Invertible Objects: An Elementary Introduction to Picard Groups

Richard Wong

Math Club 2020

Slides can be found at
http://www.ma.utexas.edu/users/richard.wong/

How many numbers have inverses?

- $(\mathbb{N}, \times)$ has one invertible element, 1.
- $(\mathbb{N}_{\geq 0}, +)$ has one invertible element, 0.
- $(\mathbb{Z}, \times)$ has two invertible elements, 1 and -1.
- $(\mathbb{Z}, +)$ every element is invertible.
- $(\mathbb{Q}, \times)$ every element except 0 is invertible.

Recall that a ring R is a set with two operations, $+$ and $\times$ such that

- $+$ is associative and commutative, with additive identity 0.
- Every element has an additive inverse.
- $\times$ is associative, with multiplicative identity 1.
- Distributive axioms.

Example

Our favorite examples of rings include $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}/n$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$.

Given a ring R, one can always ask what the invertible elements (with respect to $\times$) are.

Definition

The set of invertible elements in a ring R is denoted by

$$R^{\times} := \{r \in R \mid r \times s = s \times r = 1\}$$

Note that 0 is never in $R^{\times}$ (except if $R = 0$).

Note that $R^{\times}$ is closed under $\times$, and in fact forms a group under $\times$. It is usually referred to as the group of units.

Example

- $\mathbb{Z}^\times = \{1, -1\}$
- $\mathbb{Q}^\times = \mathbb{Q} \setminus 0$
- $\mathbb{R}^\times = \mathbb{R} \setminus 0$
- $(\mathbb{Z}/n)^\times = \{[m] \mid 0 \leq m \leq n, m \text{ coprime to } n\}$

Question: When is an element r of R invertible?

Theorem

The following are equivalent:

(i) *There exists an element of R, s, such that $r \times s = 1$.*

(ii) *The map given by multiplication by $r : R \to R$ is an isomorphism.*

Proposition

For R a commutative ring, the group of units of $R[x]$ is as follows:

$$(R[x])^\times = \{p(x) \mid p(x) = \sum a_i x^i \text{ such that } a_0 \in R^\times, a_i \text{ nilpotent}\}$$

Challenge: Prove it!

Example

If R is an integral domain, then $(R[x])^\times = R^\times$.

How can we generalize this idea?

From now onwards, let R be a commutative ring.

Instead of trying to study R by itself, one might instead study $\mathrm{Mod}(R)$, the category of modules over R.

Recall that an R-module is an abelian group $(M, +)$, and an operation $\cdot : R \times M \to M$ such that

- $\cdot$ is associative
- $1 \cdot m = m$ for all $m \in M$
- $\cdot$ is distributive over addition.

Example

If k is a field, then k-modules are exactly the same as k-vector spaces.

Example

For $R = \mathbb{Z}$, the notion of $\mathbb{Z}$-module is exactly the same as an abelian group. (That is, every abelian group is a module over $\mathbb{Z}$ in a unique way.)

In Mod(R), we have an operation called tensor product, denoted $\otimes_R$ or $\otimes$, which satisfies the following properties:

1. It has a unit, given by R: $M \otimes_R R \cong M \cong R \otimes_R M$.
2. It is associative: $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$.
3. It is symmetric: $M \otimes N \cong N \otimes M$.
4. It distributes over direct sums: $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$.
5. The scalar multiplication on $M \otimes N$ is given by scalar multiplication on M or equivalently by scalar multiplication on N (which are forced to be equal). $r \cdot (M \otimes N) \cong (r \cdot M) \otimes N \cong M \otimes (r \cdot N)$.

