Show all your work. Justify your solutions. Answers without justification will not receive full marks.

Only hand in the problems on page 2.

Practice Problems

Question 1. Show that G is abelian iff $aba^{-1}b^{-1} = 1$ for every $a, b \in G$.

Solution:
$\Longrightarrow$ G is abelian, so $ab = ba$ for all $a, b \in G$. Therefore $aba^{-1}b^{-1} = baa^{-1}b^{-1} = bb^{-1} = 1$.

$\Longleftarrow$ Have $aba^{-1}b^{-1} = 1$. Multiplying both sides on the right by ba gives $aba^{-1}b^{-1}ba = 1ba$, therefore $ab = ba$. Since $a, b \in G$ are arbitrary, G is abelian.

Question 2. Are the following subgroups of $GL_n(\mathbb{R})$? Prove your answer.

(a) The set of $n \times n$ real-valued matrices with positive determinant.
(b) The set of $n \times n$ real-valued matrices with determinant -1.

Solution: Let $S \subseteq GL_n(\mathbb{R})$ be the set of $n \times n$ real-valued matrices with positive determinant.

Note that $\det(AB) = \det(A)\det(B)$, and $\det(I) = 1$, where I is the identity matrix. Since I has positive determinant, the set is non-empty. Thus $\det(A)\det(A^{-1}) = 1$, or $\det A^{-1} = 1/\det(A)$, and hence $\det(AB^{-1}) = \det(A)/\det(B)$, which is positive if $\det(A)$ and $\det(B)$ are positive. Therefore if $A, B \in S$ then $AB^{-1} \in S$. Also S is non-empty, eg $I \in S$, so S is a subgroup. If A and B have determinant -1, then $\det(AB) = 1$, so the set is not closed under matrix multiplication and is not a subgroup.

Question 3. Let $\mathscr{M}$ be the set of monotonic functions $\mathbb{R} \to \mathbb{R}$. That is, $f \in \mathscr{M}$ if either $f(x) \geq f(y)\ \forall\ x > y$, or $f(x) \leq f(y)\ \forall\ x > y$. Is $\mathscr{M}$ a subgroup of $\mathscr{F}$ under pointwise addition?

Solution: Let $f, g \colon \mathbb{R} \to \mathbb{R}$ be given by $f(x) = e^x$, $g(x) = e^{-x}$. These are both monotonic; f is increasing while g is decreasing. But $(f + g)(x) = e^x + e^{-x}$, so $f + g$ is increasing for positive x, decreasing for negative x, and hence is not monotonic. Therefore $\mathscr{M}$ is not closed and hence not a subgroup.

Assignment Problems

Question 1.

(a) Let $G = \mathbb{R}$, $a \diamond b = (a+b)/2$. Is $(G, \diamond)$ a group?

(b) Define an operation $*$ on $H = \mathbb{R} \setminus \{0\}$ by $a * b = |a|b$. Is $(H, *)$ a group?

(c) Define $\odot$ on $K = \mathbb{R} \setminus \{-1\}$ by $a \odot b = ab + a + b$. Is $(K, \odot)$ a group?

Solution:

(a) $(1 \diamond 1) \diamond 2 = (1) \diamond 2 = 3/2$, but $1 \diamond (1 \diamond 2) = 1 \diamond (3/2) = 5/4$, therefore $(1 \diamond 1) \diamond 2 \neq 1 \diamond (1 \diamond 2)$, so $\diamond$ is not associate, and $(G, \diamond)$ is not a semigroup (or group).

(b) Clearly $H \neq \emptyset$, and $(a * b) * c = (|a|b) * c = \Big||a|b\Big|c = |ab|c = |a||b|c = |a|(b * c) = a * (b * c)$ so $*$ is associative.

However H does not have an identity. Proof: suppose e is an identity. Then $(-1) * e = (-1)$ so $|(-1)|e = -1$, so $e = -1$ is the only possibility. But $1 * e = 1 * (-1) = -1 \neq 1$, so in fact e is not an identity. So H is not a group. Note that for every $a \in H$, $1 * a = |1|a = a$, so 1 is a "left identity", but the definition of group requires a two-sided identity.

(c) Clearly K is non-empty. We must check that $\odot$ is a binary operation on K. The issue here is that $-1 \notin K$, so we must check that if a, $b \in K$ then $a \odot b \neq -1$, otherwise $\odot$ is not a function $K \times K \to K$.

