INTRODUCTION TO ALGEBRA

CARSON JAMES

Contents

1. Groups

1.1. Direct Products.

Definition 1.1.1. Let G, H be groups. Define a product $* : (G \times H) \times (G \times H) \to G \times H$ by

$$(x_1, y_1) * (x_2, y_2) = (x_1 x_2, y_1 y_2)$$

Then $(G \times H, *)$ is called the **direct product of G and H**.

Exercise 1.1.2. Let G, H be groups. Then the direct product $G \times H$ is a group.

Proof. Clear. □

Definition 1.1.3. Let G, H be groups. Define $\pi_G : G \times H \to G$ and $\pi_H : G \times H \to H$ by $\pi_G(x, y) = x$ and $\pi_H(x, y) = y$. Then π_G and π_H are respectively called the **projection maps onto G and H**.

Exercise 1.1.4. Let G, H be groups. Then

(1) $\pi_G : G \times H \to G$ and $\pi_H : G \times H \to H$ are homomorphisms
(2) $\ker \pi_G \cong H$ and $\ker \pi_H \cong G$

Proof.

(1) Clear
(2) Define $\iota_G : G \to \ker \pi_H$ by

$$\iota_G(x) = (x, e_H)$$

Then ι_G is an isomorphism. Similarly, we can define $\iota_H : H \to \ker \pi_G$ and show that it is an isomorphism.

□

Definition 1.1.5. Let G, H, K be groups, $\phi \in \mathrm{Hom}(G, K)$ and $\psi \in \mathrm{Hom}(H, K)$. We define $\phi \times \psi : G \times H \to K$ by $\phi \times \psi(x, y) = \phi(x)\psi(y)$

Exercise 1.1.6. Let G, H, K be groups, $\phi \in \mathrm{Hom}(G, K)$ and $\psi \in \mathrm{Hom}(H, K)$. If K is abelian, then $\phi \times \psi \in Hom(G \times H, K)$.

Proof. Let $x_1, x_2 \in G$ and $y_1, y_2 \in H$. Then

$$\begin{aligned}
\phi \times \psi[(x_1, y_1)(x_2, y_2)] &= \phi \times \psi(x_1 x_2, y_1 y_2) \\
&= \phi(x_1 x_2)\psi(y_1 y_2) \\
&= \phi(x_1)\phi(x_2)\psi(y_1)\psi(y_2) \\
&= \phi(x_1)\psi(y_1)\phi(x_2)\psi(y_2) \\
&= [\phi \times \psi(x_1, y_1)][\phi \times \psi(x_2, y_2)]
\end{aligned}$$

□

Exercise 1.1.7. Let G, H, K be groups and $\phi \in \mathrm{Hom}(G \times H, K)$. Then there exist $\phi_G \in \mathrm{Hom}(G, K)$, $\phi_H \in \mathrm{Hom}(H, K)$ such that $\phi_G \times \phi_H = \phi$.

Proof. Suppose that K is abelian. Define $\iota_G \in \mathrm{Hom}(G, \ker \pi_H)$ and $\iota_H \in \mathrm{Hom}(H, \ker \pi_G)$ as in part (2) of Exercise 1.1.4 Define $\phi_G \in \mathrm{Hom}(G, K)$ and $\phi_H \in \mathrm{Hom}(H, K)$ by $\phi_G = \phi \circ \iota_G$ and $\phi_H = \phi \circ \iota_H$. Let $(x, y) \in G \times H$. Then

$$\begin{aligned}
\phi_G \times \phi_H(x, y) &= \phi_G(x)\phi_H(y) \\
&= \phi \circ \iota_G(x)\phi \circ \iota_H(y) \\
&= \phi(x, e_H)\phi(e_G, y) \\
&= \phi(x, y)
\end{aligned}$$

So $\phi = \phi_G \times \phi_H$ $\square$

2. Rings

Definition 2.0.1. Let R be a set and $+, * : R \times R \to R$ (we write $a+b$ and ab in place of $+(a,b)$ and $*(a,b)$ respectively). Then R is said to be a **ring** if for each $a,b,c \in R$,

(1) R is an abelian group with respect to $+$. The identity element with respect to $+$ is denoted by 0.
(2) R is a monoid with respect to $*$. The identity element of R with respect to $*$ is denoted 1.
(3) R is commutative with respect to $*$.
(4) $*$ distributes over $+$.

