Math 402A

Due October 1, 2008

1. (a) Prove that $GL_n(\mathbb{R})$ is a group.

(b) Prove that S_n is a group.

Proof. (a) The $n \times n$ general linear group over $\mathbb{R}$

$$GL_n(\mathbb{R}) = \{A = (a_{ij})_{1 \le i,j \le n} | a_{ij} \in \mathbb{R}, \det A \neq 0\}.$$

The identity matric $I \in GL_n(\mathbb{R})$, so $GL_n(\mathbb{R}) \neq 0$. For any $A, B \in GL_n\mathbb{R}, \det A \neq 0$ and $\det B \neq 0$, then $\det AB = \det A \det B \neq 0$, so that $AB \in GL_n(\mathbb{R})$.

Obviously the associative law holds and I is the identity element.

Finally, if $A \in GL_n(\mathbb{R})$, then A^{-1} exists and $\det A^{-1} = (\det A)^{-1} \neq 0$, so $A^{-1} \in GL_n(\mathbb{R})$. Therefore $GL_n(\mathbb{R})$ is a group. $\square$

(b) Any element σ of S_n can be described as $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}$, which denotes the permutation that maps $1 \mapsto i_1, 2 \mapsto i_2, \ldots, n \mapsto i_n$. Then the inverse of σ is $\begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} \in S_n$. The product $\sigma\tau$ of two elements of S_n is the composition of function τ followed by σ, so that $\sigma\tau \in S_n$. The identity map is the identity element in S_n. Therefore S_n is a group. $\square$

2. Let G be a group, with multiplicative notation. We define an opposite group G^0 with law of composition $a \circ b$ as follows: The underlying set is the same as G, but the law of composition is the opposite; that is, we define $a \circ b = ba$. Prove that this define a group.

Proof. Clearly the law of composition holds in G^0 and the identity element 1 in G is also an identity element in G^0. Second, the law of associative: $(a \circ b) \circ c = ba \circ c = cba = a \circ (cb) = a \circ (b \circ c)$. Finally, $a \circ a^{-1} = 1$ so every element has an inverse in G^0. Here a^{-1} is the inverse of a in G. $\square$

3. Determine the elements of the cyclic group generated by the matrix $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ explicitly.

Solution. Let $A = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$. Then $A^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$, $A^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $A^4 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$, $A^5 = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ and $A^6 = I$ the identity matric. Therefore the group generated by A is isomorphic to the cyclic group of order 6. $\square$

4. Which of the following are subgroups?

(a) $GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$.

(b) $\{1, -1\} \subset \mathbb{R}^\times$.

(c) The set of positive integers in $\mathbb{Z}^+$.

(d) The set of positive reals in $\mathbb{R}^\times$.

(e) The set of all matrix $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, with $a \neq 0$, in $GL_2(\mathbb{R})$.

Solution. (a), (b), (d), (e). $\square$

5. Let $U_n = \{n\text{th roots of unity}\} \subseteq \mathbb{C}, n \geq 2$. Prove that U_n is a commutative subgroup of $\mathbb{C}$ under the multiplication operation and $|U_n| = n$. Draw a picture of U_n, when $n = 4, 6, 8$ and describe how the operation works geometrically. Verify there is an element $\xi_n \in U_n$ with the property that $\langle \xi_n \rangle = U_n$ and describe ξ_n^k geometrically for $1 \leq k \leq n$. (ξ is called the primitive root of unity.)

Proof. $U_n = \{e^{i\frac{2k\pi}{n}} | 0 \leq k \leq n-1\}$. It is easy to see that U_n is a commutative subgroup of $\mathbb{C}$ and $|U_n| = n$. We may take $\xi_n = e^{i\frac{2\pi}{n}}$ and then U_n is a cyclic group generated by ξ_n. $\square$

6. Let $S^1 = \{\text{unit circle}\} \subseteq \mathbb{C}$. Prove S^1 is a subgroup of $\mathbb{C}$ under multiplication.

Proof. $S^1 = \{e^{i\theta} | -\pi \leq \theta \leq \pi\}$. Then $e^{i\theta}e^{i\eta} = e^{i(\theta+\eta)} \in S^1$ and $(e^{i\theta})^{-1} = e^{-i\theta} \in S^1$, so that S^1 is a subgroup of $\mathbb{C}$. $\square$

7. Let $G = \mathbb{Z}$ and let the operation $a * b = a - b$(substraction); Is G a group? Explain.

Proof. No. It does not satisfy the associative law: for any $a, b, c \in G$, we have $(a * b) * c = (a - b) - c; a * (b * c) = a - (b - c) = a - b + c \neq (a * b) * c$.

OR: G dose not have an identity element. Suppose there is an identity element in G. say e, then for any nonzero integer a we have $a * e = a - e = a$, so $e = 0$. But $e * a = 0 - a = -a \neq a$.$\square$

8. Let $G = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. Prove that G is a group under "+". Prove that $G^* = \{\text{nonzero elements of } G\}$ is a group under multiplication.

