Basic Algebra

Part III prepatory notes based on Basic Algebra by Nathan Jacobson

Notes taken by James Arthur

Autumn 2021

Part III requires a load of complex and interesting Mathematics that I have not covered thus far in my course and will not. These collections of notes are my thoughts on topics and needed intuition to bits of Mathematics. They aren't here to teach or to be used a stand alone text.

Contents

1 Monoids and Groups

Let's start from the beginning as the beginning is a good place to start,

1.1 Monoids

Definition 1.1 (Monoid)**.** A triple (M, p, e) where M is a nonempty set, or carrier, p is an associative binary operation and e is an identity such that, $p(e, a) = p(a, e) = a$

If we let p be non-associative, then we have a *monad* and if we drop the hypothesys on 1, then we get a *semigroup*.

Lemma 1.2 (Unique Identity)**.** The identity of a monoid is unique.

We can define a submonoid,

Definition 1.3 (Submonoid)**.** A subset N of M is a submonoid if it contains e and id closed under p.

Definition 1.4 (Finite Monoid)**.** A monoid is said to be finite if it has a finite number of elements. We shall call it's cardinality, it's *order*.

1.2 Groups

An element u of a monoid is said to invertible if there exists a $v \in M$ such that,

$$uv = 1 = vu$$

Definition 1.5 (Group)**.** A group G is a monoid all of whose elements are invertible.

We define the subgroup in the same way as the submonoid.

Definition 1.6 (Group of Units)**.** If we take a monoid M, then we can denote all of the units as a set $U(M)$. Then we can prove this is a group and call it a group of units.

If we now just take a load of monoids or groups, we can create another monoid or group out of them. Take $M_1, \ldots, M_n$ and then consider $M = M_1 \times \cdots \times M_n$, we introduce the following product,

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

We call this the direct product of monoids and groups.

1.3 Isomorphisms

We can call two groups, basically the same using ismorphisms,

Definition 1.7 (Isomorphism)**.** Two monoids $(M, p, 1)$ and $(M', p', 1')$ are said to be isomorphic if there exists a bijective map η of M to M' such that,

$$\eta(1) = 1' \qquad \eta(x \circ y) = \eta(x)\eta(y) \qquad x, y \in M$$

This shall be denoted as $M \cong M'$

Example. We can find an ismorphism between $(\mathbb{R}, +, 0)$ and $(\mathbb{R}^+, \cdot, 1)$. We just need to find an η and that here is just, $\eta(x) = e^x$ as we can say,

$$e^{x+y} = e^x e^y$$

This then has an inverse $y \mapsto \log y$ and hence is bijective.

Theorem 1.8 (Cayley Theorem for Monoids and Groups)**.** The following is true:

(i) Any monoid is isomorphic to a monoid of transformations

(ii) Any group is isomorphic to a transformation group.

Proof. We shall treat two parts of the theorem individually

(i) Firstly, we are going to take a monoid M and consider the map $a_L : a \to ax$ for an $a \in M$, note that this map is always in M. Now we claim that $\{a_L : a \in M\}$ is a monoid of transformations. We can see this is closed under composition, then we can consider $a_L b_L$ and see that this is just $x \to a(bx)$ and by the associative law $x \to (ab)x$ and so, $a_l b_L = (ab)_L$. So $a \to a_L$ is an isomorphism of M onto the monoid of transformations. This map is obviously surjective and we can also say it is injective as if $a_L = b_L$ then $a = a_L 1 = b_L 1 = b$

(ii) If we have G as a group, then everything follows from (1) if we can see that G_L is the group of transformations. We need to show that a_L is bijective and G_L is closed under inverses. We can see this from $1_L = (a^{-1}a)_L = (a^{-1})_L a_L$ and $1_L = a_L(a^{-1})_L$

□

Corollary 1.9. Any finite group of order n is isomorphic to some subgroup of S_n.

1.4 Generalised Associativity, Commutativity

Associativity lets us just consider any string of multiplications and just ignore the brackets as we can preform the multiplications in any order.

Definition 1.10 (Commutativity)**.** For all $a, b \in M$ where M is a monoid, if the following holds,

$$ab = ba$$

Then we say we have a commutative monoid or abelian monoid.

When we defined the identity we said for some $a \in M$, we have $a \cdot e = a = e \cdot a$. We notice that e is commutative in every monoid (and group). We can consider something more general than this now, we can consider all the elements of a group or a monoid that are commutative, the centraliser.

Definition 1.11 (Centraliser)**.** Let M be a monoid, then the centraliser of $m \in M$ is,

$$C_M(m) = \{n \in M : mn = nm\}$$

Furthermore we define the centre of the monoid (or group) as,

$$C(M) = \bigcap_{m \in M} C_M(m)$$