A first Course in Abstract Algebra

Notes

Brendan Matthews

2026-02-06

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

$= 2^n$.

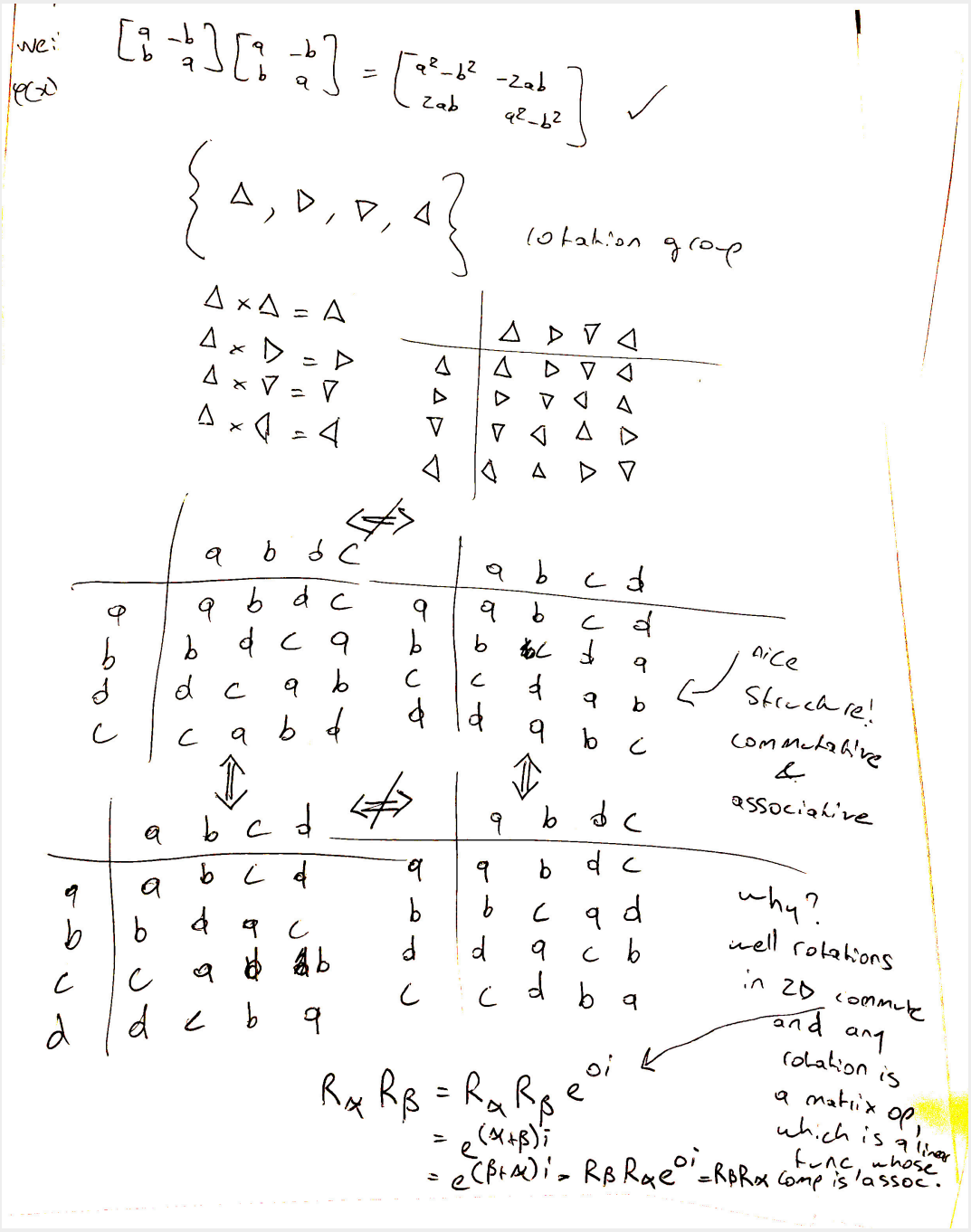
18. Map the function $f \in B^A$ to the subset of A, $\{a \in A : f(a) = 1\}$. Claim this is onto. Pick any subset of A, $\{a_1, \ldots, a_m\}$ with $a_i \in A$, $m \leq n$. Then $f: A \to B$,

