

## REVISION ON GROUPS AND LINEAR ALGEBRA

### 1. GROUPS

A *group* consists of a set  $G$  together with a rule for combining any  $g, h \in G$  to get another element  $gh \in G$ , called the product. This should satisfy

1. for all  $g, h, k \in G$  we have  $(gh)k = g(hk)$ ;
2. there exists  $e \in G$  such that  $eg = g = ge$  for all  $g \in G$ ;
3. for all  $g \in G$  there exists  $g^{-1} \in G$  such that  $gg^{-1} = e = g^{-1}g$ .

The *order* of  $G$ , written  $|G|$ , is the number of elements in  $G$  (either a positive integer or infinity).

**Examples.** (a)  $C_n$ , the *cyclic group* of order  $n$ : the elements of  $C_n$  are  $(e, x, x^2, \dots, x^{n-1})$  and  $x^n = e$ ; the product is multiplication.

(b)  $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$  is a group under multiplication.

(c)  $S_n$ , the *symmetric group* (on  $n$  letters): the elements of  $S_n$  are permutations (i.e. rearrangements) of  $\{1, \dots, n\}$ ; the product is composition. A simple count gives  $|S_n| = n!$ .

For example if  $n = 6$  then if  $g = (1\ 2\ 4)(3\ 5)$  and  $h = (1\ 4)(2\ 6)$  we get  $gh = (2\ 6\ 4)(3\ 5)$ .

(d)  $D_n$ , the *dihedral group* of order  $2n$ : the elements of  $D_n$  are the symmetries of the regular polygon with  $n$  vertices sitting in the plane; the product is composition. There are rotations and reflections in this group (how many of each?)

(e) Let  $F$  be any field.  $GL(n, F)$ , the *general linear group*: the elements are  $n$ -by- $n$  invertible matrices with entries from  $k$ ; the product is matrix multiplication. (e.g.  $F = \mathbb{C}$  and  $n = 1$  gives example (d))

As a good exercise show that  $|GL(2, \mathbb{F}_q)| = (q^2 - 1)(q^2 - q)$ , where  $\mathbb{F}_q$  is the field with  $q$  elements (and  $q$  is a prime power).

### 2. SUBGROUPS

A subset  $H \subseteq G$  is a subgroup if  $H$  is a group under the product operation inherited from  $G$ . We write  $H \leq G$ .

**Examples.** (a) Suppose  $d|n$ . Then  $(e, x^d, x^{2d}, \dots, x^{n-d})$  is a subgroup of  $C_n$ .

(b)  $\mu_n$ , the  $n$ th roots of 1.

(c) All rotations in  $D_n$ .

(d)  $A_n$ , the *alternating group*, consisting of even permutations. (e.g. the elements  $e, (1\ 2\ 3), (1\ 3\ 2)$  comprise  $A_3$ ).

(e)  $SL(n, F)$ , the *special linear group*, consisting of matrices whose determinant is 1.

Show that  $|SL(2, \mathbb{F}_q)| = q(q+1)(q-1)$ .

### 3. HOMOMORPHISMS

A mapping  $\theta : G \longrightarrow H$  between groups is called a *homomorphism* if

$$\theta(gg') = \theta(g)\theta(g') \quad \text{for all } g, g' \in G.$$

If  $\theta$  is a bijection (i.e. invertible) then  $\theta$  is an *isomorphism* and  $G$  and  $H$  are *isomorphic* (which means that they are algebraically indistinguishable).

It's good to think about why  $\mu_n$  and  $C_n$  are isomorphic, but not **canonically** isomorphic.

We define

$$\text{im } \theta = \{h : h = \theta(g) \text{ for some } g \in G\} \text{ and } \ker \theta = \{g : \theta(g) = e\}.$$

Then  $\text{im } \theta \leq H$  and  $\ker \theta \leq G$ .

We have  $\theta$  is injective if and only if  $\ker \theta = \{e\}$ , the trivial subgroup;  $\theta$  is surjective if and only if  $\text{im } \theta = H$ .

### 4. COSETS AND NORMAL SUBGROUPS

Let  $H \leq G$ . For  $x \in G$  the subset  $Hx = \{hx : h \in H\}$  is a *right coset* of  $H$  in  $G$ ;  $xH = \{xh : h \in H\}$  is a *left coset*.

