Chapter 2

Basic definitions, notations and examples

2.1 Preliminaries

2.1.1 Definition summary

There follows a list of definitions in the form
ALGEBRAIC SYSTEM $A = (A$ a set, $n-$ary operations), axioms.
(The selection of a special element $u \in A$, say, counts as a 0-ary operation.)
Extended examples are postponed to the relevant sections.

SEMIGROUP	$S = (S, \square)$, $\square$ a closed associative binary operation on S.
MONOID	$M = (M, \square, u)$, $(M, \square)$ a semigroup, $u \in M$ a *unit element* (i.e. $au = a = ua \ \ \forall a \in M$). Example: $(\mathbb{N}_0, +, 0)$.
GROUP	$G = (G, ., u)$, G a monoid, $\forall a \in G \exists a'$ such that $aa' = u = a'a$.
ABELIAN GROUP	$G = (G, +, 0)$, G a group, $a + b = b + a$.
RING	$R = (R, +, ., 1, 0)$, $(R, +, 0)$ an abelian group, $(R, ., 1)$ a monoid, $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.
DIVISION RING	D, D a ring, every non–zero element has a multiplicative inverse.
LOCAL RING	A, A a ring, sum of two nonunits is a nonunit (a a nonunit means there does not exist b such that $ab = ba = 1$). [1]
DOMAIN	K, K a ring, $0 \neq 1$, $mn = 0$ implies either $m = 0$ or $n = 0$.
INTEGRAL DOMAIN	K, K a ring, . commutative, $0 \neq 1$, $mn = 0$ implies either $m = 0$ or $n = 0$. (I.e. an integral domain is a commutative domain.)
PRINCIPAL IDEAL DOMAIN	K, K an integral domain, every ideal $J \subseteq K$ is principal (i.e. $\exists$ $a \in K$ such that $J = aK$).
FIELD	F, F an integral domain, every $a \neq 0$ has a multiplicative inverse.

Our other core definitions are, for S a semigroup, R a ring as above:

S–IDEAL J: $J \subset S$ and $rj, jr \in J$ for all $r \in S$, $j \in J$.
R–IDEAL J: $J \subset R$ and $rj, jr \in J$ for all $r \in R$, $j \in J$.

(LEFT) R–MODULE M: M an abelian group with map $R \times M \to M$ such that $r(x+y) = rx+ry$, $(r+s)x = rx+sx$, $(rs)x = r(sx)$, $1x = x$ ($r \in R$, $x, y \in M$).
Right modules defined similarly.

(LEFT) R–MODULE HOMOMORPHISM : Ψ from left R-module M to N is a map $\Psi : M \to N$ such that $\Psi(x+y) = \Psi(x) + \Psi(y)$, $\Psi(rx) = r\Psi(x)$ for $x, y \in M$ and $r \in R$.

(**2.1.1**) EXERCISE. $\mathbb{Z}$ is a ring. Form examples of as many of the other structures as possible from this one. (And some non-examples.)

In the following table k is a field and $\mathbb{H}$ is the ring of real quaternions (see §2.3.2).

	$DivR$	LR	ID	PID
$\mathbb{Z}$	×	×	√	√
$\mathbb{Z}[x]$	×	×	√	×
$k[x]$	×	×	√	√
$k[x,y]$	×	×	√	×
$\mathbb{H}$	√	√	×	×

(**2.1.2**) For more on semigroups see for example Howie [**?**].

2.1.2 Glossary

$GL(N)$ general linear group on $\mathbb{C}^N$
Λ set of integer partitions
Λ_n set of integer partitions of n
$O(N)$ orthogonal group on $\mathbb{C}^N$
P_S partitions of a set S
J_S pair partitions of a set S
$P(S)$ power set (lattice) of a set S

2.2 Elementary set theory notations and constructions

As in Green [22], let

$$\underline{n} := \{1, 2, .., n\}$$

Similarly here $\underline{n'} := \{1', 2', .., n'\}$ (and so on).

