1 Quaternions

We view the quaternions $\mathcal{H}$ as a "complexification" of $\mathbb{R}^4$ when given a ring structure. Namely, the elements look like

$$a + bi + cj + dk, \quad (a, b, c, d \in \mathbb{R}),$$

Where we identify $i^2 = j^2 = k^2 = -1$, and $ij = k,\ jk = i$, and $ki = j$. Notice that from this we get the normal negative relations implied.

We also get a very nice norm in $\mathcal{H}$, given by quaternion conjugation by inheriting the norm from $\mathbb{R}^4$ as

$$\mathbf{v}\overline{\mathbf{v}} = (a + bi + cj + dj)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2.$$

Notice also that $\mathcal{H}$ is a division ring, and that in particular $\mathbf{v}^{-1} = \frac{\overline{\mathbf{v}}}{||\mathbf{v}||}$.

2 Subrings and Ideals

Note. I didn't typeset the extended discussion of polynomial rings. It's mostly a trivial construction in the category $\mathcal{R}_A$. However, there is the interesting idea of indexing sums to represent polynomials in arbitrarily many variables. It's worth noting for that a polynomial in $\frac{k[X_1,\ldots X_n]}{\langle X_1^d,\ldots,X_n^d\rangle}$, you will be able to index your sum over the partitions of d, so we can notice that there are precisely $\binom{d-1}{n-1}$ terms in the sum.

As we always do when studying a thing in math, we've studied morphisms betewen these things, so now we'll talk about substructure.

Definition 2.1. A *subring* of a ring R is a subset of R which inherits the ring structure and $S \hookrightarrow R$ is a homomorphism

2.1 The endomorphism group

Let G be an abelian group, and let $\mathrm{End}_{Ab}(G)$ be the endomorphisms. Then this is a ring in the obvious way (addition is pointwse, multiplication is composition).

Example 2.2. Notice that $\mathrm{End}_{\mathrm{AB}}(\mathbb{Z}) \cong \mathbb{Z}$ as rings, with the isomorphism given by evaluation at 1.

2.2 Cayley's Theorem for Rings

Cayley's theorem, which states that every group is a subgroup of a symmetric group, in particular states that a group acts on itself by left-multiplication. Now we define

Definition 2.3. Take $r \in R$, then let $\lambda_r : R \to R$ be given by $\lambda_r(s) = rs$.

Theorem 2.4. *Let R be a ring. Then $r \overset{\lambda}{\mapsto} \lambda_r$ is an injective ring homomorphism.*

The proof of this statement is actually just boiling down to chcking that the map is indeed an injective homomorphism. Nothing new. We've admitted it.

2.3 Ideals

Ideals are the analogue of normal subgroups for rings.

Definition 2.5. An ideal I of a ring R is a subgroup such that

$$\begin{aligned} lI \subseteq I \quad (\forall l \in R) \\ Ir \subseteq I \quad (\forall r \in R) \end{aligned}$$

Taking only one of these two conditions will give the definition of a left or right ideal respectively.

So now we can study what's so nice about ideals:

Theorem 2.6. *Let $\varphi : R \to S$ be a ring homomorphism. Then* $\ker\varphi$ *is an ideal.*

2.4 Quotients

We define a quotient ring in the same way that we define quotient groups on groups, simply replacing our language of normal subgroups with our language of ideals.

Definition 2.7. Let $I \leq R$ be an ideal. Then R/I is an abelian group with

$$(r + I) + (s + I) = (r + s) + I = (s + r) + I$$

and a ring with

$$(r + I) \cdot (s + I) = r \cdot s + I$$

Showing that ths is well defined is no trick.

Suppose that $r_1 - r_2 \in I$, and $s_1 - s_2 \in I$, in other words, r_1 and r_2 are in the same coset of our ideal (and for s). Then consider $r_1 s_1 - r_2 s_2 = r_1(s_1 - s_2) + (r_1 - r_2)s_2$, so we have well definedness.

Example 2.8. $\mathbb{Z}/n\mathbb{Z}$ is a ring.

Consider the cannonical map

$$\begin{aligned} \mathbb{Z} &\to R \\ n &\mapsto \underbrace{1_R + \ldots + 1_R}_{n \text{ times}} \end{aligned}$$

the kernel of this map is an ideal, and is either $n\mathbb{Z}$ or 0

From this example, there is a natural definition

Definition 2.9. As in the example above, n is the *characteristic* of R. If the ideal generated is the 0 ideal, then the ring is characteristic 0.

Theorem 2.10. *Let I be an ideal of R. Then for every ring homomorphism $\varphi : R \to S$ such that $I \subseteq \ker\varphi$, there is a unique ring homomorphism $\overline{\varphi}$ such that the diagram*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & S \\ & R/I \arrow[u, "\overline{\varphi}"'] \end{tikzcd}$$

commutes.

Then just like for groups, we get that if $\varphi : R \to S$ is a ring homomorphism, then

$$\begin{tikzcd} R \arrow[r, two heads] \arrow[rrr, bend right] & R/\ker(\varphi) \arrow[r, "\cong", "\varphi"'] & \mathrm{im}\varphi \arrow[r, hook] & S \end{tikzcd}$$

and hence the first isomorphism theorem for rings:

Theorem 2.11. *Let $\varphi : R \to S$ be a surjective map, then*

$$R/\ker\varphi \cong S$$