More ring basics

In this lecture we continue our study of the basic properties of rings.

Let us begin with an example. The ring of quaternions $\mathbb{H}$ is the set of expressions

$$x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

where $a, b, c, d \in \mathbb{R}$, and where addition and multiplication are done in a similar fashion to the complex numbers, but where we have the relations $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ and $\mathbf{ij} = \mathbf{k}$. Note a consequence is that $\mathbf{ij} = -\mathbf{ji}$, $\mathbf{jk} = -\mathbf{kj}$, $\mathbf{ki} = -\mathbf{ik}$. In particular, $\mathbb{H}$ is not a commutative ring.

For another example, consider the quaternions $x = 1 + 2\mathbf{j}$ and $y = \mathbf{i} - \mathbf{k}$. Then

$$xy = (1 + 2\mathbf{j})(\mathbf{i} - \mathbf{k}) = (\mathbf{i} - \mathbf{k}) + 2\mathbf{j}(\mathbf{i} - \mathbf{k}) = \mathbf{i} - \mathbf{k} - 2\mathbf{k} - 2\mathbf{i} = -\mathbf{i} - 3\mathbf{k}$$

$$yx = (\mathbf{i} - \mathbf{k})(1 + 2\mathbf{j}) = \mathbf{i}(1 + 2\mathbf{j}) - \mathbf{k}(1 + 2\mathbf{j}) = \mathbf{i} + 2\mathbf{k} - \mathbf{k} + 2\mathbf{i} = 3\mathbf{i} + \mathbf{k}$$

The *norm* of a quaternion $x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ is given by the non-negative real number

$$|x| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

The *conjugate* of $x \in \mathbb{H}$ is defined by $\overline{x} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$. We compute

$$x\overline{x} = (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = a^2 + b^2 + c^2 + d^2 = |x|^2$$

As a consequence, if $x \neq 0$ (so that $|x| \neq 0$), we have $xy = 1$ where $y = (\overline{x}/|x|^2)$. Clearly y is a quaternion, and we have found a multiplicative inverse for every nonzero $x \in \mathbb{H}$. Thus:

▸ **The ring of quaternions $\mathbb{H}$ is a non-commutative division ring.**

Another example of a non-commutative ring that we saw earlier was the ring of 2×2 matrices. In fact the quaternions fit into this framework as we will see shortly. For now we continue to introduce fundamental notions in ring theory.

A *subring* of a ring R is a subset $S \subset R$ which contains $0, 1$ and with the operations $+$ and $\times$ inherited from R is a ring in its own right. Note that a subring must be closed under the operations $+$ and $\times$. The following is a simple test of whether a subset is a subring.

▸ **$S \subset R$ is a subring if and only if the multiplicative identity 1 is in S and for all $a, b \in S$ we have $ab \in S$ and $a - b \in S$.**

The proof is straightforward and omitted. For example, the inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ exhibit a chain of subrings, each one contained in the next.

A *homomorphism* $\phi : R \to R'$ is a map of sets which satisfies $\phi(1) = 1$[1] and for all $a, b \in R$:

$$\phi(ab) = \phi(a)\phi(b), \qquad \phi(a + b) = \phi(a) + \phi(b)$$

[1] Some references do not require this condition.

A homomorphism of rings is an *isomorphism* if it is 1-1 and onto.

The map $\phi : R \to R$ given by $\phi(a) = a$ for all $a \in R$ is a homomorphism, called the *identity homomorphism*. The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ which is reduction mod n is an onto ring homomorphism.

For a more interesting example, let us define a map

$$\phi : \mathbb{H} \longrightarrow \mathrm{M}_2(\mathbb{C})$$

where the ring on the right consists of 2×2 complex matrices. We define ϕ by

$$\phi(\mathbf{i}) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \phi(\mathbf{j}) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \phi(\mathbf{k}) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

and of course $\phi(1)$ is the identity matrix. These relations determine ϕ completely if extend linearly over the real numbers. Explicitly, this means that for a general quaternion,

$$\phi(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = a\phi(1) + b\phi(\mathbf{i}) + c\phi(\mathbf{j}) + d\phi(\mathbf{k}) = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

From this we have $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in \mathbb{H}$. To show $\phi(xy) = \phi(x)\phi(y)$ is a straightforward computation. Note that special cases of this include the fact that the matrices $\phi(\mathbf{i})^2$, $\phi(\mathbf{j})^2$, $\phi(\mathbf{k})^2$ are minus the identity matrix, and also

$$\phi(\mathbf{ij}) = \phi(\mathbf{k}) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \phi(\mathbf{i})\phi(\mathbf{j})$$

You can check that ϕ is 1-1, but it is not onto.

▸ **Let $\phi : R \to S$ be a ring homomorphism. Then**

1. **The map ϕ restricts to a group homomorphism $\phi^\times : (R^\times, \times) \to (S^\times, \times)$.**
2. **If ϕ is an isomorphism then $\phi^\times$ is an isomorphism of groups.**
3. **If ϕ is an isomorphism, and R is commutative, then so is S.**

It also easily follows that if ϕ is an isomorphism and R is an integral domain (resp. division ring, field) then S is an integral domain (resp. division ring, field).

Consider the ring homomorphism $\phi : \mathbb{H} \to \mathrm{M}_2(\mathbb{C})$ from above. We obtain a homomorphism of groups $\phi^\times : \mathbb{H}^\times \to \mathrm{GL}_2(\mathbb{C})$. It is instructive to consider the subgroup

$$G = \{x \in \mathbb{H}^\times : \ |x| = 1\}$$

of unit quaternions, with quaternion multiplication. Note that this group $G \subset \mathbb{H}^\times$ is in 1-1 correspondence with the 3-dimensional sphere

$$S^3 = \{(a, b, c, d) \in \mathbb{R}^4 : a^2 + b^2 + c^2 + d^2 = 1\} \subset \mathbb{R}^4$$

Indeed, the quaternion $x \in G$ where $x = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ corresponds to the point $(a, b, c, d) \in S^3$. Thus we have defined a group structure on the 3-sphere!

This is analogous to the unit complex numbers $U(1) \subset \mathbb{C}^\times$ being in 1-1 correspondence with the unit circle S^1 in $\mathbb{R}^2$, which is defined to be

$$S^1 = \{(x, y) \in \mathbb{R}^2 : \ x^2 + y^2 = 1\} \subset \mathbb{R}^2$$

In this case the unit complex number $z = x + yi$ corresponds to $(x, y) \in S^1$. Thus complex multiplication defines a group structure on the "1-sphere" S^1 in this way.

More generally we can define the n-sphere to be the following subset of points in $\mathbb{R}^{n+1}$:

$$S^n = \{(x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1} : \ x_1^2 + \cdots + x_{n+1}^2 = 1\}$$

A natural question arises: which spheres S^n have group structures? To put this question on more firm footing we require that the group operation $S^n \times S^n \to S^n$ is the restriction of a differentiable function $\mathbb{R}^{n+1} \times \mathbb{R}^{n+1} \to \mathbb{R}^{n+1}$.

We have seen such group structures on S^1 and S^3 above, using complex and quaternion multiplication respectively. A somewhat uninteresting example is that of the 0-sphere: $S^0 = \{1, -1\} \subset \mathbb{R}^1$ is a group, in fact a subgroup of $\mathbb{R}^\times$. Remarkably:

▸ **The only spheres that admit (differentiable) group structures are S^0, S^1, S^3.**

The proof is outside the scope of this class and is a result in the theory of Lie groups.