(**2.2.1**) For S a set, let $P(S)$ be the lattice of subsets of S. For S, T sets, let $U_{S,T}$ be the set of relations on S to T. That is,

$$U_{S,T} = P(S \times T).$$

Set $U_S = U_{S,S}$, and

$$T^S := \hom(S, T) \subset U_{S,T}$$

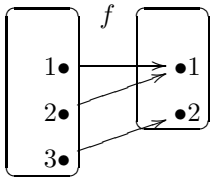
For example

$$\underline{2}^{\underline{2}} = \{\{(1,1),(2,1)\},\{(1,1),(2,2)\},\{(1,2),(2,1)\},\{(1,2),(2,2)\}\}$$

(**2.2.2**) It will be useful to have in mind the *mapping diagram* realisation of such functions. For example

$$f = \{(1,1),(2,1),(3,2)\} \in \underline{2}^{\underline{3}}$$

is



(**2.2.3**) If T, S finite it will be clear that any total order on each of T and S puts T^S in bijection with $\underline{|T|}^{\underline{|S|}}$. We may represent the elements of T^S as T-ordered lists of elements from S. Thus

$$\underline{2}^{\underline{2}} = \{11, 12, 21, 22\}$$

(for example $22(1) = 2$, since the first entry in 22 is the image of 1).

(**2.2.4**) A *composition* of n is a finite sequence λ in $\mathbb{N}_0$ that sums to n. We write $\lambda \vDash n$.

We define the *shape* of an element f of $\underline{m}^{\underline{n}}$ as the composition of n given by

$$\lambda(f)_i = |f^{-1}(i)|$$

Example: for $111432525 \in \underline{6}^{\underline{9}}$ we have $\lambda(111432525) = (3,2,1,1,2,0)$.

If $\lambda \vDash n$ we write $|\lambda| = n$.

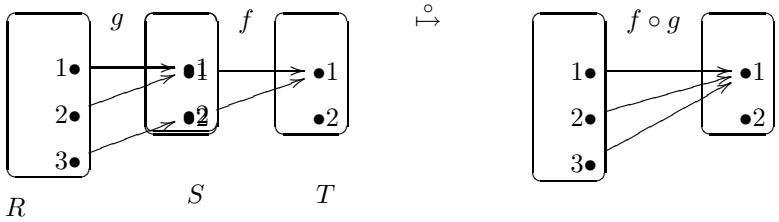
(**2.2.5**) Of course, composition of functions defines a map

$$\hom(S,T) \times \hom(R,S) \quad \to \quad \hom(R,T) \tag{2.1}$$

$$(f,g) \mapsto f \circ g \tag{2.2}$$

where as usual $(f \circ g)(x) = f(g(x))$. For example $11 \circ 22 = 11$ (since $11(22(1)) = 11(2) = 1$; and so on).

The *mapping diagram realisation* of composition is to first juxtapose the two functions so that the two instances of the set S coincide, then define a direct path from R to T for each path of length 2 so formed:



(2.3)

(**2.2.6**) If the image $f(S)$ of a map $f : S \to T$ is of finite order we shall say that f has order $|f(S)|$ (otherwise it has infinite order). We have the *bottleneck principle*

$$|(f \circ g)(R)| \ \leq \ \min(|f(S)|, |g(R)|)$$

(**2.2.7**) PROPOSITION. *(i) For S a set, $S^S = \hom(S, S)$ is a monoid under composition of functions. (ii) For each $d \in \mathbb{N}$ then set $\{f \in S^S \mid |f(S)| < d\}$ is an ideal (hence a sub-semigroup) of S^S.*

2.2.1 Set partitions

(**2.2.8**) Let E_S be the set of equivalence relations on set S, and let P_S be the set of partitions of S. Note the natural bijection

$$E_S \leftrightarrow P_S.$$

We have $E_S \subset U_S$. For $\rho \in U_S$ let $\bar{\rho} \in U_S$ be the smallest transitive relation containing ρ — this is called the *transitive closure* of ρ.

(**2.2.9**) For a, b equivalence relations on any two finite sets let ab be the transitive closure of $a \cup b$ (an equivalence relation on the union of the two finite sets).

(**2.2.10**) Let $J_S \subset P_S$ be the set of pair-partitions of S. Let $P_{n,m} = P_{\underline{n} \cup \underline{m'}}$ and

$$J_{n,m} = J_{\underline{n} \cup \underline{m'}} \ \subset P_{n,m}$$

(**2.2.11**) For $a \in P_{n,m}$ let a' be the partition of $\underline{n'} \cup \underline{m''}$ obtained by adding a prime to each object in every part. We may define a map

$$\circ : P_{l,m} \times P_{m,n} \to P_{l,n}$$

as follows. For $a \in P_{l,m}$, $b \in P_{m,n}$ partitions (and hence equivalence relations) note that ab' is an equivalence relation on $\underline{l} \cup \underline{m'} \cup \underline{n''}$. Restricting to $\underline{l} \cup \underline{n''}$ this equivalence relation is again a partition, call it $r(ab')$ (indeed if a, b are pair-partitions then so is $r(ab')$). For $x \in \underline{l} \cup \underline{n''}$ let $u(x) \in \underline{l} \cup \underline{n'}$ be the image under the action of replacing double primes with single. Let $a \circ b = u(r(ab')) \in P_{l,n}$ be the image under the obvious application of this map.