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

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, $\phi(y)*\phi(y) = \phi(y)$, $\phi(y+y) = \phi(y)$

	a	b
a	a	a
b	a	a

$\cong$

	a	b
a	b	b
b	b	b

Class 1

identity isomorphism is use for counting

$\phi(a)=a$
$\phi(b)=b$
or
$\phi(a)=b$
$\phi(b)=a$

if $\phi(a)=\phi(b)$ then we have $a=b$ can't happen.

~~we know~~ $\phi(a)=a$
$\phi(b)=a$.

we effectively only care about the case $\phi(a)=b, \phi(b)=a$.

they are determined because of the loner property

$\phi(a\times a)=b\times b$.

	a	b
a	a	b
b	b	b

$\cong$

	a	b
a	a	a
b	a	b

Class 2

	a	b
a	b	b
b	a	b

$\cong$

	a	b
a	a	b
b	a	a

Class 3

	a	b
a	b	b
b	b	a

$\cong$

	a	b
a	b	a
b	a	a

Class 4

	a	b
a	b	a
b	b	b

$\cong$

	a	b
a	a	a
b	b	a

Class 5

	a	b
a	a	b
b	b	a

Class 6

isomorphic to themselves under non-Id isomorphism

	a	b
a	a	b
b	b	a

$\cong$

	a	b
a	b	a
b	a	b

Class 10

	a	b
a	b	b
b	a	a

Class 7

	a	b
a	a	b
b	a	b

Class 8

	a	b
a	b	a
b	b	a

Class 9

loners

→ count the loners to determine # isos!!!

loners = 4 since $a\times a$, $a\times b$ determine $b\times b$ and $b\times a$ if $\phi(a)=b$, $\phi(b)=a$

isos = $4+\frac{16-4}{2}=10$!!!

5. Groups

Here are some examples of groups:

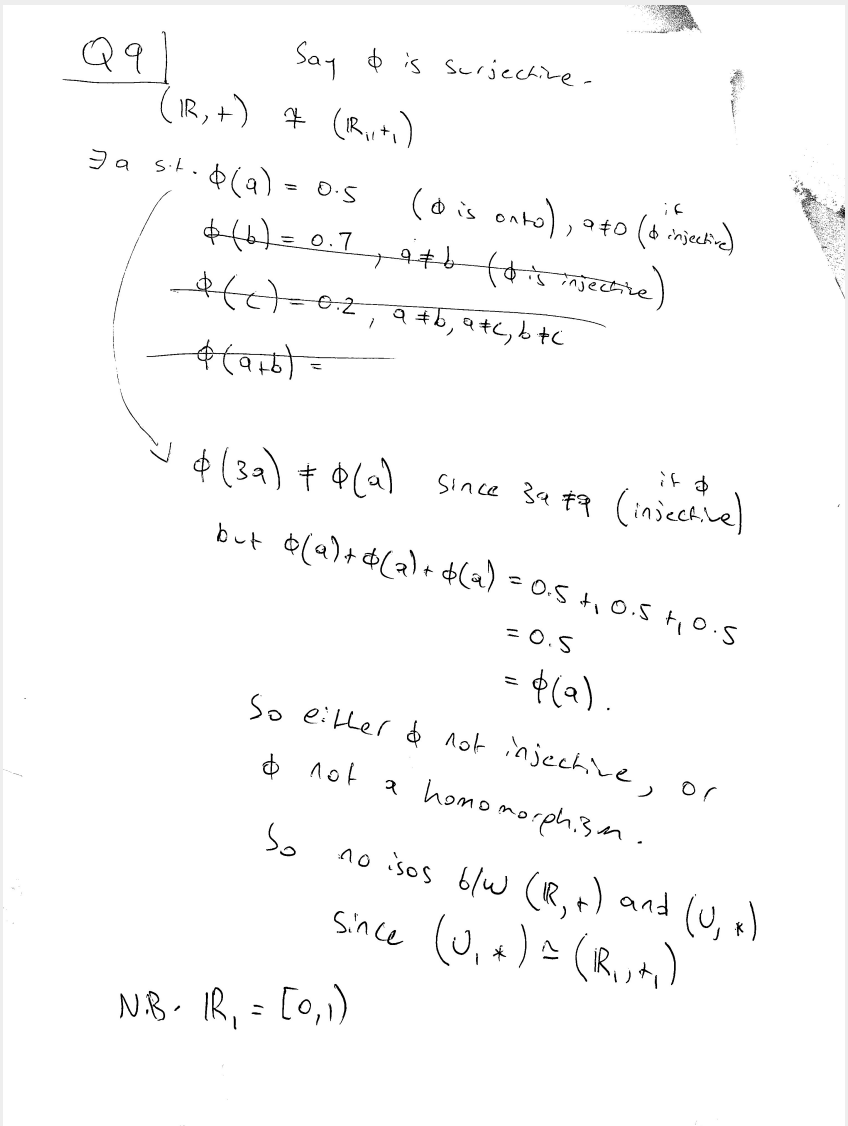
$$(U, *) \text{ with } U = \{z \in \mathbb{C} : |z| = 1\}, \text{and } (U_n, *) \text{ with } U_n = \{z \in \mathbb{C} : z^n = 1\}$$

