Homework 3

Jaden Wang

Problem (5.9)**.** Yes. By Problem 4.13, we have already shown that D_n^* is a group, where D_n^* denotes the set of diagonal $n \times n$ matrices with no zeros on the diagonal. Since we are told that elements in this set are invertible (or by definition of a group), it follows that $D_n^* \subseteq GL(n, \mathbb{R})$.Since D_n^* is a group under the same operation as $GL(n, \mathbb{R})$, namely matrix multiplication, by the definition of subgroup, D_n^* is a subgroup of $GL(n, \mathbb{R})$.

Problem (5.10)**.** Yes. Denote this set as U_n^*, since we are told that its elements are invertible (or by full-rankness), $U_n^* \subseteq GL(n, \mathbb{R})$. Given $A, B \in U_n^*$,

(i) Notice that I_n is the identity of $GL(n, \mathbb{R})$, and I_n is an upper triangle matrix with no zeros on the diagonal, so $I_n \in U_n^*$.

(ii) We want to show that A^{-1} is also an upper triangle matrix with no zeros on the diagonal, so that $A^{-1} \in U_n^*$.

First let's show that it is upper triangular via the inversion process using its adjugate matrix. Since A_n is upper triangular, A^T must be lower triangular. That is, $A_{pq} = A_{pq}^T = 0 \quad \forall 1 \leq q < p \leq n$. Now let's consider its adjugate matrix Adj(A). For its lower triangular entires, *i.e.* $1 \leq j < i \leq n$, $\text{Adj}(A)_{ij}$ $=\det(M_{ij}^T)$ $=\det(M_{ji})$, where M_{ji} is the minor matrix of A after removing jth row and ith column. Since $j < i$, A_{ji} is one of the upper triangular entries of A, and eliminating its row and column would necessarily yields $\det(M_{ji})$ $=\text{Adj}(A) = 0$. Since the rest of the inversion process only involves scalar multiplication on each entry, this 0 will carry over to A^{-1}, *i.e.* $A_{ij}^{-1} = 0 \quad \forall 1 \leq j < i \leq n$. Therefore, A^{-1} is upper triangular by definition. When $j = i$, it is easy to see that M_{ji} still has full rank and cannot equal to 0. Hence after nonzero scalar multiplication it is still nonzero. Hence, we establish that A^{-1} is an upper triangular matrix with no zeros on the diagonal, so $A^{-1} \in U_n^*$.

(iii) Let $C = A \times B$, so $c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$. Since A, B are upper triangular, $a_{ik} = 0 \quad \forall i > k$ and $b_{kj} = 0 \quad \forall k > j$. Now consider the lower triangular entries of C, *i.e.* c_{ij} when $i > j$.

$$\begin{aligned} c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} &= \sum_{k=1}^{i-1} a_{ik}b_{kj} + \sum_{k=i}^{n} a_{ik}b_{jk} \\ &= \sum_{k=1}^{i-1} 0 \cdot b_{kj} + \sum_{k=i}^{n} a_{ik} \cdot 0 \\ &= 0 \end{aligned}$$

Hence C is upper triangular. When $i = j$, $c_{ij} = c_{ii} = a_{ii}b_{ii} \neq 0$. Therefore, $C \in U_n^*$.

Then by Theorem 5.14, U_n^* is a subgroup of $GL(n, \mathbb{R})$.

Problem (5.11)**.** No. I_n is the identity of $GL(n, \mathbb{R})$, yet $\det(I_n) = 1 \neq -1$, so $I_n \notin GL(n, \mathbb{R})$. Thus it cannot be a subgroup.

Problem (5.12)**.** Yes. Denote this set as H. Again by assumption $H \subseteq GL(n, \mathbb{R})$. Given $A, B \in H$,

(i) $\det(I_n) = 1 \Rightarrow I_n \in H$.

(ii) $\det(A)\det(A^{-1}) = \det(I_n) = 1 \Rightarrow \det(A^{-1}) = \pm 1 \Rightarrow A^{-1} \in H$.

(iii) $\det(A)\det(B) = \pm 1 = \det(C) \Rightarrow C \in H$.

Hence by Theorem, 5.14, H is a subgroup of $GL(n, \mathbb{R})$.