Set $P_n = P_{n,n}$ and $J_n = J_{n,n}$.

(**2.2.12**) PROPOSITION. *For each $n \in \mathbb{N}$ the map $\circ : (a, b) \mapsto u(r(ab'))$ defines an associative unital product on P_n, making it a monoid. The construction also restricts to make J_n a monoid.*

2.3 Initial examples in representation theory

2.3.1 The monoid $\hom(\underline{2}, \underline{2})$

Two matrices A, B are conformable to a product AB if (i) the number of rows of A equals the number of columns of B; (ii) they have entries in the same ring R. By convention, if R is a

K-algebra, then a matrix over K is considered a matrix over R by the homomorphism ψ (see (1.1.11)), taking elements of K to scalar multiples of 1_R.

(**2.3.1**) Consider the monoid $M = \underline{2}^{\underline{2}}$, and the free $\mathbb{Z}$-module $\mathbb{Z}M$ with basis M. This is a $\mathbb{Z}$-algebra (by virtue of the monoid multiplication). Totally ordering this (or any other) basis we may encode $x \in \mathbb{Z}M$ by

$$x = \begin{pmatrix} x_{11} & x_{12} & x_{21} & x_{22} \end{pmatrix} \begin{pmatrix} 11 \\ 12 \\ 21 \\ 22 \end{pmatrix}$$

(here we have used the shorthand for monoid elements give in (2.2.3)). This organisational scheme yields a generalisation of the regular representation construction mentioned in the Introduction. Indeed there is both a left and a right regular construction. We shall consider both.

(**2.3.2**) Firstly consider the encoding of multiplication by

$$\begin{pmatrix} 11 \\ 12 \\ 21 \\ 22 \end{pmatrix} * (11,\ 12,\ 21,\ 22) \ = \ \begin{pmatrix} 11\circ 11 & 11\circ 12 & 11\circ 21 & 11\circ 22 \\ 12\circ 11 & 12\circ 12 & 12\circ 21 & 12\circ 22 \\ 21\circ 11 & 21\circ 12 & 21\circ 21 & 21\circ 22 \\ 22\circ 11 & 22\circ 12 & 22\circ 21 & 22\circ 22 \end{pmatrix}$$

(we put the $*$ in on the left, to emphasise that this is matrix multiplication over a non-commutative ring) and hence

$$\begin{pmatrix} 11 \\ 12 \\ 21 \\ 22 \end{pmatrix} * m = \begin{pmatrix} 11\circ m \\ 12\circ m \\ 21\circ m \\ 22\circ m \end{pmatrix} \qquad m \in \underline{2}^{\underline{2}}$$

That is

$$\begin{pmatrix} 11 \\ 12 \\ 21 \\ 22 \end{pmatrix} * 11 = \begin{pmatrix} 11\circ 11 \\ 12\circ 11 \\ 21\circ 11 \\ 22\circ 11 \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \\ 22 \\ 22 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 11 \\ 12 \\ 21 \\ 22 \end{pmatrix}$$

$$\begin{pmatrix} 11 \\ 12 \\ 21 \\ 22 \end{pmatrix} * 12 = \begin{pmatrix} 11\circ 12 \\ 12\circ 12 \\ 21\circ 12 \\ 22\circ 12 \end{pmatrix} = \begin{pmatrix} 11 \\ 12 \\ 21 \\ 22 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 11 \\ 12 \\ 21 \\ 22 \end{pmatrix}$$

and so on. By this (general) construction we have a map $R_r : M \to M_4(\mathbb{Z})$

$$R_r(11) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ R_r(12) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ R_r(21) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ R_r(22) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

These matrices give a representation.