The right cosets of  $H$  (or equally, the left cosets) form a partition of  $G$  into equally sized pieces. The number of cosets (i.e. pieces) is the *index* and is written  $|G : H|$  (it is same whether you choose right or left cosets). The index is calculated by **Lagrange's Theorem**.

**Example.**  $H = \{e, (1\ 2)\} \leq S_3$ . The right cosets are

$$\{e, (1\ 2)\} = He = H(1\ 2), \{(1\ 3), (1\ 3\ 2)\} = H(1\ 3) = H(1\ 3\ 2), \{(2\ 3), (1\ 2\ 3)\} = H(2\ 3) = H(1\ 2\ 3).$$

The left cosets are

$$\{e, (1\ 2)\} = eH = (1\ 2)H, \{(1\ 3), (1\ 2\ 3)\} = (1\ 3)H = (1\ 3\ 2)H, \{(2\ 3), (1\ 3\ 2)\} = (2\ 3)H = (1\ 2\ 3)H.$$

Note that these partitions into right or left cosets are not the same.

$H$  is a *normal subgroup* of  $G$  if the partition of  $G$  into left cosets of  $H$  is equal to the partition of  $G$  into right cosets of  $H$ . We write  $H \triangleleft G$ . An equivalent formulation is  $H \triangleleft G$  if and only if  $xH = Hx$  for all  $x \in G$  if and only if  $xHx^{-1} = H$  for all  $x \in G$ .

If  $H \triangleleft G$  then we can form the *factor group*  $G/H$  whose elements are left (=right) cosets  $xH$  and whose product is given by

$$(xH)(yH) = (xy)H \quad \text{for all } x, y \in G.$$

For example if  $\theta$  is a group homomorphism then  $\ker \theta \triangleleft G$  whilst  $\text{im } \theta$  is not in general normal. You should remind yourself of the First Isomorphism Theorem.

### 5. CONJUGACY CLASSES

Given  $x, y \in G$  we say that  $x$  and  $y$  are *conjugate* (in  $G$ ) if there exists  $g \in G$  such that  $y = gxg^{-1}$ .

Let  $Cl(x) = \{y : y = gxg^{-1} \text{ for some } g \in G\}$  be the *conjugacy class* of  $x$ . Conjugacy classes partition  $G$  into subsets of various sizes.

**Example.** In  $S_3$  the conjugacy classes are  $\{e\} = Cl(e)$ ,  $\{(12), (13), (23)\} = Cl((12)) = Cl((13)) = Cl((23))$ , and  $\{(123), (132)\} = Cl((123)) = Cl((132))$ .

We set  $C_G(x) = \{g \in G : gxg^{-1} = x\} \leq G$ , the *centraliser* of  $x$  in  $G$ . A special case of the **orbit-stabiliser theorem** states that

$$\frac{|G|}{|C_G(x)|} = |Cl(x)|.$$

### 6. VECTOR SPACES AND THEIR BASES

Let  $F$  be a field. A *vector space* over  $F$  is a set  $V$  together with an addition and a scalar multiplication satisfying the following:

1.  $V$  is an abelian group under addition (the identity is written as 0),
2. for all  $u, v \in V$  and for all  $\lambda, \mu \in F$  we have
  - (a)  $\lambda(u + v) = \lambda u + \lambda v$
  - (b)  $(\lambda + \mu)v = \lambda v + \mu v$
  - (c)  $(\lambda\mu)v = \lambda(\mu v)$
  - (d)  $1v = v$ .

(In another language,  $V$  is an  $F$ -module.)

**Examples.** (a)  $\mathbb{R}^2$ .

(b)  $F^n$ : it's elements are column vectors of length  $n$  with entries in  $F$ .

(c)  $C^\infty(\mathbb{R}) = \{\text{smooth functions on } \mathbb{R}\}$

The vectors  $v_1, \dots, v_n$  are a *basis* of  $V$  if and only if

- they *span*  $V$  i.e. every element of  $V$  can be written as  $\lambda_1 v_1 + \dots + \lambda_n v_n$  for some  $\lambda_1, \dots, \lambda_n \in F$ ,
- they are *linearly independent* i.e.  $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$  implies that  $\lambda_1 = \dots = \lambda_n = 0$ .

(From now on we will only consider finite dimensional vector spaces.) The number of elements in a basis depends only on  $V$ , not on the choice of basis; we call the number the *dimension* of  $V$  and write  $\dim V$ .