The invertible n by n matrices and the invertible linear maps on $\mathbb{R}^n$:

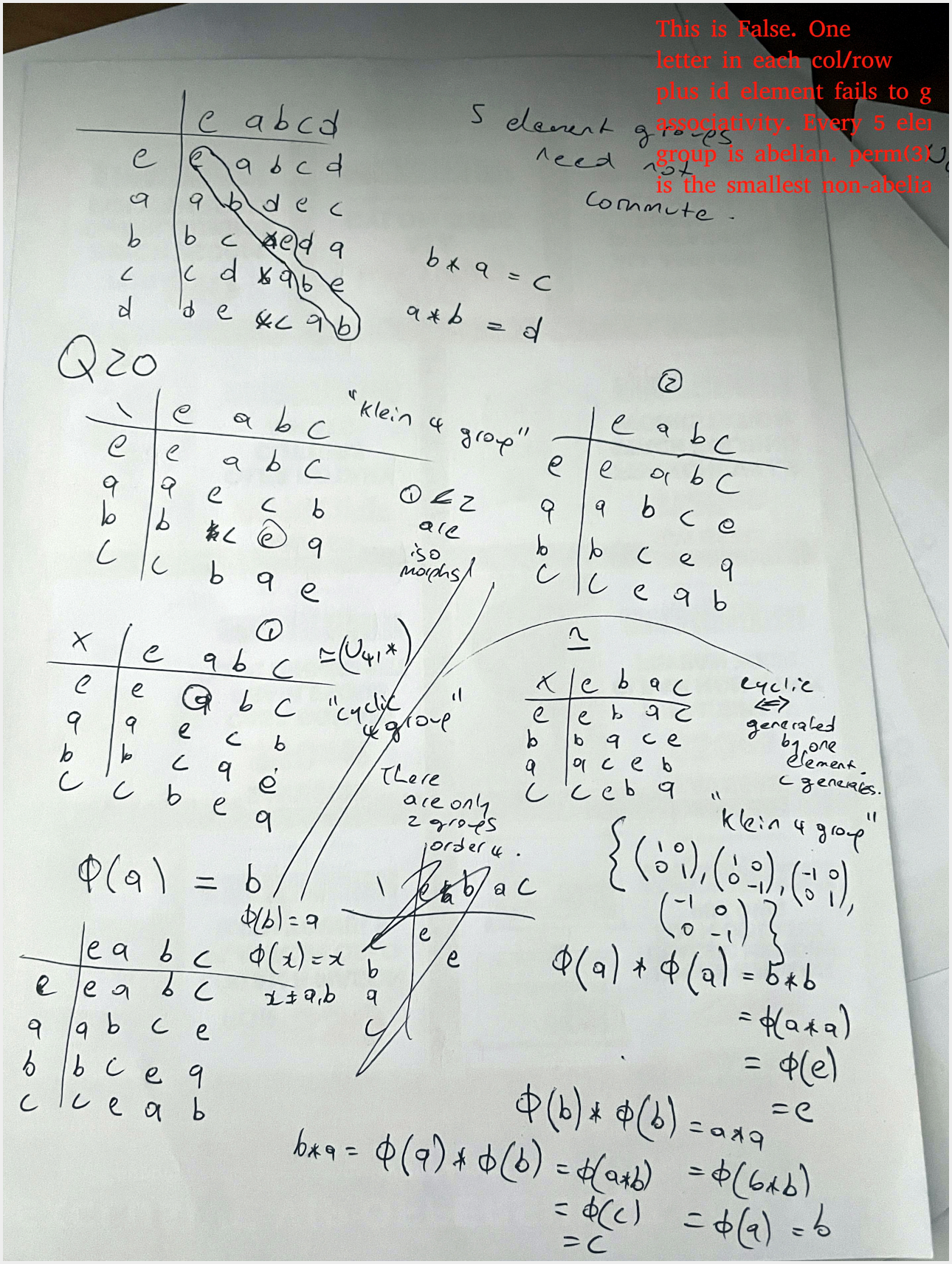
$$\mathrm{GL}_n(\mathbb{R}) \simeq \mathrm{GL}(\mathbb{R}^n)$$

