Math 250A Lecture 8 Notes

Daniel Raban

September 19, 2017

1 Rings

1.1 Definition and examples

Definition 1.1. A *ring* is a set R along with two binary operations, $+$ and $\times$, such that

1. R is an abelian group under $+$
2. $\times$ is associative
3. $a(b+c) = ab + ac$, $(a+b)c = ac + bc$.

We also have two optional axioms:

1. $\times$ has identity[1] 1 such that $1a = a1 = a$.
2. $ab = ba$ (commutative rings).

Example 1.1. The integers, $\mathbb{Z}$, are a ring.

Example 1.2. The Gaussian integers, $\mathbb{Z}[i] = \left\{m + ni : m, n \in Z, i^2 = -1\right\}$, are a ring.

Example 1.3. Polynomials over a field K, $K[x]$, are a ring.

Example 1.4. The set of $n \times n$ matrices with entries in K, $M_n(K)$, is a ring.

Example 1.5. The Burnside ring of a group $G = S_3$ is the set of all sums $\sum n_i A_i$ for $n_i \in \mathbb{Z}$ and A_i some transitive permutation representation of G (up to isomorphism). The 4 transitive permutation representations of S_3 are conjugacy classes: $\{1, (1\,2)\}$, $\{1, (1\,3)\}$, $\{1, (2\,3)\}$, $\{1, (1\,2\,3), (1\,3\,2)\}$. We get the adjoint representation on 6 points, 3 points, 2 points, and 1 point, so we get sums of the form $aA^1 + bA^2 + cA^3 + dA^6$.

[1] It is sometimes common in analysis to consider rings that do not have an identity element.

Any permutation representation is the union of transitive ones. So the set of all finite permutation representations (up to isomorphism) is the elements of $aA^1+bA^2+cA^3+dA^6$. This is not a ring, but we can force it to be by adding $-$.[2]

$+$ in this ring is the disjoint union of representations. $\times$ in this ring is the product of permutation representations. In particular, we have the multiplication table

$\times$	A^1	A^2	A^3	A^6
A^1	A^1	A^2	A^3	A^6
A^2	A^2	$A^2 \oplus A^2$	A^6	$A^6 \oplus A^6$
A^3	A^3	A^6	$A^3 \oplus A^6$	$A^6 \oplus A^6 \oplus A^6$
A^6	A^6	$A^6 \oplus A^6$	$A^6 \oplus A^6 \oplus A^6$	$A^6 \oplus A^6 \oplus A^6 \oplus A^6 \oplus A^6 \oplus A^6$

1.2 Analogies between groups and rings

We can draw a parallel between groups and rings.

- A set S (in relation to groups) corresponds to the vector space with basis S (for rings).
- The symmetric group S_n (symmetries of $\{1, 2, \ldots, n\}$) corresponds to $M_n(K)$ (linear transformations of K^n).[3]
- We study G by making G act on some set. We study rings by making them act on K^n.
- Sets A, B have $A \amalg B$ and $A \times B$ with $a + b$ and ab elements, respectively. Given vector spaces V, W with respective dimensions a and b, $V \oplus W$ has dimension $a + b$; the tensor product[4] $V \otimes W$ has the property that if A is a basis for V and B is a basis for W, then $A \times B$ is a basis for $V \otimes W$, so $V \otimes W$ has dimension ab.
- $|A \cup B| = |A| + |B| - |A \cap B|$. Similarly, if V and W are vector spaces, $\dim(V \cup W) = \dim(V) + \dim(W) - \dim(V \cap W)$.

Remark 1.1. If $D = A \cup B \cup C$, then $|D| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$. This is not true for vector spaces. Let U, V, W be 2 dimensional vector spaces in $\mathbb{R}^3$ containing some fixed line.

[2] This is the same thing one does in the construction of the integers from the natural numbers. Doing this to any commutative monoid returns what is called the Grothendieck group.

[3] S_n is the Weyl group of $GL_n(K)$

[4] In older texts, this is sometimes referred to as the Kronecker product.

1.3 Group rings

Definition 1.2. Let G be a group and R a commutative ring. The *group ring* $R[G]$ is the free abelian group with basis G, where $\times$ is the group operation on G extended linearly.

Example 1.6. Let G be the Klein 4 group $\{1, a, b, c\}$ with $a^2 = b^2 = c^2 = 1$, $ab = c$, ... So $\mathbb{C}[G]$ is a 4 dimensional vector space with basis a, b, c, d. It is a product of 4 copies of the ring $\mathbb{C}$.

