A first Course in Abstract Algebra

Notes

Brendan Matthews

2026-02-05

1. What is this stuff used for

Topic	Is It used	What Part	Is it Physics
Combinatorics	yes	Group Actions: Burnside	no
Statistics	sparsely	Renormalisation group, Haar Measure	yes, dunno
Statistics	sparsely	Galois Fields: Fractional factorial design	no
Math			
Math			
Math			
Math			

2. Group tables are dumb and playing sudoku doesn't guarantee associativity.

$\circ$	0	1	2	3	4
0	0	1	2	3	4
1	1	4	0	2	3
2	2	3	4	1	0
3	3	0	1	4	2
4	4	2	3	0	1

$D_3 = S_3$ but $D_n \neq S_n, \qquad n \geq 4$

Moonshine Theory

A relation b/w sets A, B is $R \subset A \times B$ —
A relation on A is $R \subset A \times A$.

ex. The graph of a function is the subset

$$\{(x, f(x)) : x \in \mathrm{dom}(f)\} \subset \mathrm{dom}(f) \times \mathrm{codom}(f).$$

The graph of a function $f: \mathbb{R} \to \mathbb{R}$ is a relation on $\mathbb{R}$.

A function $\phi: X \to Y$ is a relation b/w X and Y such that (for each $x \in X$, $\exists!\ y \in Y$ so that $(x, y) \in \phi \subset X \times Y$ or equivalently, $\phi(x) = y$.

The range of ϕ is $\phi(X) = \{\phi(x) : x \in X\}$.

ex. $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is a map from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$.

A partition of S is a collection of nonempty disjoint subsets with union S. These define equivalence relations on S

$x \sim_{eq} x$, $x \sim_{eq} y$ and $y \sim_{eq} z \Rightarrow x \sim_{eq} z$,

$x \sim_{eq} y \Rightarrow y \sim_{eq} x$.

17. claim $|P(A)| = 2^{|A|}$

well $|A| = n$ finite and

$|P(A)| =$ |Subsets with 0 elements| + --- + |Subsets with n elements|

$= {}_nC_0 + \cdots + {}_nC_n$

$= (1+1)^n$ by binomial theorem

$= 2^n$.

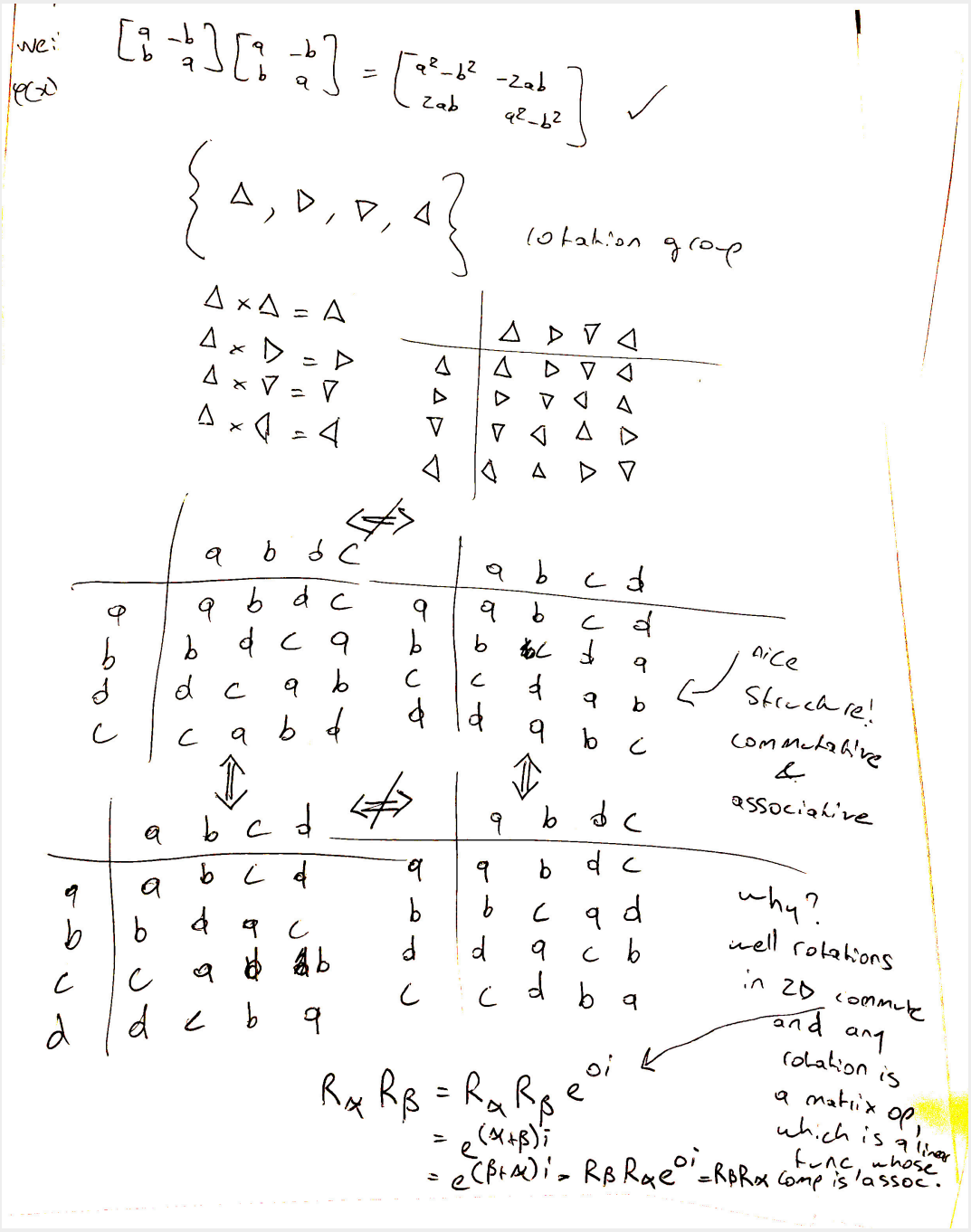
18. Map the function $f \in B^A$ to the subset of A, $\{a \in A : f(a) = 1\}$. Claim this is onto. Pick any subset of A, $\{a_1, \ldots, a_m\}$ with $a_i \in A$, $m \leq n$. Then $f: A \to B$,

