MathSoc Second Year Linear Algebra MATH2601 Abstract Algebra Notes

August 13, 2019

This resource was compiled by Rui Tong. Please be ethical with it. It is for the use of MathSoc members - do not repost it on other forums or groups without asking for permission. If you appreciate our resources, please consider supporting us by coming to our events! Also, happy studying :)

We cannot guarantee that our solutions are correct - please notify us of any errors or typos at unswmathsoc@gmail.com, or on our Facebook page. Remember that providing clear reasons is absolutely essential to earning all the marks in the exam!

Definition 1. *A **group** $(G, *)$ is a non-empty set G along with a binary operation $*$ on G satisfying the following axioms:*

1. ***Closure**: $a * b \in G$ for all $a, b \in G$*
2. ***Associativity**: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$*
3. ***Existence of identity**: there exists $e \in G$ such that $e * a = a * e = a$ for all $a \in G$*
4. ***Existence of inverses**: for every $a \in G$ there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$*

*A group $(G, *)$ is said to be **abelian** if it also satisfies the **commutative** axiom: $a * b = b * a$ for all $a, b \in G$.*

Example 1. *(2017 Test 1 Version A) Let*

$$G = \{(a, b) \in \mathbb{R}^2 \mid a \neq 0\}$$

and for any $(a_1, b_1), (a_2, b_2) \in G$, define

$$(a_1, b_1) * (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1)$$

where the operations in the right hand side are usual addition and multiplication in $\mathbb{R}$. Prove that G is a group under $*$.

Proof. **Closure:** Let $(a_1, b_1), (a_2, b_2) \in G$. Then $a_1 \neq 0$ and $a_2 \neq 0$. Hence $a_1 a_2 \neq 0$, so since

$$(a_1, b_1) * (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1),$$

it follows that $(a_1, b_1) * (a_2, b_2) \in G$. Therefore G is closed under $*$.

Associativity: Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$. Then

$$\begin{aligned}
((a_1, b_1) * (a_2, b_2)) * (a_3, b_3) &= (a_1 a_2, a_1 b_2 + b_1) * (a_3, b_3) \\
&= ((a_1 a_2) a_3, (a_1 a_2) b_3 + (a_1 b_2 + b_1)) \\
&= (a_1 a_2 a_3, a_1 a_2 b_3 + a_1 b_2 + b_1) \\
\text{and } (a_1, b_1) * ((a_2, b_2) * (a_3, b_3)) &= (a_1, b_1) * (a_2 a_3, a_2 b_3 + b_2) \\
&= (a_1 (a_2 a_3), a_1 (a_2 b_3 + b_2) + b_1) \\
&= (a_1 a_2 a_3, a_1 a_2 b_3 + a_1 b_2 + b_1) \\
&= ((a_1, b_1) * (a_2, b_2)) * (a_3, b_3).
\end{aligned}$$

Hence $*$ is associative in G.

Existence of identity: Consider $(1, 0) \in G$. Observe that for any $(a, b) \in G$,

$$\begin{aligned}
(a, b) * (1, 0) &= (a \times 1, a \times 0 + b) = (a, b) \\
\text{and } (1, 0) * (a, b) &= (1 \times a, 1 \times b + 0) = (a, b)
\end{aligned}$$

so $(1, 0)$ is the identity element of G.

Existence of inverse: For any $(a, b) \in G$, consider $\left(\frac{1}{a}, -\frac{b}{a}\right) \in G$, noting $\frac{1}{a}$ is well-defined and non-zero. Observe that

$$\begin{aligned}
(a, b) * \left(\frac{1}{a}, -\frac{b}{a}\right) &= \left(a\left(\frac{1}{a}\right), a\left(-\frac{b}{a}\right) + b\right) = (1, 0) \\
\text{and } \left(\frac{1}{a}, -\frac{b}{a}\right) * (a, b) &= \left(\left(\frac{1}{a}\right) a, \left(\frac{1}{a}\right) b - \frac{b}{a}\right) = (1, 0).
\end{aligned}$$

Hence every $(a, b) \in G$ has a corresponding inverse element $(a, b)^{-1} = \left(\frac{1}{a}, -\frac{b}{a}\right) \in G$.