Example

If k is a field, and V and W are modules (vector spaces) over k with bases $\{e_i\}$ and $\{f_j\}$ respectively, then $V \otimes W$ is defined to be the vector space with basis given by $\{e_i \otimes f_j\}$.
For example, on elements, if $v = a_1 e_1 + a_2 e_2 \in V$ and $w = b_1 f_1 + b_2 f_2 \in W$, then
$v \otimes w = a_1 e_1 \otimes b_1 f_1 + a_1 e_1 \otimes b_2 f_2 + a_2 e_2 \otimes b_1 f_1 + a_2 e_2 \otimes b_2 f_2$
$= a_1 b_1 (e_1 \otimes f_1) + a_1 b_2 (e_1 \otimes f_2) + a_2 b_1 (e_2 \otimes f_1) + a_2 b_2 (e_2 \otimes f_2)$.

Challenge: Does $v \otimes w$ depend on the choice of basis?

Example

However, if R is a commutative ring, and M and N are R-modules, then $M \otimes N$ is merely *spanned* by elements $m \otimes n$.
We have distributivity:

$$(m + m') \otimes n = m \otimes n + m' \otimes n$$

$$m \otimes (n + n') = m \otimes n + m \otimes n'$$

And scalar multiplication tells us:

$$r \cdot (m \otimes n) = (r \cdot m) \otimes n = m \otimes (r \cdot n)$$

Challenge: How can we define equality of elements without a basis?

Question: When is a module N invertible with respect to $\otimes$?

Given an R-module N, we have a functor

$$- \otimes_R N : \mathrm{Mod}(R) \to \mathrm{Mod}(R)$$

Analogy: Given an element $r \in R$, we have a map $- \times r : R \to R$.

Theorem

The following are equivalent:

(i) *There exists an R-module M such that $M \otimes N \cong R$. We say that N is invertible.*

(ii) $- \otimes N : \mathrm{Mod}(R) \to \mathrm{Mod}(R)$ *is an equivalence of categories. (**Analogy:** $- \times r : R \to R$ an isomorphism)*

(iii) *N is finitely generated projective module of rank 1.*

In fact, in case (ii) we have that $M \cong \mathrm{Hom}_R(N, R)$.

Observation: The set of isomorphism classes of invertible R-modules has a group structure:

Definition

The Picard group of R, denoted $\mathrm{Pic}(R)$, is the set of isomorphism classes of invertible modules, with

$$[M] \cdot [N] = [M \otimes N]$$

$$[M]^{-1} = [\mathrm{Hom}_R(M, R)]$$

Example

For R a local ring or PID, $\mathrm{Pic}(R)$ is trivial.

Proof.

For local rings/PIDs, a module is projective iff it is free. Hence $M \in \mathrm{Pic}(R)$ iff M is a free rank 1 R-module. □

Chain Complexes of R-modules

Let's see what happens if we work with chain complexes of R-modules, $\mathrm{Ch}(R)$, instead.

Definition

A chain complex of R-modules is a sequence of R-modules A_k, along with homomorphisms (called **differentials**) $d_k : A_k \to A_{k-1}$, such that for all k, $d_k \circ d_{k+1} = 0$.

$$\cdots \xrightarrow{d_{k+2}} A_{k+1} \xrightarrow{d_{k+1}} A_k \xrightarrow{d_k} A_{k-1} \xrightarrow{d_{k-1}} \cdots$$

Chain Complexes of R-modules

Example

Given an integer n, and an R-module M, there is a chain complex $M[n]$ given by

$$(M[n])_k = \begin{cases} M & k = n \\ 0 & \text{else} \end{cases}$$

$$\cdots \to 0 \to M \to 0 \to \cdots$$

Chain Complexes of R-modules

Definition

The tensor product of two chain complexes $X_\bullet$ and $Y_\bullet$ is defined at degree n by

$$(X \otimes Y)_k = \bigoplus_{i+j=k} (X_i \otimes Y_j)$$

This tensor product is also associative and symmetric, and has unit given by $R[0]$.

Challenge: What are the differentials for $(X \otimes Y)_\bullet$?

Question: When is $Y_\bullet$ invertible?