To get an isomorphism, map an invertible linear function $T : \mathbb{R}^n \to \mathbb{R}^n$ to a matrix using its action on the standard basis. Left inverses and identities plus associative is enough to define a group. Identity is a right identity:

$$\begin{aligned} x + e_L &= e_L + (x + e_L) \\ &= (x_{\mathrm{LL}} + x_L) + (x + (x_L + x)) \\ &= x_{\mathrm{LL}} + (x_L + x) + (x_L + x) \\ &= x_{\mathrm{LL}} + e_L + (x_L + x) \\ &= (x_{\mathrm{LL}} + x_L) + x \\ &= e_L + x \\ &= x. \end{aligned}$$



It's easy to do the same argument with $\phi(e^{i\pi}) = a > 0$ if you'd like to prove it directly with U. For $(U, *) \not\cong (\mathbb{R}^*, *)$, supposing ϕ is a monomorphism, $a = \phi(e^{i\pi})$ is not one by Theorem 4.4 then we would have $a^2 = a * a = \phi(e^{i\pi}) * \phi(e^{i\pi}) = \phi(e^{2i\pi}) = \phi(1) = 1$ but no element of $\mathbb{R}^*$ has order two, contradiction.

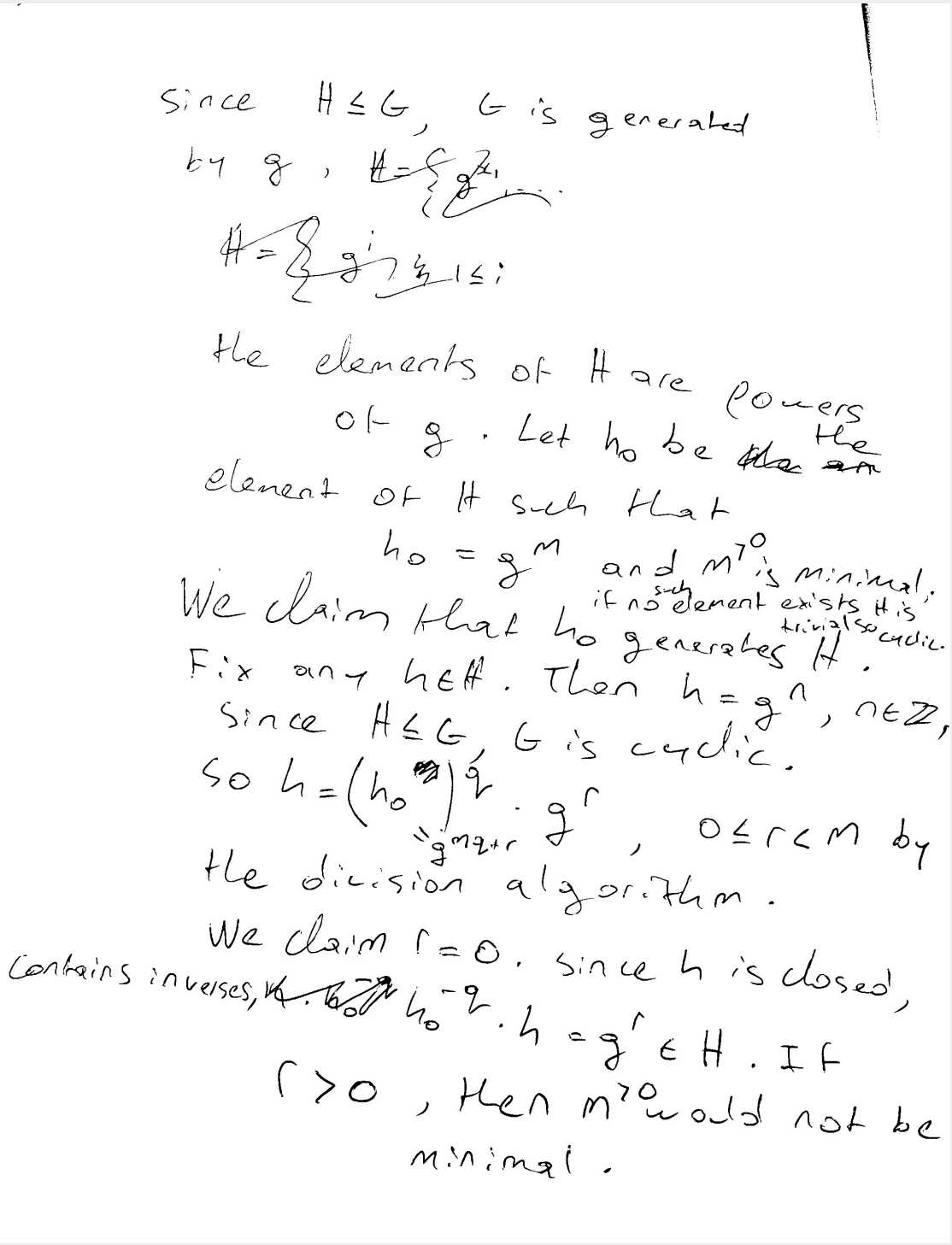


6. Subgroups

Subgroups are closed, contain identity and inverses. An element a generates G if the cyclic subgroup $\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = G$. We say that G is cyclic if there is some element that generates it. So obviously $\langle a \rangle$ is a cyclic group (its always a group). Any group with no proper nontrivial subgroups is generated by every non identity element (except the trivial group (or not, vacuous??)), so is cyclic.

7. Cyclic Groups

Subgroup of a cyclic group is cyclic.



Pick any subgroup H of the integers under addition. Then H is cyclic, so some h generates H. So $h \in \mathbb{Z}$ and we must have $H = h\mathbb{Z}$. The following is unrelated. A finicky but easy enough proof shows that any cyclic group is isomorphic to the integers under

addition or the integers under modular addition. The prior fact about subgroups of $\mathbb{Z}$ characterises subgroups of infinite cyclic groups, since their parents are isomorphic to $\mathbb{Z}$.

7.1. The hard bit: Cyclic Subgroups

Definition 7.1.1: The greatest common divisor of m, n is the generator d of the group

$$\{rm + sn : r, s \in \mathbb{Z}\}$$

Theorem 7.1.1: Let $G = \langle a \rangle$ be a cyclic group of order n. Then the order of the subgroup generated by a^m is $\frac{n}{d}$. Further, $\langle a^m \rangle = \langle a^p \rangle$ iff $\gcd(m, n) = \gcd(p, n)$.