Therefore G is a group under $*$. □

Side note: The identity and inverse element in the above proof were actually **discovered** by working **backwards**. Just remember that you can't actually give your final answer (proof) in reverse!

Definition 2. *For a **finite** group, the order of a group G is its cardinality $|G|$.*

Example 2. *Consider the group*

$$G = \left\{ z \in \mathbb{C} \mid z = e^{\frac{k\pi i}{3}} \mid k \in \mathbb{Z} \right\}.$$

This group has order $|G| = 6$. (Exercise: List the elements out.)

Lemma 1. *Let $(G, *)$ be a group. Then*

1. *The identity element of G is unique.*
2. *The inverse of any $a \in G$ is unique.*
3. *$(a^{-1})^{-1} = a$ for all $a \in G$*
4. *$(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$*
5. ***Cancellation**: Let $a, b, c \in G$.*
   - *If $a * b = a * c$, then $b = c$.*
   - *If $b * a = c * a$, then $b = c$.*

Example 3. *Prove statement 4 of Lemma 1.*

Proof. Let $a, b \in G$ and let $e \in G$ be the identity element. Then

$$\begin{aligned}
& (a*b)^{-1} * (a*b) = e && \text{(def. of id.)} \\
\implies \quad & (a*b)^{-1} * (a*b) * b^{-1} = e * b^{-1} && \\
\implies \quad & (a*b)^{-1} * a * (b * b^{-1}) = b^{-1} && \text{(assoc law, defn of id)} \\
\implies \quad & (a*b)^{-1} * a * e = b^{-1} && \text{(def. of inv)} \\
\implies \quad & (a*b)^{-1} * a = b^{-1} && \text{(def. of id)} \\
\implies \quad & [(a*b)^{-1} * a] * a^{-1} = b^{-1} * a^{-1} && \\
\implies \quad & (a*b)^{-1} * (a * a^{-1}) = b^{-1} * a^{-1} && \text{(assoc law)} \\
\implies \quad & (a*b)^{-1} * e = b^{-1} * a^{-1} && \text{(def. of inv)} \\
\implies \quad & (a*b)^{-1} = b^{-1} * a^{-1} && \text{(def. of id)}
\end{aligned}$$

□

Definition 3. *Let $(G, *)$ be a group and $H \subseteq G$. We say H is a subgroup of G if $(H, *)$ is also a group. We write $H \leq G$.*

Lemma 2. ***Subgroup lemma:*** *For a group G and non-empty set $H \subseteq G$, $H \leq G$ if we have the following axioms:*

- ***Closure**: $a * b \in H$ for all $a, b \in H$*
- ***Inverses contained**: If $a \in H$, then $a^{-1} \in H$, where a^{-1} is the corresponding inverse element of a in G*

Example 4. *Let $GL(n, \mathbb{R})$ denote the set of all invertible $n \times n$ matrices over $\mathbb{R}$ and let $SL(n, \mathbb{R})$ denote the matrices in $GL(n, \mathbb{R})$ with determinant equal to 1. Prove that $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$.*

Proof. **Closure under the group operation**: Let $A, B \in SL(n, \mathbb{R})$. Then $\det(A) = 1$ and $\det(B) = 1$.

Using known properties of the determinant, $\det(AB) = \det(A)\det(B) = 1 \times 1 = 1$. Therefore $AB \in SL(n, \mathbb{R})$ and hence $SL(n, \mathbb{R})$ is closed under $*$.