Proof. Obviously both G and G^* are non-empty. (1) Let $a+b\sqrt{2}, c+d\sqrt{2} \in G$. Then $(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2} \in G$. 0 is the identity element in G and the inverse of $a+b\sqrt{2}$ is $-a+(-b)\sqrt{2}$. Clearly the associative law holds. (2) Let $a+b\sqrt{2}, c+d\sqrt{2} \in G^*$. Then $0 \neq (a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in G^*$. 1 is the identity element in G^* and the inverse of $a+b\sqrt{2}(a+b\sqrt{2} \neq 0)$ is $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in G^*$. Here $a - b\sqrt{2} \neq 0$ because otherwise $\frac{a}{b} = \sqrt{2}$ but $\frac{a}{b} \in \mathbb{Q}$ which is a contradiction. Again clearly the associative law holds.$\square$

9. Let $G = \mathbb{Q} - \{2\}$. Define $a * b = ab - 2a - 2b + 6$, where the right hand side involves the usual addition and multiplication of rational numbers.

(a) Prove that G is a group;

(b) What is the identity element?

(c) Calculate $(\frac{3}{2})^{-1}$ and $(-1)^{-1}$;

(d) What is $\langle 4 \rangle$?

Solution. For any $a, b \in G, a * b - 2 = ab - 2a - 2b + 4 = (a-2)(b-2) \neq 0$ since $a \neq 2$ and $b \neq 2$, so that $a * b \in G$. Furthermore, since $a * 3 = 3a - 2a - 6 + 6 = a$ and $3 * a = 3a - 6 - 2a + 6 = a$, 3 is the identity element in G. It is straightforward to verify that $a^{-1} = \frac{2a-3}{a-2} = 2 + \frac{1}{a-2}$. Especially, $(\frac{3}{2})^{-1} = 4$ and $(-1)^{-1} = \frac{5}{2}$. It is easy to verify the associative law holds. Therefore G is a group. Finally the subgroup generated by 4 is all the rational numbers of the form $2(a-1)$ with $a \neq 2$.□

10. Prove that in any group the orders of ab and of ba are equal.

Proof. Note that $ab = b^{-1}(ba)b$. If $(ba)^n = e$, then $(ab)^n = (b^{-1}(ba)b)^n = b^{-1}(ba)^n b = e$. Conversely, if $(ab)^n = e$, then $(b^{-1}(ba)b)^n = b^{-1}(ba)^n b = e$, namely, $(ba)^n = e$.□

11. Describe all groups G which contain no proper subgroup.

Solution. If any element of G is of order 1, then $G = \{e\}$. We may assume that $G \neq \{e\}$. Then there exists an element $a \in G$ whose order is $m, m > 1$. Then $\langle a \rangle \neq \{e\}$, so that $G = \langle a \rangle$ since G has no proper subgroup, i.e. G is a cyclic group. But a cyclic group has no proper group if and only if its order is prime. Consequently, $G = \{e\}$ or $G \backsimeq \mathbb{Z}_q$ with q prime. □

12. Prove that every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$ be a cyclic group and H a subgroup of G. Then either $H = \{e\}$ or there exists a least positive integer m such that $a^m \in H$. Clearly, $\langle a^m \rangle \subset H$. Conversely, if $a^k \in H$, then $k = qm + r$ with $q, r \in \mathbb{Z}$ and $0 \geq r < m$ (division algorithm). Since $a^r = a^k(a^{qm})^{-1} \in H$ then the minimality of m implies that $r = 0$ and $k = qm$. Hence $H \subset \langle a^m \rangle$ and $H = \langle a^m \rangle$ thereby. □

13. Let G be a cyclic group of order n, and let r be an integer dividing n. Prove that G contains exactly one subgroup of order r.

Proof. Let $G = \langle a \rangle$ and $n = rk$. Then a^k is of order r and hence $\langle a^k \rangle$ is a subgroup of order r. Suppose that $H < G$ and $|H| = r$. By the conclusion of Exercise 12, $H = \langle a^m \rangle$ with a^m of order r. But the order of a^m is $\frac{n}{(m,n)}$, so $\frac{n}{(n,m)} = r$, i.e. $n = r(m,n)$. Hence $k = (m,n)$ and $k|m$, which implies that $a^m \in \langle a^k \rangle$ and hence $\langle a^m \rangle \subset \langle a^k \rangle$. But $|\langle a^m \rangle| = |\langle a^k \rangle|$, we must have $H = \langle a^k \rangle$.□

14. Define $T = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} : 0 \leq \theta \leq 2\pi \right\} \subset GL_2(\mathbb{R})$.

(a) Prove T is a commutative subgroup of $GL_2(\mathbb{R})$;

It is straightforward to verify.

(b) Is T is a cyclic group?

No.

(c) Describe the geometric effect of applying an element of T to a column vector $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbb{R}^2$.

Rotate the vector counterclockwise by θ.

15. Prove or disprove: Let G be a group with the property that every element has finite order. Then G is a finite group.

Proof. The statement is NOT true. Let $G = \bigcup_{n=1}^{\infty} U_n$. Then G is an infinite group while every element in G is of finite order. $\square$

16. Describe lattice of all subgroups of S_3 and U_{20}.

Solution. (1) $S_3 = \{(1), (12), (13), (23), (123), (132)\}$. Subgroup of order 1: (1); subgroups of order 2: $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$; subgroups of order 3: $\langle(123)\rangle$; subgroup of order 6: S_3. (2) $U_{20} = \{e^{i\frac{2k\pi}{20}} | 0 \leq k \leq 19\}$ is a cyclic group of order 20. Subgroup of order 1: 1; subgroup of order 2: $\langle -1 \rangle$; subgroup of order 4: $\langle i \rangle$; subgroup of order 5: $\langle e^{i\frac{2\pi}{5}} \rangle$; subgroup of order 10: $e^{i\frac{\pi}{5}}$; subgroup of order 20: U_{20} itself. $\square$

References