Proof: Go read the first bit. The iff statement is badly explained. What they are saying is that

$$\{m \in \mathbb{Z}_n : \gcd(m, n) = d\} \subset \langle d \rangle$$

since $d \mid m \implies m = kd = d^k \in \langle d \rangle$. Any subgroup with $\frac{n}{d}$ elements contains all elements a^p of G such that $\gcd(p, n) = d$. In the case of $\mathbb{Z}_n$, this is just integers p with $\gcd(p, n) = d$. Then $\langle a^m \rangle$ contains a^p and $\langle a^p \rangle \subset \langle a^m \rangle$ and similarly $\langle a^m \rangle \subset \langle a^p \rangle$ so $\langle a^m \rangle = \langle a^p \rangle$. That is to say, if the gcd's are the same then the subgroups are the same. If the subgroups are the same, they have the same number of elements, $\frac{n}{d_1} = \frac{n}{d_2} \implies d_1 = d_2$. ■

Corollary 7.1.1.1: For each divisor d of n, where n is the order of a cyclic group G, there is at most one subgroup of G.

Corollary 7.1.1.2: Given any generator a of G of order n, the generators are a^p such that p is coprime with n.

Definition 7.1.2: The least common divisor of m, n is the generator of the group

$$\{k \in \mathbb{Z} : m \mid k, n \mid k\}.$$

The smallest possible LCM is mn because if $k \mid m$ then $mn = (ak)n = (an)k$ so $k \mid mn$. If m, n are coprime then $m \mid nk$ implies $m \mid k$. In particular, if $n \mid k$ then $k = qn$ so $m \mid k$ implies $m \mid q$ so that $k = qn = (am)n = a(mn)$, i.e. $mn \mid k$.

Theorem 7.1.2: For positive integers m, n

$$\gcd(m,n) * \mathrm{Lcm}(m,n) = mn.$$

Proof: Let $\mathrm{Lcm}(m,n) = am = bn$. Then

$$\frac{mn}{\mathrm{Lcm}(m,n)} * a = n, \frac{mn}{\mathrm{Lcm}(m,n)} * b = m$$

so it is a divisor of a, b, proving $\frac{mn}{\gcd(m,n)} \leq \mathrm{Lcm}(m,n)$. Since $\frac{mn}{\gcd(m,n)}$ is a multiple of both m and n, $\frac{mn}{\gcd(m,n)} \geq \mathrm{Lcm}(m,n)$. ■

Theorem 7.1.3: Abelian groups with cyclic subgroups H, K of coprime orders r and s have a cyclic subgroup of order rs. More generally, there is a subgroup of order $\mathrm{Lcm}(r,s)$.

Proof: We know that $H \cap K$ is a cyclic subgroup. So it must be generated by $x = h^p = k^q$. Let $m = |\langle x \rangle|$. Then $m = \frac{r}{\gcd(p,r)} = \frac{s}{\gcd(q,s)}$ so $m \mid r$ and $m \mid s$. Then $m \mid \gcd(r,s) = 1$ and $m = 1$. So $H \cap K$ is the trivial group. Now consider the group $Z = \{xy : x \in H, y \in K\}$ (it is a group since the whole group is Abelian). Since H, K are finite cyclic groups, there generators h, k of H, K. We define a bijection $f : Z_r \times Z_s \to Z$, $f(a,b) = h^a k^b$. if $f(a,b) = f(c,d)$, then $h^{a-b} = k^{d-c} = e$ since $H \cap K = \{e\}$. So $(a,b) = (c,d)$. Fix $z \in Z$. Then $z = xy = h^a k^b$ where $0 \leq a, b < r, s$ so $f(a,b) = z$. So f is a bijection as asserted. There are rs elements in $Z_r \times Z_s$ so the cardinality of Z is rs. We claim that Z is cyclic when r, s are coprime and gh generates Z. Since r, s are coprime there exist integers m_1, m_2 so that $1 = m_1 r + m_2 s$. Fix $z \in Z$ and write $z = h^a k^b$. Then we have

$$(hk)^{bm_1 r + am_2 s} = h^{bm_1 r + am_2 s} * k^{bm_1 r + am_2 s} = h^{am_2 s} * k^{bm_1 r} = h^{a(1-m_1 r)} * k^{b(1-m_2 s)} = h^a * k^b = z.$$