(**2.3.3**) We do not yet have the tools for a systematic analysis of representations of a monoid, but a couple of observations are in order. This representation is, up to a reordering of the basis, in the

form of (1.10):

$$R_{r'}(11)=\left(\begin{array}{cc|cc} 0&0&0&1\\ 0&0&1&0\\ \hline 0&0&1&0\\ 0&0&0&1 \end{array}\right),\ R_{r'}(21)=\left(\begin{array}{cc|cc} 0&1&0&0\\ 1&0&0&0\\ \hline 0&0&1&0\\ 0&0&0&1 \end{array}\right)$$

This corresponds to the fact that the free $\mathbb{Z}$-submodule of $\mathbb{Z}M$ with basis $\{11, 22\}$ is also invariant under this action of M from the right.

This representation does not have a manifest direct sum decomposition, but we can ask if such a decomposition can be manifested by basis change. However the possibilities for basis change beyond reordering depend on the choice of ring.

(**2.3.4**) *Provided we pass to a ring in which 2 is invertible*, another basis is $\{-11 + 12 + 21 - 22, 11, 11 - 22, 12 - 21\}$. (Questions: Where did this come from?! How did the restriction arise?) Using this basis we get another representation:

$$R'_r(11)=\begin{pmatrix} 0&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&1&0 \end{pmatrix},\ R'_r(12)=\begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix},\ R'_r(21)=\begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&-1 \end{pmatrix},\ R'_r(22)=\begin{pmatrix} 0&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&-1&0 \end{pmatrix}$$

In other words there is a direct sum decomposition:

$$R' = R_1 \oplus R_{1'} \oplus R_2$$

Note that R_2 is not irreducible, but it is not amenable to a direct sum decomposition in any basis over any ring. It is, however, of the form in Equation (1.10). In this sense it 'contains' two one-dimensional (hence irreducible) representations:

$$R_2 = R_{1'} \dot{+} R_{1''}$$

(**2.3.5**) Alternatively, we may encode multiplication by

$$m * \begin{pmatrix} 11\\12\\21\\22 \end{pmatrix} = \begin{pmatrix} m\circ 11\\ m\circ 12\\ m\circ 21\\ m\circ 22 \end{pmatrix} \qquad m \in \underline{2^{\underline{2}}}$$

That is

$$11 * \begin{pmatrix} 11\\12\\21\\22 \end{pmatrix} = \begin{pmatrix} 11*11\\11*12\\11*21\\11*22 \end{pmatrix} = \begin{pmatrix} 11\\11\\11\\11 \end{pmatrix} = \begin{pmatrix} 1&0&0&0\\1&0&0&0\\1&0&0&0\\1&0&0&0 \end{pmatrix}\begin{pmatrix} 11\\12\\21\\22 \end{pmatrix}$$

$$12 * \begin{pmatrix} 11\\12\\21\\22 \end{pmatrix} = \begin{pmatrix} 12*11\\12*12\\12*21\\12*22 \end{pmatrix} = \begin{pmatrix} 11\\12\\21\\22 \end{pmatrix} = \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}\begin{pmatrix} 11\\12\\21\\22 \end{pmatrix}$$

and so on. By this construction we have another map $R^r : M \to M_4(\mathbb{Z})$

$$R^r(11)=\begin{pmatrix} 1&0&0&0\\1&0&0&0\\1&0&0&0\\1&0&0&0 \end{pmatrix},\ R^r(12)=\begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix},\ R^r(21)=\begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0 \end{pmatrix},\ R^r(22)=\begin{pmatrix} 0&0&0&1\\0&0&0&1\\0&0&0&1\\0&0&0&1 \end{pmatrix}$$

These matrices give an antirepresentation. That is

$$R^r(a)R^r(b) = R^r(ba)$$

This becomes a representation once we compose with the matrix transpose map. Note however that there is no similarity transformation between R_r and $(R^r)^t$ (the map from the algebra to the ring defined for each representation by matrix trace is not changed by similarity, and differs between the two), so they are not equivalent representations.

Quite generally, if a representation can be expressed in the form of Equation (1.10):

$$\rho_{12}(g) = \begin{pmatrix} \rho_1(g) & V(g) \\ 0 & \rho_2(g) \end{pmatrix} \tag{2.4}$$

then

$$\mathrm{Tr}(\rho_{12}(g)) = \mathrm{Tr}(\rho_1(g)) + \mathrm{Tr}(\rho_2(g)) \qquad (\text{any } g)$$

If we assume that $(R^r)^t$ is a (not necessarily direct) sum of the irreducible representations we have already seen, then we can deduce immediately that this sum contains two copies of $R_{1''}$, since $\mathrm{Tr}(R_{1''}(21)) = -1$ and $\mathrm{Tr}(R_1(21)) = \mathrm{Tr}(R_{1'}(21)) = 1$, and so this is the only way to get $\mathrm{Tr}(R^r(21)) = 0$. Considering $\mathrm{Tr}(R^r(11)) = 1$ we then see that

$$(R^r)^t = R_1 + R_{1'} + R_{1''} + R_{1''}$$

(under the stated assumption). In other words $(R^r)^t$ does not even have quite the same irreducible summands as R_r — at least the multiplicities are different.

