Z}/2\mathbb{Z})[x]$

Proposition: Let R be an entire ring (integral domain)

a. If p and q are nonzero elements of $R[x]$, then $\deg pq = \deg p + \deg q$ (and $pq \neq 0$).
b. $R[x]$ is entire; and
c. $(R[x])^\times = R^\times$ (units in $R[x]$ = units in R)

Proof:

a. If p and q have leading terms $a_n x^n$ and $b_m x^m$, respectively then pq has the leading term $a_m b_m x^{n+m}$ (since $a_n b_m \neq 0$).
b. $R[x]$ is commutative and has $1 \neq 0$ because R is. Also, it has no zero divisors by (a).
c. By (a), if $uv = 1$ then $\deg u + \deg v = 0$, so u and v are constants, $\therefore$ $u, v \in R^\times$. And conversely.

Group Rings

Let R be a commutative ring with 1 and let G be a finite group (not necessarily abelian).
Write $G = \{g_1, g_2, \ldots, g_n\}$, with $g_1 = 1$. Then the *group ring* $R[G]$ or RG is the set of all formal sums: $a_1g_1 + a_2g_2 + \ldots + a_ng_n$ with $a_1, \ldots, a_n \in R$ with addition defined component wise:
$\sum\limits_{i=1}^{n} a_ig_i + \sum\limits_{i=1}^{n} b_ig_i = \sum\limits_{i=1}^{n}(a_i + b_i)g_i$
and multiplication defined so that $(a_ig_i)(b_jg_j) = (a_ib_j)(g_ig_j)$. This is a ring.
For ease of notation we write $a1 = g_1$ as a $\forall a \in R$ and $1g$ (with $1 \in R$) as g $\forall g \in G$ (So $1 \in RG$ means $1_R \cdot 1_G$, with $1_R \in R$ and $1_G \in G$. This is the identity element in RG.)

Examples:

1. If R is the zero ring, then $R[G]$ is the zero ring.
2. If G is the trivial group, then $R[G]$ is just R.
3. $\mathbb{Q}[\mathbb{Z}/2\mathbb{Z}]$ is $\{a + bx : a, b \in \mathbb{Q}\}$ (here $x = \bar{1}$) with $(a + bx)(c + dx) = (ac + bd) + (ad + bc)x$ because $(bx)(dx) = (bd)x^2 = bd$ ($x^2 = 1 \in \mathbb{Z}/2\mathbb{Z}$: $\bar{0} + \bar{0} = \bar{0}$, $\bar{1} + \bar{1} = \bar{0}$.

Comments:

1. $R = 0$ or G is abelian $\iff$ $R[G]$ is commutative
2. If $G \neq 1$ and $R \neq 0$, then $R[G]$ always has zero divisors. Let $g \in G$, $g \neq 1$, and let $n = |g|$. Then $(1 - g)(1 + g + g^2 + \ldots + g^{n-1}) = 1 - g^n = 0$.

Ring Homomorphisms

Definiition:

a. Let R and S be rings. Then a (ring) homomorphism from R to S is a function $\phi : R \to S$ that preserves addition and multiplication:
$\phi(a + b) = \phi(a) + \phi(b)$ ($\implies$ ϕ is a homomorphism from the additive group of R to the additive group of S. and $\phi(ab) = \phi(a)\phi(b)$ $\forall a, b \in R$
b. The kernel of a (ring) homomorphism $\phi : R \to S$ is $\ker\phi = \{r \in R : \phi(r) = 0\}$ = kernel of ϕ as a homomorphism of additive groups.
c. An *isomorphism* from a ring R to a ring S is a bijective (ring) homomorphism from R to S.

Note: If R and S both have 1, we (still) don't assume that a homomorphism $\phi : R \to S$ has $\phi(1) = 1$.
For example: If R_1 and R_2 are rings, then the direct product $R_1 \times R_2$ is defined to

be the cartesian product $R_1 \times R_2$ (as a set or additive group) with componentwise adddition and multiplication ($(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$). If R_1 and R_2 have 1, then so does $R_1 \times R_2$ (it's $(1,1)$). Define $\phi : R_1 \to R_1 \times R_2$ by $\phi(r) = (r, 0)$. This is a ring homomorphism, but $\phi(1) \neq (1,1)$.

More examples of ring homomorphisms:

1. For all $m \in \mathbb{Z}_{>0}$, $\phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $\phi(n) = \bar{n}$, is a ring homomorphism.
2. $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(n) = 2n$ is *not* a ring homorphism ($\phi(1 \cdot 1) = \phi(1) = 2 \neq \phi(1) \cdot \phi(1) = 2 \cdot 2 = 4$).
3. $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ given by $\phi(a, b) = (b, a)$ is a nonidentity ring automorphism (isomorphism from a ring to itself).
4. If R is a commutative ring with 1 and $c \in R$ then "evaluation at c" is a homomorphism from $R[x]$ to R ($p(x) \mapsto p(c)$)

Proposition: Let $\phi : R \to S$ be a ring homomorphism

a. If R' is a subring of R then $\phi(R')$ is a subring of S.
b. If S' is a subring of S then $\phi^{-1}(S')$ is a subring of R.

Proof: Exercise.

Since $\{0\}$ is a subring of S, we get: **Corollary**: The kernel of a ring homomorphism $\phi : R \to S$ is a subring of R.

Next question: Which subgrings of a ring can be kernels of homomorphisms? *Hint*: In S, we have $0 \times s = s \times 0\ \forall s \in S$. So this gives an additional property of $\ker \phi$.