Thus, suppose a, $b \neq -1$ but $a \odot b = -1$. Then $ab + a + b = -1$ so $0 = ab + a + b + 1 = (a+1)(b+1)$ so either $a = -1$ or $b = -1$, a contradiction.

Let a, b, $c \in K$. Then $(a \odot b) \odot c = (ab+a+b) \odot c = (ab+a+b)c + (ab+a+b) + c = abc + ab + bc + ca + a + b + c$, and $a \odot (b \odot c) = a \odot (bc+b+c) = a(bc+b+c) + a + bc + b + c = abc + ab + bc + ca + a + b + c$, so $\odot$ is associative.

Observe that $a \odot b = b \odot a$ so $\odot$ is commutative. This is not required to prove that K is a group, but shortens some of the remaining calculations. Thus, for all $a \in K$ we have $0 \odot a = a \odot 0 = a \cdot 0 + a + 0 = a$, so 0 is the identity.

If $a \in K$, let $b = -a/(a+1)$. Since $a \neq -1$ the denominator of b is not 0. If $b = -1$ then $a/(a+1) = 1$ so $a = a+1$, which is impossible. Thus $b \in K$. And $b \odot a = a \odot b = a \odot \frac{-a}{(a+1)} = a \cdot \frac{-a}{(a+1)} + a + \frac{-a}{(a+1)} = (-a^2 + a(a+1) - a)/(a+1) = 0$, the identity in K. Thus b is the inverse of a, so K is a group.

Of course, the calculations leading to this proof occur in the reverse order. Suppose $a\dot{e} = a$. Then $a = ae + a + e$ so $e(a+1) = 0$ and $a \neq -1$ so $e = 0$ is the only possible identity. So in the proof we should check that 0 actually is the identity. Similarly, if $a \odot b = 0$ then $ab + a + b = 0$, so $-a = b(a+1)$, so $b = -a/(a+1)$. Etc.

Question 2. For $n = 10, 11, 12, 13, 14, 15, 16$, list the elements of the group $(\mathbb{Z}/n\mathbb{Z})^\times$. In each case is the group abelian? Is it cyclic? If so, give a generator.

Solution: $(\mathbb{Z}/n\mathbb{Z})^\times$ consists of all congruence classes a with $\gcd(a, n) = 1$. There are $\varphi(n)$ of these. All these groups are abelian since $xy \equiv yx \pmod{n}$. To determine if the group is cyclic, we must see if there is an element of order $\varphi(n)$.

$n = 10$: $\{1, 3, 7, 9\}$. The powers of 3 are $3, 9, 7, 1$ respectively, so the group is cyclic, generated by 3.

$n = 11$: $\{1, 2, \ldots, 10\}$. The powers of 2 are $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$ respectively, so 2 has order 10, and the group is cyclic, generated by 2.

$n = 12$: $\{1, 5, 7, 11\}$. Since $5^2 = 7^2 = 11^2 = 1$, no element has order 4.

$n = 13$: $\{1, 2, \ldots, 12\}$. This is cyclic, generated by 2. The powers of 2 are $2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$.

$n = 14$: $\{1, 3, 5, 9, 11, 13\}$. This is cyclic, generated by 3. The powers of 3 are $3, 9, 13, 11, 5, 1$.

$n = 15$: $\{1, 2, 4, 7, 8, 11, 13, 14\}$. This is not cyclic: $2^4 = 7^4 = 8^4 = 13^4 = 1$ and $4^2 = 11^2 = 14^2 = 1$, so no element has order more than 4.

$n = 16$: $\{1, 3, 5, 7, 9, 11, 13, 15\}$. $3, 5, 11, 13$ have order 4 and $7, 9, 15$ have order 2, so this group is not cyclic.

Question 3. Let G be the collection of 2×2 matrices with entries in $\mathbb{Z}/2\mathbb{Z}$ and with determinant 1:

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}/2\mathbb{Z}, \quad ad - bc \equiv 1 \pmod 2 \right\}.$$

It is easy to check that G is a group.

(a) List all the elements of G, and calculate their orders.

(b) Is G cyclic? Is it abelian?

Solution: There are at most 2 choices for each of a, b, c, d so G has at most 16 elements. The determinant condition implies $a, d \neq 0$ or $b, c \neq 0$ so $G = \left\{ I, T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$.

