Chapter 1

crigs and modules

1.1 crigs, modules and cancellation

Definition 1.1.1. Consider the natural numbers $\mathbb{N} = \mathbb{N}_0$, with $+, \cdot$ defined as usual. Then $(\mathbb{N}, +, 0)$ is a commutative monoid, as is $(\mathbb{N}, \cdot, 1)$, and $+$ and $\cdot$ satisfy distributivity just as in a ring, i.e. with negatives for addition.

Consider the natural numbers $\mathbb{N}_{>0}$, with $+, \cdot$ defined as usual. Then $(\mathbb{N}, +)$ is a commutative semigroup, $(\mathbb{N}, \cdot, 1)$ is a commutative monoid, and $+$ and $\cdot$ satisfy distributivity just as in a ring.

Consider the natural numbers $\mathbb{N}_{>k}$ for any $k \in \mathbb{N}$ which is at least 1. Then $(\mathbb{N}, +)$ is a commutative semigroup, as is $(\mathbb{N}, \cdot, 1)$, and $+$ and $\cdot$ satisfy distributivity just as in a ring.

Example 1.1.2. In particular we note that for a ring like structure the absence of invertibles allows for maps to not fix units and zeros but still be compatible with addition and multiplication.

As an example consider the chain of inclusions $\ldots \subset \mathbb{N}_{>k} \subset \ldots \subset \mathbb{N}_{>0} \subset \mathbb{N}_0$. Each of these induces a map which is compatible with addition and multiplication, however a zero is only added in the final step, a unit in the second to last step, in particular, all inclusions before are "unpointed" with respect to such neutral elements.

Hence introduce a category to host these objects and morphisms.

Definition 1.1.3. Call a tuple $(A, +, \cdot)$ a crig (commutative ring without negatives) where A is an arbitrary set and $+ \colon A \times A \to A$ and $\cdot \colon A \times A \to A$ are binary composition maps, which are associative and commutative, and satisfy:

$$\forall a, b, c \in A \colon a \cdot (b + c) = a \cdot b + a \cdot c.$$

Call a crig unital, if there exists a unit $1 \in A$ with $\forall a \colon 1 \cdot a = a$. By commutativity it is necessarily a two-sided unit, hence unique if it exists.

As usual call a crig a ring if $(A, +, 0)$ is in fact a commutative group, that is, a monoid such that each $a \in A$ has a (unique) negative $-a \in A$ such that $a + (-a) = 0$.

In a crig that is unital and a ring it follows as usual $-a = -1 \cdot a$, that is the group inverse of $(A, +, 0)$ is controlled by only the additive inverse of the multiplicative unit -1.

Remark 1.1.4. Similarly a crig can have a zero, which is unique, if it exists, but adding a zero is not much of a problem usually, so we choose not to assign a word to that state of a crig.

Proposition 1.1.5. *For each crig there is an associated polynomial rig in one variable. More specifically, given a crig A there is a crig $A[X]$, such that for each target crig B and a crig morphism $\varphi\colon A \to B$ and a chosen element $b \in B$, there exists a unique extension morphism$\Phi\colon A[X] \to B$ with $X \mapsto b$.*

Proof. By the usual abstract nonsense $A[X]$ is unique up to crig isomorphism, fixing zeros and units if A has either one, because the canonical isomorphism is induced by the identity $A \to A$.

So prove existence, as a set write $A[X] := \{\ \sum' a_i X^i \mid i \in \mathbb{N}, a_i \in A\ \}$ with $\sum'$ denoting finite formal sums and define addition and multiplication as usual for a polynomial ring, negatives, zeroes or units are not required for that definition. Clearly a target crig structure is all that is required to define a unique extending morphism for any choice $X \mapsto b$. $\qquad\square$

Proposition 1.1.6. *For each unital crig there is an associated laurent rig in one variable. It satisfies the same universal property as above, except that b is required to be a unit in B and hence the target B also has to be unital for this to be well-defined.*

Remark 1.1.7. Note that for the laurent ring over the integers $A = \mathbb{Z}[t^{\pm 1}]$ we have the proper ideal $2A$ of all laurent polynomials with all coefficients divisible by 2. Then clearly it makes sense to consider $2A$ as the laurent polynomials on $2\mathbb{Z}$, even though $t \cdot t^{-1} = 1$ cannot be interpreted internally to the ring A.