Closure under inverses: Let $A \in SL(n, \mathbb{R})$. Then $\det(A) = 1$. Hence

$$\det\left(A^{-1}\right) = \frac{1}{\det(A)} = \frac{1}{1} = 1$$

so $A^{-1} \in SL(n, \mathbb{R})$. Therefore $SL(n, \mathbb{R})$ is closed under taking inverses.Hence by the subgroup lemma, $SL(n, \mathbb{R})$ is a subgroup of $GL(n, \mathbb{R})$. □

Definition 4. *A **field** $(\mathbb{F}, +, \times)$ is a set $\mathbb{F}$ with two binary operations $+$ and $\times$ on $\mathbb{F}$, such that:*

1. *$(\mathbb{F}, +)$ is an **abelian group**.*
2. *$(\mathbb{F}\backslash\{\mathbf{0}\}, \times)$ is an **abelian group**, where $\mathbf{0}$ is the identity element of $(\mathbb{F}, +)$.*
3. *The **distributive laws** $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ hold.*

We define $a - b = a + (-b)$, where $-b$ is the additive inverse (negative) of b. We also define $a/b = ab^{-1}$ for all $b \neq 0$, where b^{-1} is the multiplicative inverse of b.

Example 5. *(2017 Tutorial) Show that $S = \left\{x + y\sqrt{2} + iz \in \mathbb{C} \mid x, y, z \in \mathbb{Q}\right\}$ is NOT a field.*

Proof. Take, for example, $w = \sqrt{2} \in S$ and $i \in S$. Then,

$$iw = \sqrt{2}i \notin S$$

since the imaginary part of every element of S must be rational, and $\operatorname{Im} iw = \sqrt{2} \notin \mathbb{Q}$). Hence S is not closed under multiplication and thus not a field. □

Lemma 3. *Let $(\mathbb{F}, +, \times)$ be a group and 0 be the identity element of $(\mathbb{F}, +)$. Then furthermore,*

1. *Multiplication by 0 gives 0: $a0 = 0$*
2. *Product with a negative is the negative of the product: $a(-b) = -(ab)$*
3. *Distributive law operates on negatives: $a(b - c) = ab - ac$*
4. ***Null factor law:** If $ab = 0$, then either $a = 0$ or $b = 0$.*

Example 6. *Prove statement 2 of Lemma 3, assuming that statement 1 holds.*

Proof. By definition, $ab + (-(ab)) = 0$. However also observe that

$$\begin{aligned} ab + a(-b) &= a(b + (-b)) && \text{(distributive law)} \\ &= a0 && \text{(definition of additive identity)} \\ &= 0. && \text{(from the lemma)} \end{aligned}$$

Hence upon equating, $ab + a(-b) = ab + (-(ab))$, so by the **cancellation lemma** of groups, $a(-b) = -(ab)$. □

Definition 5. *Let $(\mathbb{F}, +, \times)$ be a group and $\mathbb{H} \subseteq \mathbb{F}$. We say $\mathbb{H}$ is a subfield of $\mathbb{F}$ if $(\mathbb{H}, +, \times)$ is also a field. We write $\mathbb{H} \leq \mathbb{F}$.*

Lemma 4. ***Subfield lemma**: For a field $\mathbb{F}$ and non-empty set $\mathbb{H} \subseteq \mathbb{F}$, $\mathbb{H} \leq \mathbb{F}$ if we have the following closure axioms for all $a, b \in \mathbb{H}$:*

1. *$a + b \in \mathbb{H}$ (closure under addition)*
2. *$a - b \in \mathbb{H}$ (closure under adding negatives)*
3. *$ab \in \mathbb{H}$ (closure under multiplication)*
4. *$a/b \in \mathbb{H}$, here for $b \neq 0$ (closure under multiplying inverses)*

Example 7. *(Only partially...) Show that $\mathbb{E} = \left\{ z \in \mathbb{R} \mid z = p + q\sqrt{2} \mid p, q \in \mathbb{Q} \right\}$ is a subfield of $\mathbb{R}$ equipped with usual addition and multiplication.*