**Example.**  $\dim F^n = n$ : it has a basis  $(1, 0, \dots, 0)^T, (0, 1, \dots, 0)^T, \dots, (0, 0, \dots, 1)^T$ ; it also has a basis  $(1, 1, \dots, 0)^T, (0, -1, \dots, 0)^T, \dots, (0, 0, \dots, 1)^T$ .

## 7. SUBSPACES AND DIRECT SUMS

A *subspace* of  $V$  over  $F$  is a subset of  $V$  which is a vector space under the inherited addition and scalar multiplication.

**Examples.** (a)  $\{0\}$  and  $V$  are always subspaces.

(b) Given elements  $u_1, \dots, u_r \in V$  then  $\text{sp}(u_1, \dots, u_r) = \{\lambda_1 u_1 + \dots + \lambda_r u_r : \lambda_i \in F \text{ for } 1 \leq i \leq r\}$  is a subspace, the *subspace spanned by*  $u_1, \dots, u_r$ .

Note that if  $U$  is a subspace of  $V$  then any basis of  $U$  can be extended to a basis of  $V$ . In particular, this means that  $\dim U \leq \dim V$  with equality if and only if  $U = V$ .

If  $U_1, \dots, U_r$  are subspaces of  $V$  then

$$U_1 + \dots + U_r := \{u_1 + \dots + u_r : u_i \in U_i \text{ for } 1 \leq i \leq r\}$$

is a subspace of  $V$  called the *sum of the  $U_i$ 's*. We say that  $U_1 + \dots + U_r$  is a *direct sum* if every element of the sum can be written in a unique way as  $u_1 + \dots + u_r$  with  $u_i \in U_i$  for  $1 \leq i \leq r$ . In this case we write  $U_1 \oplus \dots \oplus U_r$ .

The case of  $r = 2$  will be used again and again in the course. Suppose  $U, W \subseteq V$  are subspaces with respective bases  $u_1, \dots, u_s$  and  $w_1, \dots, w_t$ . The following are equivalent

1.  $V = U \oplus W$
2.  $u_1, \dots, u_s, w_1, \dots, w_t$  is a basis of  $V$

3.  $V = U + W$  and  $U \cap W = \{0\}$ .

There is also an *external direct sum*: let  $U_1, \dots, U_r$  be vector spaces over  $F$  and let

$$V = \{(u_1, \dots, u_r) : u_i \in U_i \text{ for } 1 \leq i \leq r\}$$

with componentwise addition and scalar multiplication (i.e.  $(u_1, \dots, u_r) + (u'_1, \dots, u'_r) = (u_1 + u'_1, \dots, u_r + u'_r)$  and  $\lambda(u_1, \dots, u_r) = (\lambda u_1, \dots, \lambda u_r)$ .) Then  $V$  is the external direct sum of  $U_1, \dots, U_r$  and  $V = U'_1 \oplus \dots \oplus U'_r$  where  $U'_i = \{(0, \dots, 0, u_i, 0, \dots, 0) : u_i \in U_i\}$  is the set of vectors concentrated in the  $i$ th component.

## 8. LINEAR TRANSFORMATIONS

A mapping  $\theta : V \longrightarrow W$  is a *linear transformation* (from  $V$  to  $W$ ) if for all  $v, v' \in V$  and  $\lambda \in F$

$$\theta(v + v') = \theta(v) + \theta(v')$$

$$\theta(\lambda v) = \lambda \theta(v).$$

As before we set

$$\ker \theta = \{v \in V : \theta(v) = 0\} \quad \text{and} \quad \text{im } \theta = \{w \in W : \theta(v) = w\}.$$

We call  $\theta$  an *endomorphism* if  $V = W$  and we write  $\text{End}(V)$  for the set of endomorphisms of  $V$ . We can add, subtract, multiply and scalar multiply endomorphisms: for  $\theta, \psi \in \text{End}(V)$ ,  $v \in V$  and  $\lambda \in F$

$$(\theta \pm \psi)(v) = \theta(v) \pm \psi(v)$$

$$(\theta\psi)(v) = \theta(\psi(v))$$

$$(\lambda\psi)(v) = \lambda(\psi(v)).$$

Since  $0_V$  (sending  $v$  to  $0$  for all  $v \in V$ ) and  $\text{id}_V$  (sending  $v$  to  $v$  for all  $v \in V$ ) belong to  $\text{End}(V)$  we see that  $\text{End}(V)$  is a ring (in fact an  $F$ -algebra).