Definition 2.0.2. Let R be a ring and $I \subset R$. Then I is said to be an **ideal** of R if for each $a \in R$ and $x, y \in I$,

(1) $x + y \in I$
(2) $ax \in I$

Definition 2.0.3. Let R be a ring and $A, B \subset R$. We define the **product** of A and B, denoted AB, to be

$$AB = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in A, b_i \in B, n \in \mathbb{N} \right\}$$

Exercise 2.0.4. Let R be a ring and $I \subset R$. Then I is an ideal of R iff $RI \subset I$.

Proof. Suppose that $RI \subset I$. Let $a \in R$ and $x, y \in I$. Then by assumption $x+y = 1x+1y \in I$ and $ax \in I$. So I is an ideal of R
Conversely, suppose that I is an ideal of R. Let $a_1, \cdots, a_n \in R$ and $x_1, \cdots, x_n \in I$. Then by assumption, for each $i = 1, \cdots, n$, $a_i x_i \in I$ and therefore $\sum\limits_{i=1}^{n} a_i b_i \in I$. Hence $RI \subset I$. $\square$

3. Modules

3.1. Introduction.

Definition 3.1.1. Let R be a ring, M a set, $+ : M \times M \to M$ and $* : R \times M \to M$ (we write rx in place of $*(r, x)$). Then M is said to be an R**-module** if

1. M is an abelian group with respect to $+$. The identity element of M with respect to $+$ is denoted by 0.
2. for each $r \in R$, $*(r, \cdot)$ is a group endomorphism of M
3. for each $x \in M$, $*(\cdot, x)$ is a group homomorphism from R to M
4. $*$ is a monoid action of R on M

Note 3.1.2. For the remainder of this section, we assume that R is a commutative ring.

Exercise 3.1.3. Let M be an R-module. Then for each $r \in R$ and $x \in M$,

1. $r0 = 0$
2. $0x = 0$
3. $(-1)x = -x$

Proof. Let $r \in R$ and $x \in M$. Then

(1)
$$\begin{aligned} r0 &= r(0+0) \\ &= r0 + r0 \end{aligned}$$
which implies that $r0 = 0$.

(2)
$$\begin{aligned} 0x &= (0+0)x \\ &= 0x + 0x \end{aligned}$$
which implies that $0x = 0$.

(3)
$$\begin{aligned} (-1)x + x &= (-1)x + 1x \\ &= (-1+1)x \\ &= 0x \\ &= 0 \end{aligned}$$
which implies that $(-1)x = -x$.

□

Definition 3.1.4. Let M an R-module and $N \subset M$. Then N is said to be a **submodule** of M if for each $r \in R$ and $x, y \in N$, we have that $rx \in N$ and $x + y \in N$.

Definition 3.1.5. Let M be an R-module. We define $\mathcal{S}(M) = \{N \subset M : N \text{ is a submodule of } M\}$.

Exercise 3.1.6. Let M be an R-module and $N \in \mathcal{S}(M)$. Then N is a subgroup of M.

Proof. Let $x, y \in M$. Then $x - y = 1x + (-1)y \in N$. So N is a subgroup of M. □

Definition 3.1.7. Let M be an R-module and $N \in \mathcal{S}(M)$. We define

1. $M/N = \{x + N : x \in M\}$

(2) $+ : M/N \times M/N \to M/N$ by
$$(x+N)+(y+N) = (x+y)+N$$
(3) $* : R \times M/N \to M/N$ by
$$r(x+N) = (rx)+N$$

Under these operations (see next exercise), M/N is an R-module known as the **quotient module** of M by N.

Exercise 3.1.8. Let M be an R-module and $N \in \mathcal{S}(M)$. Then

(1) the monoid action defined above is well defined
(2) the quotient M/N is an R-module

Proof.