Proof. Let $z_1, z_2 \in \mathbb{E}$. Write

$$\begin{aligned} z_1 &= p_1 + q_1\sqrt{2} \\ z_2 &= p_2 + q_2\sqrt{2} \end{aligned}$$

where $p, q \in \mathbb{Q}$. Then supposing that $z_2 \neq 0$ we have

$$\begin{aligned} z_1/z_2 &= \frac{p_1 + q_1\sqrt{2}}{p_2 + q_2\sqrt{2}} \\ &= \frac{\left(p_1 + q_1\sqrt{2}\right)\left(p_2 - q_2\sqrt{2}\right)}{\left(p_2 + q_2\sqrt{2}\right)\left(p_2 - q_2\sqrt{2}\right)} \\ &= \frac{p_1p_2 - 2q_1q_2}{p^2 - 2q^2} + \frac{q_1p_2 - q_2p_1}{p^2 - 2q^2}\sqrt{2} \\ &\in \mathbb{E}, \end{aligned}$$

noting that $\frac{p_1p_2 - 2q_1q_2}{p^2 - 2q^2}$ and $\frac{q_1p_2 - q_2p_1}{p^2 - 2q^2}$ are well defined rational numbers. Hence $\mathbb{E}$ is closed under 'division'.

The remainder is left as your exercise. □

Definition 6. *Let $(G, *)$ and $(H, \circ)$ be groups. A **group homomorphism** from G to H is a function $\phi : G \to H$ with the property that for all $a, b \in G$, $\phi(a * b) = \phi(a) \circ \phi(b)$.*

Definition 7. *A **group isomorphism** on groups $(G, *)$ and $(H, \circ)$ is a group homomorphism that is bijective/invertible. If a group isomorphism exists between G and H, the groups are said to be isomorphic.*

Example 8. *(2008 Exam) Let*

$$G = \left\{ \begin{pmatrix} 1 & t & t^2/2 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} : t \in \mathbb{R} \right\}.$$

You may assume that $(G, \times)$ is a group under matrix multiplication. Show that $(G, \times)$ is isomorphic to $(\mathbb{R}, +)$.

Proof. Define $\phi : \mathbb{R} \to G$,

$$\phi(t) = \begin{pmatrix} 1 & t & t^2/2 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}.$$

Then for any $s, t \in \mathbb{R}$,

$$\begin{aligned} \phi(s)\phi(t) &= \begin{pmatrix} 1 & s & s^2/2 \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & t & t^2/2 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & s+t & s^2/2 + st + t^2/2 \\ 0 & 1 & s+t \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & s+t & (s+t)^2/2 \\ 0 & 1 & s+t \\ 0 & 0 & 1 \end{pmatrix} \\ &= \phi(s+t) \end{aligned}$$

so ϕ is a homomorphism from $\mathbb{R}$ to G. However ϕ is invertible as we may define

$$\phi^{-1} \begin{pmatrix} 1 & t & t^2/2 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} = t$$

for any all real t, so that $\phi(\phi^{-1}(t)) = t$ and

$$\phi^{-1}\left(\phi\begin{pmatrix}1 & t & t^2/2\\ 0 & 1 & t\\ 0 & 0 & 1\end{pmatrix}\right) = \begin{pmatrix}1 & t & t^2/2\\ 0 & 1 & t\\ 0 & 0 & 1\end{pmatrix}.$$

Note that ϕ^{-1} is well defined since it depends only on a real number t, as is the case for G. Hence ϕ is an isomorphism on $\mathbb{R}$ to G, so the groups are isomorphic. □

Remark: This proof involved an absurdly large amount of writing, however prior to 2017 the exams were **three** hours long, so they actually had the time to do this. Your exam will (hopefully) involve slightly less writing, even with the same difficulty intended.

Lemma 5. *Let $(G, *)$ and $(H, \circ)$ be groups and suppose there exists a homomorphism $\phi : G \to H$. Then the following hold.*

1. ***Identities are mapped to identities:*** *$\phi(e) = f$, where e is the identity element of G and f is the identity element of H.*
2. ***Inverses are mappped to inverses:*** *$\phi\left(g^{-1}\right) = [\phi(g)]^{-1}$ for all $g \in G$.*

*Further, if $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is an isomorphism (albeit from H to G). (i.e. **the inverse map is an isomorphism**)*

Example 9. *(2017 Exam) Prove the result above on the inverse map is an isomorphism.*