Check that $B^2 = C^2 = T^2 = I$, $S^2 = A$, $S^3 = I$ (recall that all calculations are going on in $\mathbb{Z}/2\mathbb{Z}$). Thus $A^2 = S^4 = S$ and $A^3 = S^6 = I$.

Element	Order
I	1
B, C, T	2
S, A	3

No element has order 6, so G is not cyclic. $ST = C$, $TS = B$ so G is not abelian.

In fact, $TS = S^2T$ so $G = \{I, S, S^2, T, ST, S^2T\}$, and this is exactly the same group as D_3, with S in place of σ and T in place of τ. More formally, there is an isomorphism $D_3 \to G$ mapping $\sigma \mapsto S$ and $\tau \mapsto T$. This is an example of a *group representation* where we can study D_3 by instead studying a group of matrices.

Question 4.

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix} \in S_5$. These represent symmetries of a regular pentagon, corresponding to rotation by $2\pi/5$ and a "flip", respectively.

(a) Calculate σ^2, $\sigma^3, \ldots$ until you reach $\sigma^n = 1$. What is the order of σ?

(b) What is the order of τ?

(c) Show that $\tau\sigma = \sigma^4\tau$.

(d) Give the Cayley table for the dihedral group of symmetries of the regular pentagon D_5. Express every element in the table in the form $\sigma^m\tau^n$ where m, $n \geq 0$ are as small as possible.

Solution:

(a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$, $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$, $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$, $\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$, $\sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = 1$. So σ has order 5.

(b) $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$, and $\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = 1$. So τ has order 2.

(c) $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$, and

$\sigma^4\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} = \tau\sigma$.

(d) We have $\tau\sigma = \sigma^4\tau$. Thus $\tau\sigma^2 = \sigma^4\tau\sigma = \sigma^8\tau = \sigma^3\tau$, $\tau\sigma^3 = (\tau\sigma^2)\sigma = \sigma^3\tau\sigma = \sigma^7\tau = \sigma^2\tau$, $\tau\sigma^4 = \sigma\tau$ similarly.

Thus $\tau\sigma\tau = \sigma^4\tau^2 = \sigma^4$, $\tau\sigma^2\tau = \sigma^3\tau^2 = \sigma^3$, $\tau\sigma^3\tau = \sigma^2$, $\tau\sigma^4\tau = \sigma$.

D_5	1	σ	σ^2	σ^3	σ^4	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	$\sigma^4\tau$
1	1	σ	σ^2	σ^3	σ^4	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	$\sigma^4\tau$
σ	σ	σ^2	σ^3	σ^4	1	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	$\sigma^4\tau$	τ
σ^2	σ^2	σ^3	σ^4	1	σ	$\sigma^2\tau$	$\sigma^3\tau$	$\sigma^4\tau$	τ	$\sigma\tau$
σ^3	σ^3	σ^4	1	σ	σ^2	$\sigma^3\tau$	$\sigma^4\tau$	τ	$\sigma\tau$	$\sigma^2\tau$
σ^4	σ^4	1	σ	σ^2	σ^3	$\sigma^4\tau$	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
τ	τ	$\sigma^4\tau$	$\sigma^3\tau$	$\sigma^2\tau$	$\sigma\tau$	1	σ^4	σ^3	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^4\tau$	$\sigma^3\tau$	$\sigma^2\tau$	σ	1	σ^4	σ^3	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	$\sigma^4\tau$	$\sigma^3\tau$	σ^2	σ	1	σ^4	σ^3
$\sigma^3\tau$	$\sigma^3\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	$\sigma^4\tau$	σ^3	σ^2	σ	1	σ^4
$\sigma^4\tau$	$\sigma^4\tau$	$\sigma^3\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^4	σ^3	σ^2	σ	1

Note the structure in the group table: $\begin{pmatrix} \square & \blacksquare \\ \blacksquare & \square \end{pmatrix}$, where $\square$ contains all the powers of σ, and $\blacksquare$ all the terms $\sigma^n\tau$. This occurs because the group $H = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4\}$ is a normal subgroup of G (exercise). So G/H is a group with $10/5 = 2$ elements. It must therefore be isomorphic to the cyclic group with 2 elements. One element is H, denoted $\square$, and the other is τH, denoted $\blacksquare$. (It is more clear that $\blacksquare = H\tau = \{h\tau \mid h \in H\}$, but that turns out to be the left coset τH, as we calculated above.)