$$f(a) = \begin{cases} 1, & a \in \{a_1, \ldots, a_m\} \\ 0 & \text{otherwise} \end{cases}$$

is in B^A and maps onto $\{a_1, \ldots, a_m\}$.

Can't be bothered with 1:1.

A binary operation is a map $* : S \times S \to S$ and a subset H of S is closed under $*$ if the obvious thing happens. We say that $*$ is induced on H. There are n^{n^2} binary ops on a set of size n and $n^{\sum_n i} = n^{\frac{n(n+1)}{2}}$ commutative ones. We can see this by labelling the elements by numbers one through n and considering the number of partners for each element. If there is no need for the operation to commute, then there are n new pairs we can form for each of the n elements, by pairing them with another element $1, \ldots, n$. Otherwise, the first element can form n new pairs, $1 * 1, \ldots, 1 * n$. Then $2 * 1 = 1 * 2$, so there are $n - 1$ new pairs that 2 can form with $2, \ldots, n$. Note that for finite A, B, number of maps from A to B is $|B|^{|A|}$.



Commutative subsets $H = \{a \in S : xa = ax \ \forall x \in S\}$ of associative $(S, *)$ are closed.

Proof

$x*(a*b) = (x*a)*b$ assoc

$= (a*x)*b$ com of a

$= a*(x*b)$ assoc of everything

$= a*(b*x)$ com of b

$= (a*b)*x$ assoc of everything

$\Rightarrow (a*b) \in H$

idempotent subsets of assoc & com S, $H = \{a \in S : a*a = a\}$ are closed

Proof

$(a*b)*(a*b) = (a*b)*(b*a)$

$= ab*(b*a)$

$= (ab*b)*a$

$= ((a*b)*b)*a$

$= (a*(b*b))*a$

$= (a*b)*a$

$= (b*a)*a$

$= b*(a*a)$

$= b*a$

$= (a*b)$

4. isomorphisms

Two binary algebraic structures $(R, *), (S, +)$ are isomorphic, $R \simeq S$, if for each $x, y \in R$ with $x * y = z$, we have corresponding $x', y', z' \in S$ so that $x' + y' = z'$. That is, there exists a bijection $\phi : R \to S$ such that for all $x, y \in R$ with $x * y = z$,

$$\phi(x * y) = \phi(x) + \phi(y) = x' + y' = z' = \phi(z).$$

Each point in S is mapped to by exactly one point in R. Isomorphism is an equivalence relation.

Proof: $S \simeq S$ by identity map. If $R \simeq S$, then there exists $\phi : R \to S$, bijective and a homomorphism. So the inverse exists. The inverse is a homomorphism by injectivity of ϕ:

$$\phi(\phi^{-1}(s_1) * \phi^{-1}(s_2)) \underset{\text{homomorph}}{=} \phi(\phi^{-1}(s_1)) + \phi(\phi^{-1}(s_2)) = s_1 + s_2 = \phi(\phi^{-1}(s_1 + s_2)).$$

Transitivity is easy just compose the isos. ■

Theorem 4.1: There is at most one identity element of an algebraic structure. Suppose e, f are left and right identities. Then $e = e * f = f$.

Theorem 4.2: Suppose there is an **onto** homomorphism $\phi : (R, +) \to (S, *)$ and an identity $e \in R$. Then S has an identity, and it is $\phi(e)$. You should be able to prove this instantly.

In Theorem 4.3, we assume S has an identity.