(1) Let $r \in R$ and $x+N, y+N \in M/N$. Recall from group theory that $x+N = y+N$ iff $x-y \in N$. Suppose that $x+N = y+N$. Then $x-y \in N$ and there exists $n \in N$ such that $x-y = n$. Therefore
$$\begin{aligned} rx - ry &= r(x-y) \\ &= rn \\ &\in N \end{aligned}$$
So $rx+N = ry+N$.
(2) Properties (1) - (4) in the definition of a module are easily shown to be satisfied for M/N since they are true for M.

$\square$

Definition 3.1.9. Let M and N be R-modules and $\phi : M \to N$. Then ϕ is said to be a **module homomorphism** if for each $r \in R$ and $x, y \in M$

(1) $\phi(rx) = r\phi(x)$
(2) $\phi(x+y) = \phi(x)+\phi(y)$

Exercise 3.1.10. Let M and N be R-modules and $\phi : M \to N$. Then ϕ is a iff for each $r \in R$ and $x, y \in M$, $\phi(x+ry) = \phi(x)+r\phi(y)$.

Proof. Clear. $\square$

Exercise 3.1.11. Let M and N be R-modules and $\phi : M \to N$ a homomorphism. Then

(1) $\ker \phi$ is a submodule of M
(2) $\operatorname{Im} \phi$ is a submodule of N

Proof. Let $r \in R$, $x, y \in \ker \phi$ and $w, z \in \operatorname{Im} \phi$. Then

(1)
$$\begin{aligned} \phi(rx) &= r\phi(x) \\ &= r0 \\ &= 0 \end{aligned}$$
So $rx \in \ker \phi$. Group theory tells us that $\ker \phi$ is a subgroup of M, so $x+y \in \ker \phi$. Hence $\ker \phi$ is a submodule of M.
(2) Similar.

□

Definition 3.1.12. Let M be an R-module and $A \subset M$. We define the **submodule of** M **generated by** A, denoted $\text{span}(A)$, to be

$$\text{span}(A) = \bigcap_{N \in \mathcal{S}(M)} N$$

Exercise 3.1.13. Let M be an R-module and $A \subset M$. Then $\text{span}(A) \in \mathcal{S}(M)$

Proof. Let $r \in R$ and $x, y \in \text{span}(A)$. Basic group theory tells us that $\text{span}(A)$ is a subgroup of M. So $x + y \in \text{span}(A)$. For $N \in \mathcal{S}(M)$, by definition we have $x \in N$ and therefore $rx \in N$. So $rx \in \text{span}(A)$. Hence $\text{span}(A)$ is a submodule of M. □

Exercise 3.1.14. Let M be an R-module and $A \subset M$. If $A \neq \varnothing$, then

$$\text{span}(A) = \left\{ \sum_{i=1}^{n} r_i a_i : r_i \in R, a_i \in A, n \in \mathbb{N} \right\}$$

Proof. Clearly □

Definition 3.1.15. Let M

4. Fields

5. Vector Spaces

6. Appendix

6.1. Monoids.

Definition 6.1.1. Let G be a set and $* : G \times G \to G$ (we write ab in place of $*(a, b)$). Then

(1) $*$ is called a **binary operation** on G
(2) $*$ is said to be **associative** if for each $x, y, z \in G$, $(xy)z = x(yz)$
(3) $*$ is said to be **commutative** if for each $x, y \in G$, $xy = yx$

Definition 6.1.2. Let G be a set, $* : G \times G \to G$, $e, x, y \in G$. Then e is said to be an **identity element** if for each $x \in G$, $ex = xe = x$.

Definition 6.1.3. Let G be a set and $* : G \times G \to G$. Then G is said to be a **monoid** if

(1) $*$ is associative
(2) there exits $e \in G$ such that e is an identity element.

Exercise 6.1.4. Let G be a monoid. Then the identity element is unique.

Proof. Let $e, f \in G$. Suppose that e and f are identity elements. Then $e = ef = f$. $\square$

Note 6.1.5. Unless otherwise specified, we will denote the identity element of a monoid by e.

Definition 6.1.6. Let G be a monoid, X a set and $* : G \times X \to X$ (we write gx in place of $*(g, x)$). Then $*$ is said to be a **monoid action** of G on X if for each $g, h \in G$ and $x \in X$,

(1) $(gh)x = g(hx)$
(2) $ex = x$