Definition 1.1.8. Given a crig $(A, +, \cdot)$ we can consider the category of finitely generated A-modules: A finitely generated A-module is a tuple $(M, +, \lambda)$ with $(M, +)$ a commutative (additively denoted) semigroup, such that there exists an $n \in \mathbb{N}$ and a plain set surjection $A^n \to M$ (not part of the structure), and a map $\lambda\colon A \times M \to M$ which satisfies $\lambda(ab, m) = \lambda(a, \lambda(b, m))\forall a, b \in A\forall m \in M$, and $\lambda(a + b, m) = \lambda(a, m) + \lambda(b, m)\forall a, b \in A\forall m \in M$.

A morphism of A modules for a fixed crig A is a set map $\varphi\colon M \to N$, with M and N each A-modules, such that $\lambda(a, \varphi(m)) = \varphi(\lambda(a, m))\forall a \in A, m \in M$.

Many of the objects of our current interest do not have inverses but still satisfy a property which usually is just as strong.

Definition 1.1.9. A semigroup $(M, \cdot)$ is said to satisfy cancellation, if it satisfies

$$\forall m, n \in M\colon \exists k \in M\colon m \cdot k = n \cdot k \Rightarrow m = n.$$

Example 1.1.10. The natural numbers $(\mathbb{N}, +, \cdot)$ satisfy cancellation for $+$ because they include into the commutative group $(\mathbb{Z}, +)$. After excluding 0 the monoid $(\mathbb{N} \setminus \{0\}, \cdot)$ satisfies cancellation as well, because it includes into the integral domain $(\mathbb{Z}, +, \cdot)$.

More generally for a crig with an injective crig morphism to a unital commutative ring R, which is an integral domain $A \to R$, we can restrict the multiplication on A and $\cdot\colon A \setminus \{0\} \times A \setminus \{0\} \to A$ actually has target within $A \setminus \{0\}$, hence $(A \setminus \{0\}, \cdot)$ is in fact a submonoid of $(A, \cdot)$, but only $(A \setminus \{0\}, \cdot)$ can satisfy cancellation, which it does under the assumptions on R.

Remark 1.1.11. Note that for any ring (i.e., with negatives) R satisfying cancellation with respect to its multiplication is exactly equivalent to not having zero divisors:

$$\forall m, n \in M \colon \exists k \in M \colon m \cdot k = n \cdot k \Rightarrow m = n$$

$$\Leftrightarrow \forall m \in M \colon \exists k \in M \setminus \{0\} \colon m \cdot k = 0 \Rightarrow m = 0.$$

Note also how the reverse implication must use additive inverses and can just barely not be resolved in a plain cancellation monoid.

Proposition 1.1.12. *Consider a crig $(A, +, \cdot)$ and an A-module $(M, +, 0)$ that is a monoid satisfying cancellation. Then if A has a zero, we have $\lambda(0, m) = 0$ for all $m \in M$, as well as $\lambda(a, 0) = 0 \forall a \in A$.*

Proof. For arbitrary $a \in A, m \in M$ note:

$$\lambda(a, 0) = \lambda(a, 0 + 0) = \lambda(a, 0) + \lambda(a, 0) = 0 + \lambda(a, 0),$$

hence by cancellation in M: $\lambda(a, 0) = 0$. Similarly follows the claim for the zero of A. $\qquad\square$

Remark 1.1.13. Note that $2 \cdot \colon \mathbb{N} \to \mathbb{N}$ is a map that is clearly additive, respects zeroes and has target a cancellation monoid, however it is not true that the induced module structure satisfies $\lambda(1, x) = x \neq 2x!!$. The example $2 \cdot \colon \mathbb{Z} \to \mathbb{Z}$ shows that also very good additive structure cannot help fix the unit in place on a module, so fix it.

Definition 1.1.14. For $(A, +, \cdot)$ a unital crig and $\lambda \colon A \times M \to M$ an A-module structure on a semigroup $(M, +)$, call the module structure λ unital, if $\lambda(1,) = id_M$.

Example 1.1.15. We actively want the category of crigs to admit $\emptyset$ and $\mathbb{N}_{\geq 2}$ as members. Note how $2\mathbb{N} \subset \mathbb{N}_{\geq 2}$ already shows how new submodule structures arise in the absence of negatives.

Hence we shall take care of zeroes and units next.

1.2 crigs, modules and neutrals

Proposition 1.2.1. *Given a crig $(A, +, \cdot)$ and an A-module $\lambda \colon A \times M \to M$ with M a semigroup, there is an A-module M_+ with adjoint zero: $M_+ := M \sqcup \{0\}$, with a unique $\lambda \colon A \times M_+ \to M_+$, making M_+ into an A-module, such that λ restricted to $A \times M$ is the original A-module action.*