Theorem 4.3: Suppose ϕ is an injection from $(R, *)$ to $(S, +)$. Then if ϕ is injective and there exists $x \in R$ such that $\phi(x) = e_S$, then x is the identity of R. In particular, if ϕ is an isomorphism, then the preimage of the identity of S is the identity of R.

Theorem 4.4: Suppose S is a **group** and R, S have identities e_R, e_S. If there is a homomorphism $\phi : (R, +) \to (S, *)$, then $\phi(e_R) = e_S$.

Proof:

$$\phi(e_R) = \phi(e_R + e_R) = \phi(e_R) * \phi(e_R)$$

and so

$$e_S = \phi(e_R) * \phi(e_R)^{-1} = \phi(e_R) * e_S = \phi(e_R).$$

■

Theorem 4.5: Let X be monoid. If there exists a left inverse l of $x \in X$, then $l = x^{-1}$ and is a right inverse also. The contrapositive is that if x is not invertible then it has no left inverse.

Proof:

$$x^{-1} = e * x^{-1} = (l * x) * x^{-1} = l * (x * x^{-1}) = l * e = l$$

■

4.1. Non Isomorphism Examples

The function $\phi : (M_2(R), \times_M) \to (R, \times), \quad \phi(A) = \det(A)$ is not an isomorphism (in fact, no such isomorphism exists).

Proof: It is a homomorphism, $\det(AB) = \det(A)\det(B)$. But it isn't injective because matrix multiplication isn't commutative. Take

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

then

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \text{ and their determinants are both } 1.$$

■

Another example that fails injectivity is the map under addition from functions with derivatives to their derivatives. Being a binary operation (or even a function at all) can fail with integrals even if everything else works.

4.2. Disproving stuff using properties that're preserved under isomorphisms

Lemma 4.2.1: There is no isomorphism from $(M_2(\mathbb{R}), \times)$ to $(\mathbb{R}, \times)$.

Proof: Suppose that $\phi : M_2(\mathbb{R}) \to \mathbb{R}$ is an onto homomorphism. Let $\phi \circ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = Q_0$. If $Q_0 = 0$, then either

$$\phi \circ \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} = 0 = Q_0$$

and ϕ is not injective, or

$$\phi \circ \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} = Q \neq 0$$

but then since $Q \neq 0$, $\exists Q^{-1} \in \mathbb{R}$ so that $QQ^{-1} = 1$. Since ϕ is onto, there is some matrix M such that $\phi(M) = Q^{-1}$. Then $\phi\left(\begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} M\right) = \phi\left(M \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix}\right) = \phi(M)\phi \circ \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} = Q^{-1}Q = 1 = \phi(\mathrm{Id}_2)$ by Theorem 4.4. Since $\begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix}$ is not invertible, either $M \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} \neq \mathrm{Id}_2$ or $\begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} M \neq \mathrm{Id}_2$[1] so ϕ is not injective. Otherwise, $Q_0 \neq 0$ and we repeat the argument with $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$; whatever the case, ϕ is not injective. ■

We know the identity is preserved. So $\phi(f)(x) = xf(x)$ is not an isomorphism across $F = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is smooth}\}$ under multiplication, $\phi(\iota)(2) = 4 \neq \iota(2)$, so $\phi(\iota) \neq \iota$, where $\iota : \mathbb{R} \to \mathbb{R}$ is given by $\iota(x) = x$.

[1] Square matrices can't have a left or right inverse in isolation. They are linear maps on finite vector spaces, so one to one iff onto by rank nullity.

$(a*b)\circ\phi = a\circ\phi + b\circ\phi$

binary op done first

function evaluation second

$= (\phi\circ a) + (\phi\circ b)$

$\cong \phi\circ(a+b)$

function evaluation done first

binary op done second

24. No; e_L, e_R need not be unique. Very obviously need left and right handedness in proof.
C.E. $a*a=a$, $a*b=b$, $b*a=a$, $b*b=b$.

25. No. $e_L * e_R$ gives $e_L = e_R$, we cannot have left and right IE's that aren't equal.

29. $a*b = \phi(x)*\phi(y) = \phi(x+y) = \phi(y+x)$
$= \phi(y)*\phi(x)$
$= b*a$

30. $a*(b*c) = \phi(x)*(\phi(y)*\phi(z))$
$= \phi(x)*\phi(y+z)$
$= \phi(x+(y+z))$
$= \phi((x+y)+z) = \phi(x+y)*\phi(z)$
$= (a*b)*c$

31. $x*x=c$ has soln $\forall c \in S$.
Pick $z \in R$. Then $\phi(z) \in S$, so $x*x = \phi(z)$
$x = \phi(a)$ for some a, $\phi(a)*\phi(a) = \phi(z)$
$\phi(a+a) = \phi(z)$
$a+a = z$
$2a = z$
So $\phi^{-1}(\phi(2a)) = \phi^{-1}(\phi(z)) \leadsto 2a = z$.

32. If $b*b=b$ for some b, $\phi(y)*\phi(y) = \phi(y)$, $\phi(y+y) = \phi(y)$