N.B. The Chinese remainder theorem applies here. ■

Proof: Easier proof. Consider $\langle hk \rangle$. This group is cyclic since it is generated by hk. The order is no more than rs, since $(hk)^{\{rs\}} = e^s * e^r = e$. Suppose $p < rs$ was the order of $\langle hk \rangle$. Then $h^p = k^{-p}$ so that $h^p \in H \cap K$. So $\langle h^p \rangle = d \mid r, s$ which implies $d = 1$, $\langle h^p \rangle = \{e\}$. It follows that $h^p = k^p = e$, so $r, s \mid p$ (because they are the orders of H, K). Then $p = ar$, so $s \mid a$ and $p = brs$, $rs \mid p$ which gives a contradiction, $p \geq rs$. ■

Lemma 7.1.4: Given r, s we can construct coprime a, b so that $a \mid r$, $b \mid s$ and $ab = \mathrm{Lcm}(r,s)$.

Proof: Write $\mathrm{Lcm}(r,s) = d * \left(\frac{r}{d}\right) * \left(\frac{s}{d}\right)$ and

$$d = p_1^{a_1} ... p_n^{a_n} * q_1^{b_1} ... q_m^{b_m}$$

where $p_i \nmid \frac{r}{d}$ and $q_i \mid \frac{r}{d}$. Then $q_i \nmid \frac{s}{d}$. Consider

$$a = p_1^{a_1} ... p_n^{a_n} * \frac{r}{d},$$
$$b = q_1^{b_1} ... q_m^{b_m} * \frac{s}{d}.$$

N.B. if $ab \mid m$ then $a \mid m$, $b \mid m$ contrapositive is if neither divide m then their product doesn't. ■

Proof: (of the latter part of Theorem 7.1.3):
By the lemma, we can construct coprime divisors a, b of r, s with $ab = \text{Lcm}(r, s)$ so that for $r = a\delta_1$, $s = b\delta_2$ and $\langle h^{\{\delta_1\}} \rangle \leq \langle h \rangle$, $\langle k^{\{\delta_2\}} \rangle \leq \langle k \rangle$ we have

$$\left|\langle h^{\{\delta_1\}} \rangle\right| = \frac{r}{\gcd(\delta_1, r)} = \frac{r}{\delta_1} = a,$$
$$\left|\langle k^{\{\delta_2\}} \rangle\right| = \frac{s}{\gcd(\delta_2, s)} = \frac{s}{\delta_2} = b.$$

The first part of the theorem completes the proof. ■

Example 7.1.1: There is a generator of $Z_{\{36\}}$ because it has subgroups $\langle 2 \rangle$, $\langle 3 \rangle$ with 12 and 18 elements. We write $12 = 6 * 2$ and $18 = 6 * 3$, then separate factors to get $6 = 3 * 2$, $a = 2 * \frac{12}{6} = 4$, $b = 3 * \frac{18}{6} = 9$ so that $12 = 4 * 3$ and $18 = 9 * 2$ so we can take these new factors $3, 2$ and raise existing generators to them. We then have $\langle 3^3 \rangle = \langle 9 \rangle$ of order 4 and $\langle 2^2 \rangle = \langle 4 \rangle$ of order 9. So we can generate $Z_{\{36\}}$ with $9 + 4 = 13$.

7.2. Cayleigh Digraphs

Definition 7.2.1: An arc in a cayleigh digraph is a directed edge that represents multiplication by a generator. When a generator is an involution we use undirected arcs.

An obvious implication of this is that in a group, if $a, b, ..., x, y$ are involutions then

$$(ab...xy)^{-1} = y^{-1}x^{-1}...b^{-1}a^{-1} = yx...ba.$$

Definition 7.2.2: A vertex in a cayleigh digraph is an element generated by the generators of the graph.

A group has a correspondence with a digraph with the following properties:
- If you start at a vertex and get to another vertex in two ways then the two ways will lead to the same destination from any point
- For each vertex in the graph, there is an arc corresponding with a generator going to and from the vertex
- There exists a unique path from any vertex a to another vertex b. But, the path may involve consecutive arcs; there is at most one arc from a to b.

Pick a vertex V. If all pairs of arcs from V go to the same vertex regardless of the order they are chosen then the group is commutative.