Proof. Let $(G, *)$ and $(H, \circ)$ be isomorphic groups with isomorphism $\phi : G \to H$. We know that $\phi^{-1} : H \to G$ is bijective from properties of functions. To show that ϕ^{-1} is an isomorphism, let $h_1, h_2 \in H$. As ϕ is bijective, write

$$h_1 = \phi(g_1) \text{ and } h_2 = \phi(g_2)$$

for corresponding values of $g_1, g_2 \in G$. Then

$$\begin{aligned}\phi^{-1}(h_1 \circ h_2) &= \phi^{-1}\left(\phi(g_1) \circ \phi(g_2)\right)\\ &= \phi^{-1}\left(\phi(g_1 * g_2)\right) && (g \text{ is an isomorphism})\\ &= g_1 * g_2\\ &= \phi^{-1}(h_1) * \phi^{-1}(h_2)\end{aligned}$$

as required. Thus ϕ^{-1} is an isomorphism. □

Definition 8. *Let $(G, *)$ and $(H, \circ)$ be groups and suppose that $\phi : G \to H$ is a homomorphism.*

- *The **kernel** of ϕ is defined as*

$$\ker(\phi) = \{g \in G : \phi(g) = f\}$$

  where f is the identity element of H. (That is, it is everything mapped to the identity.)
- *The **image** of ϕ is defined as*

$$\mathrm{im}(\phi) = \{h \in H : h = \phi(g) \text{ for some } g \in G\}.$$

  (That is, it is the range of the function ϕ.)

Lemma 6. *Let $(G, *)$ and $(H, \circ)$ be groups and suppose that $\phi : G \to H$ is a homomorphism.*

1. $\ker \phi$ *is a subgroup of* G.
2. $\mathrm{im}\, \phi$ *is a subgroup of* H.
3. ϕ *is injective if and only if* $\ker \phi = \{e\}$, *where e is the identity element of G.*

Example 10. *Prove statement 2 of lemma 6.*

Proof. **Closure under the operation:** Let $h_1, h_2 \in \mathrm{im}\, \phi$. Then

$$h_1 = \phi(g_1) \text{ and } h_2 = \phi(g_2)$$

for some $g_1 \in G$ and $g_2 \in G$. Observe that

$$h_1 \circ h_2 = \phi(g_1) \circ \phi(g_2) = \phi(g_1 * g_2)$$

and since G is a group, $g_1 * g_2 \in G$. Hence we've expressed $h_1 \circ h_2 = \phi(g)$ by taking $g = g_1 * g_2 \in G$, so $h_1 \circ h_2 \in \mathrm{im}\, \phi$.

Closure under inverses: Let $h \in \mathrm{im}\, \phi$. Then $h = \phi(g)$ for some $g \in G$. Hence from

lemma 5 (which you will probably be asked to prove beforehand in an exam),

$$h^{-1} = [\phi(g)]^{-1} = \phi(g^{-1})$$

and since $g^{-1} \in G$, it follows that $h^{-1} \in \operatorname{im}\phi$.

Hence by the subgroup lemma, $\operatorname{im}\phi \leq H$. □

Example 11. *(2017 Exam) Let $(G, *)$ be a group with identity element e and let $(H, \circ)$ be a group with identity element f. Let $\phi : G \to H$ be a group homomorphism. Show that if $g \in G$ and $k \in \ker\phi$, then $g * k * g^{-1} \in \ker\phi$.*

Proof. Suppose that $g \in G$ and $k \in \ker\phi$. Then $\phi(k) = f$. Observe that

$$\begin{aligned}
\phi\left(g * k * g^{-1}\right) &= \phi(g) * \phi(k) * \phi(g^{-1}) && \text{(using associative law)} \\
&= \phi(g) * f * \phi(g^{-1}) \\
&= \phi(g) * \phi(g^{-1}) && \text{(definition of identity)} \\
&= \phi(g) * [\phi(g)]^{-1} && \text{(from lemma 5)} \\
&= f. && \text{(definition of inverses)}
\end{aligned}$$

Hence $g * k * g^{-1} \in \ker\phi$. □