Look at $e_1 = (1 + a + b + c)/4$, $e_2 = (1 + a - b - c)/4$, $e_3 = (1 - a + b - c)/4$, and $e_4(1 - a - b + c)/4$. Any product of two different ones of these is 0 and all have square themselves. This is $e_i e_j = 0$(if $i \neq j$) and $e_i^2 = e_i$. This latter statement says that the e_i are *idempotent*.

More generally, for a ring R, suppose $e \in R$ is idempotent. Then $R = eR \oplus (1 - e)R$, both of which are rings. Conversely, in $A \times B$, $(1, 0)$ is idempotent. So the presence of idempotents is equivalent to the ring splitting as a product.

Example 1.7. Let G be the monoid $G = \mathbb{N}$. Then $\mathbb{Z}[G]$ is still a ring if we take our basis to be $x^0, x^1, x^2, \ldots$. This makes $Z[G] = \left\{n_0x^0 + n_1x^1 + n_2x^2 + \cdots\right\}$, the polynomial ring. If we take $G = \mathbb{Z}$, we get the Laurent polynomials in $\mathbb{Z}$.

1.3.1 An alternative description of $R[G]$

We can think of elements of $R[G]$ as functions from $G \to R$, where $f(g_i) = r_i$. Then the product of $R[G]$ is given by $fh(g) = \sum_{g_1 g_2 = g} f(g_1)h(g_2)$, which is called the convolution of f and h.

Let $G = \mathbb{R}$, which is not finite. Consider the ring of all compactly supported continuous functions f. Then $f * h(x) = \int f(y)h(x - y)\, dy$, another type of convolution. This is a ring under convolution, but it does not have an identity element for convolution.[5]

1.4 Ideals

Ideals correspond to normal subgroups (kernels of homomorphisms). We define ideals by the properties we need for the kernel of a homomorphism.

Definition 1.3. An ideal I of a ring R is a subset of R such that

1. I contains 0_R and is closed under addition and subtraction (I is a normal subgroup of R with respect to addition)
2. If $r \in I$ and $t \in R$ then $rt, tr \in I$ (stronger than saying that I is closed under $\times$).

[5]The Dirac δ distribution is actually an identity for convolution for a larger ring than this.

We must check that the two conditions above are sufficient. Suppose I satisfies these. Can we form R/I? Addition is well defined since I is a normal subgroup of R with respect to addition. To see if multiplication is well defined, we first define multiplication to be $(aI)(bI) = (ab)I$. We want that if $a \equiv b$ $(a - b \in I)$ and $c \equiv d$ $(c - d \in I)$, then $ac \equiv bd$ $(ac - bd \in I)$. Let $b = a + i_1$ and $d = c + i_2$. Then

$$ac - bd = ac - (a + i_1)(c + i_2) = ac - ac - i_1c - i_2a - i_1i_2 = -(\underbrace{i_1c}_{\in I} + \underbrace{i_2a}_{\in I} + \underbrace{i_1i_2}_{\in I}).$$

If S is any subset of a ring R, we can force S to be 0 by taking the smallest ideal $I \supseteq S$. In this case, I is the set of finite sums of the form $\sum_{s_i \in S} r_i s_i t_i$ with $r_1, t_i \in R$.

1.5 Generators and relations

We form a free ring on a set S. We have 2 choices:

1. Free commutative ring: First form the free commutative monoid on S. If $S = \{x, y, z\}$, then this is $\{x^{n_1}y^{n_2}z^{n_3} : n_i \in \mathbb{N}\}$ The free commutative ring is the ring $\left\{n_{a,b,c}x^a y^b z^c : a, b, c \geq 0\right\}$.

   Say we have the elliptic curve $y^2 = x^3 - x$. We can form the coordinate ring $Z[x, y]/(y^2 - x^3 + x)$, where we are quotienting out by the ideal generated by $y^2 - x^3 + x$.

2. Noncommutative free ring: Take the noncommutative free monoid on $\{x, y, z\}$. This is all words in $\{x, y, z\}$. The noncommutative free ring is the group ring of the free monoid.

   Now we can construct rings such as $Z[x, y, z]/(x^2 + y^2z - zy^2)$ (some ideal generated by some elements), which is noncommutative.

Example 1.8. Suppose A and B are rings. We can construct the coproduct as follows: assume $A \cap B = \varnothing$, and form the free ring F on the set $A \cup B$. Quotient out by an ideal to force the map from $A \to F$ to be a homomorphism; we have $I = (f(a + b) - f(a) - f(b), f(ab) - f(a)f(b) \forall a, b, \in R)$ and so on (including all the relations we want). Then F/I is the coproduct of A and B.

Example 1.9. The coproduct of $Z[x]$ and $Z[y]$ in the category of rings is the free noncommutative ring on x, y. However, the coproduct of $Z[x]$ and $Z[y]$ in the category of commutative rings is the polynomial ring $Z[x, y]$.