Theorem

The following are equivalent for a local ring R:

(i) $Y_\bullet$ *is invertible. That is, there exists a chain complex* $X_\bullet$ *such that* $X_\bullet \otimes Y_\bullet \cong R[0]$.

(ii) $- \otimes Y_\bullet : \mathrm{Ch}(R) \to \mathrm{Ch}(R)$ *is an equivalence of categories.*

(iii) $Y_\bullet$ *is the chain complex* $R[n]$, *that is, the complex* R *concentrated in a single degree* n.

Example

For R a local ring, $\mathrm{Pic}(\mathrm{Ch}(R))$ is isomorphic to $\mathbb{Z}$.

Generalizations

What did we need to define Pic(R) and Pic(Ch(R))?

We only really needed the associative, symmetric, and unital structure of $\otimes$.

Definition

Suppose we have a category $\mathcal{C}$ that has bifunctor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ with unit 1 and is associative and symmetric.
Then we say that $(\mathcal{C}, \otimes, 1)$ is a **symmetric monoidal category**.

Example

The following categories are symmetric monoidal:

(a) $(\text{Set}, \times, \{*\})$
(b) $(\text{Group}, \times, \{e\})$
(c) $(\text{Mod}(R), \otimes, R)$
(d) $(\text{Ch}(R), \otimes, R[0])$

Definition

The Picard group of a symmetric monoidal category $(\mathcal{C}, \otimes, 1)$, denoted $\text{Pic}(\mathcal{C})$, is the set of isomorphism classes of invertible objects X, with

$$[X] \cdot [Y] = [X \otimes Y]$$

$$[M]^{-1} = [\text{Hom}_{\mathcal{C}}(X, 1)]$$

Example

We have that $\text{Pic}(R) = \text{Pic}(\text{Mod}(R))$.

However, we had more interesting structure in $\mathrm{Pic}(\mathrm{Ch}(R))$ since we could shift the unit $R[0]$ up or down.

"Definition"

A symmetric monoidal category $(\mathcal{C}, \otimes, 1)$ is called ***stable*** *if it also has a suspension functor $\Sigma : \mathcal{C} \to \mathcal{C}$ that is an equivalence of categories.*
In addition, Σ should play nicely with the tensor product. That is, $\Sigma(A \otimes B) \cong \Sigma A \otimes B$.

Warning: This definition is only right when using ∞-categories. (**Stable** has homotopical meaning). Alternatively, we can make a similar definiton using triangulated categories.

Example

The following categories are stable symmetric monoidal:

(a) $(D(R), \hat{\otimes}_R, R[0], -[1])$ for R a commutative ring.

(b) $(\mathrm{Sp}, \wedge, \mathbb{S}, \Sigma)$

(c) $(\mathrm{Mod}(R), \wedge_R, R, \Sigma)$ for R a commutative ring spectrum.

(d) $(L_E(\mathrm{Sp}), L_E(- \wedge -), L_E\mathbb{S}, \Sigma)$ for a spectrum E. In particular, $E = E(n)$ or $K(n)$.

(e) $(\mathrm{StMod}(kG), \otimes_k, k, \Omega^{-1})$ for G a p-group and k a field of characteristic p.

Theorem (Hopkins-Mahowald-Sadofsky)

$\mathrm{Pic}(\mathrm{Sp}) \cong \mathbb{Z}$

Proposition (Baker-Richter)

For R a commutative ring spectrum, we have a monomorphism

$$\Phi : \mathrm{Pic}(\pi_*(R)) \hookrightarrow \mathrm{Pic}(R)$$

“Theorem” (Hopkins)

For the spectra $K(n)$ and $E(n)$ at some fixed prime p, the Picard groups $\mathrm{Pic}(L_{E(n)}(\mathrm{Sp}))$ and $\mathrm{Pic}(L_{K(n)}(\mathrm{Sp}))$ are extremely interesting.

This is a subject of active research!

Thanks for listening!