A choice of basis  $\mathcal{B}$  for  $V$ , say  $(v_1, \dots, v_n)$ , allows us to associate to any  $\psi \in \text{End}(V)$  the *matrix of  $\psi$  relative to  $\mathcal{B}$* ,  $A = (a_{ij})_{1 \leq i, j \leq n}$  where by definition

$$\theta v_i = a_{1i}v_1 + \dots + a_{ni}v_n.$$

If we choose another basis  $\mathcal{B}'$  for  $V$ , say  $(v'_1, \dots, v'_n)$ , then the new matrix  $A' = (a'_{ij})$  we get is conjugate to the old matrix  $A$ . More precisely if we write  $v'_i = c_{1i}v_1 + \dots + c_{ni}v_n$  then we get a

new square matrix  $C = (c_{ij})$  and we have

$$A' = C^{-1}AC.$$

**Examples.** (a)  $\text{id}_V$  produces the  $n$ -by- $n$  identity matrix, no matter which basis  $\mathcal{B}$  we choose.

(b) Let  $V = \mathbb{R}^2$  and suppose  $\psi(x, y) = (x + 2y, y - x)$ . With the standard basis  $v_1 = (1, 0)^T$  and  $v_2 = (0, 1)^T$  we get the matrix

$$\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}.$$

With basis  $v_1 = (1, 1)^T$  and  $v_2 = (1, -1)^T$  we get

$$\frac{1}{2} \begin{pmatrix} 3 & -3 \\ 3 & 1 \end{pmatrix}.$$

$\theta$  is an *invertible linear transformation* if  $\theta$  is a bijection (this is equivalent to  $\ker \theta = \{0\}$  and  $\text{im } \theta = W$ ). The invertible endomorphisms of  $V$  form a group,  $GL(V)$ , under multiplication; it's called the *general linear group* of  $V$ . On choosing a basis we see this group is isomorphic to  $GL(n, F)$  where  $n = \dim V$ .

## 9. EIGENVALUES

Let  $V$  be an  $n$ -dimensional vector space over  $F$  and let  $\psi \in \text{End}(V)$ . We say  $\lambda \in F$  is an *eigenvalue* of  $\psi$  if there exists a non-zero vector  $v \in V$  such that  $\psi(v) = \lambda v$ . In this case we say that  $v$  is an *eigenvector*.

Thanks to the fundamental theorem of algebra every  $\psi$  has an eigenvalue if  $F = \mathbb{C}$ .

## 10. PROJECTIONS

Suppose that  $V = U \oplus W$ . We define a mapping by

$$\pi_U : V \longrightarrow V$$

by  $\pi_U(u + w) = u$  for all  $u \in U, w \in W$ . Then  $\pi_U \in \text{End}(V)$  (a very easy check – do it!) and  $\text{im } \pi_U = U, \ker \pi_U = W$  and  $\pi_U^2 = \pi_U$  (you should check all these claims).

Any endomorphism  $\pi$  of  $V$  such that  $\pi^2 = \pi$  is called a *projection*.

**Lemma.** *Suppose  $\pi$  is a projection of  $V$ . Then  $V = \text{im } \pi \oplus \ker \pi$ .*

*Proof.* We know that  $\text{im } \pi, \ker \pi$  are subspaces of  $V$ .

- $V = \text{im } \pi + \ker \pi$ : let  $v \in V$ . Then

$$v = \pi(v) + (v - \pi(v)).$$

The first term belongs to  $\text{im } \pi$  while the second term belongs to  $\ker \pi$  because

$$\pi(v - \pi(v)) = \pi(v) - \pi(\pi(v)) = \pi(v) - \pi^2(v) = \pi(v) - \pi(v) = 0.$$

- $\text{im } \pi \cap \ker \pi = \{0\}$ : suppose that  $v \in \text{im } \pi \cap \ker \pi$ . Then, following the definitions of  $\text{im}$  and  $\ker$ , we have  $v = \pi(w)$  for some  $w \in V$  and  $\pi(v) = 0$ . Thus  $\pi^2(w) = \pi(v) = 0$ . But  $v = \pi(w) = \pi^2(w) = 0$ , as required.  $\square$

NOW LET'S GO!