That was Too much linear algebra! How can we be more slick? We shall shortly begin to address this question.

(**2.3.6**) For K a given commutative ring, and M a left K-module write $End(M)$ for the set of linear transformations of M. For any subset $S \in End(M)$ we define $End_S(M)$ as the subset of linear transformations that commute with every element of S.

(**2.3.7**) Exercise. Consider R'_r as a subset of $End(\mathbb{Z}\underline{2}^{\underline{2}})$. What is $End_{R'}(\mathbb{Z}\underline{2}^{\underline{2}})$?

2.3.2 quaternions

Set

$$\mathbf{i} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \mathbf{j} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

We define $\mathbb{H}$ as the subring of $M_4(\mathbb{R})$ generated as an $\mathbb{R}$-algebra by these matrices (as an $\mathbb{R}$-vector space it is spanned by $\{\mathbf{i}, \mathbf{j}, \mathbf{ii}, \mathbf{ij}\}$). This is a noncommutative division ring.

2.4 Basic tools: topology

(**2.4.1**) A *sigma-algebra* over a set S is a subset Σ of the power set $P(S)$ which includes S and $\emptyset$ and is closed under countable unions, and complementation in S.

Any subset S' of $P(S)$ defines a sigma-algebra — the smallest sigma-algebra generated by S'. For example $\{\{1\}\} \subset P(\{1,2,3\})$ generates $\Sigma = \{\emptyset, \{1\}, \{2,3\}, \{1,2,3\}\}$.

(**2.4.2**) A *topological space* is a set S together with a subset T of the power set $P(S)$ which includes S and $\emptyset$ and is closed under unions and finite intersections.

The set T is called a *topology* on S. The elements of T are called the *open sets* of this topology. A set is *closed* if it is the complement in S of an open set. A function between topological spaces is *continuous* if the inverse image of every open set is open. Two spaces are *homeomorphic* if there is a bijection between them, continuous in both directions.

The restriction of T to $S' \subset S$ is a topology on S', called the *subspace topology.*

A subset S' of a topological space (S,T) is *irreducible* if $S' = S_1 \cup S_2$ with S_1 closed implies S_2 not closed.

(**2.4.3**) Let k be a field. A polynomial $p \in k[x_1, ..., x_r]$ determines a map from k^r to k by evaluation. For $P = \{p_i\}_i \subset k[x_1, ..., x_r]$ define

$$Z(\{p_i\}_i) = \{x \in k^r \ : \ p_i(x) = 0 \ \forall \ i\}$$

An *affine algebraic set* is any such set, in case k algebraically closed. An *affine variety* is any such set, that cannot be written as the union of two proper such subsets. (See for example, Hartshorne [23, I.1].)

The set of affine varieties in k^r satisfy the axioms for closed sets in a topology. This is called the *Zariski topology.* The Zariski topology on an affine variety is simply the corresponding subspace topology.

The set $I(P) \in k[x_1, ..., x_r]$ of all functions vanishing on $Z(P)$ is the ideal in $k[x_1, ..., x_r]$ generated by P. We call

$$k_P = k[x_1, ..., x_r]/I(P)$$

the *coordinate ring* of $Z(P)$.

(**2.4.4**) Let Z be an affine variety in k^r and $f : Z \to k$. We say f is *regular* at $z \in Z$ if there is an open set containing z, and $p_1, p_2 \in k[x_1, ..., x_r]$, such that f agrees with p_1/p_2 on this set.

(**2.4.5**) A morphism of varieties is a Zariski continuous map $f : Z \to Z'$ such that if V is open in Z' and $g : V \to k$ is regular then $g \circ f : f^{-1}(V) \to k$ is regular.

(**2.4.6**) Given affine varieties X, Y then $X \times Y$ may be made in to an algebraic variety in the obvious way.

(**2.4.7**) An *algebraic group* G is a group that is an affine variety such that inversion is a morphism of algebraic varieties; and multiplication is a morphism of algebraic varieties from $G \times G$ to G.