Problem (5.22)**.** Let $a = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$. Then $a^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and $a^3 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = a$. Therefore,

$$\langle a \rangle = \left\{ \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Problem (5.23)**.** Let $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. $a^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. And by induction we can easy show that $a^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Since $a \in GL(2, \mathbb{R})$, $\langle a \rangle$ is a subgroup by

Theorem 5.17. Thus, $a^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \in \langle a \rangle$ and $(a^n)^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = a^{-n} \in \langle a \rangle$. Putting them together,

$$\langle a \rangle = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \forall n \in \mathbb{Z}.$$

Problem (5.39)**.**

a) True. It's in the definition of a group.

b) False, By the contrapositive of Theorem 4.15, if cancellation law doesn't hold in $(G, *)$, then $(G, *)$ is not a group.

c) True. $G \subseteq G$ under $*$, so it satisfies the definition of a subgroup.

d) False. By definition of an improper subgroup, only G itself is defined as such.

e) False. For the cyclic group $\mathbb{Z}_4$, $\langle 0 \rangle = \{0\} \neq \{0, 1, 2, 3\}$. Hence 0 is not a generator for $\mathbb{Z}_4$.

f) False. In $\mathbb{Z}_4$, both 1 and 3 are generators hence it's not unique.

g) False. $(\mathbb{Z}, +)$ is a group but $(\mathbb{Z}, \times)$ is not a group because $0 \in \mathbb{Z}$ yet it doesn't have an inverse.

h) False. The subset also has to be a group itself.

i) True. 1 is a generator for $\mathbb{Z}_4$.

j) False. Consider $H = (\{1\}, +)$. Clearly $H \subseteq \mathbb{Z}$, yet since the identity $0 \notin H$, H cannot be a subgroup by Theorem 5.14.

Problem (5.44)**.** Consider the empty set $\emptyset$. Since it has no element, it trivially satisfies condition 1 and 3. However, it is not a group since the identity is not in $\emptyset$, so it cannot be a subgroup. Hence, 2 is necessary to exclude this unwanted edge case.

Problem (6.5)**.** Listing all the positive divisors:

$$32 : 1, 2, 4, 8, 16, 32$$
$$24 : 1, 2, 3, 4, 6, 8, 12, 24$$

Clearly $\gcd(32, 24) = 8$.

Problem (6.6). Listing all the positive divisors:

$$48 : 1, 2, 3, 4, 6, 8, 12, 16, 24, 48$$
$$88 : 1, 2, 4, 8, 11, 22, 44, 88$$

Clearly $\gcd(48, 88) = 8$.

Problem (6.9). By Theorem 6.10, all cyclic group of order 8 is isomorphic to $(\mathbb{Z}_8, +_8)$. By Theorem 6.14, we simply need to find the number of elements that are relatively prime with $n = 8$ in $\mathbb{Z}_8$. This yields $\{1, 3, 5, 7\}$. Hence the number of generators is 4.

Problem (6.10). Similarly, the elements of $\mathbb{Z}_{12}$ that is relatively prime with $n = 12$ is $\{1, 5, 7, 11\}$. Hence the number of generators is 4.

Problem (6.17). It is easy to see that $d = \gcd(30, 25) = 5$. By Theorem 6.14, the subgroup contains

$$\frac{n}{d} = \frac{30}{5} = 6$$

elements.

Problem (6.18). Similarly, $d = \gcd(42, 30) = 3$. The subgroup contains:

$$\frac{n}{d} = \frac{42}{3} = 14$$

elements.

Problem (6.20). Notice that $\zeta = \frac{1+i}{\sqrt{2}}$ is in $U_8 \subseteq \mathbb{C}^*$. Additionally, it is a generator of U_8, since $U_8 = \{\zeta^n, 0 \leq n \leq 7\}$. Hence we know this subgroup has 8 elements.

Problem (6.21). Rewrite $1 + i$ in its polar form $a = \sqrt{2}e^{\frac{\pi}{4}i}$ and we can see that $a^n = 2^{\frac{n}{2}}e^{\frac{n\pi}{4}i}$, where the argument is repeating but the modulus keeps growing as n increases. Since $\langle a \rangle$ is a subgroup, the identity a^0 and inverses a^{-n} are all in the subgroup just like Problem 5.23. Therefore, this subgroup is infinite since there is no repeating elements and $n \in \mathbb{Z}$.

Problem (6.32)**.**

a) True. By Theorem 6.1.

b) False. Consider the example in Problem 4.19. It is an abelian group because it is clearly commutative and we proved that it is a group. However, it is not cyclic since the set is uncountable and cannot be isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$.

c) True. Since $\mathbb{Q}$ is countably infinite and has one-to-one correspondence with $\mathbb{Z}$, it is a group and isomorphic to $\mathbb{Z}$ under addition and hence is cyclic.

d) False. In $\mathbb{Z}_4$, $2 \in \mathbb{Z}_4$ is not a generator.

e) True. There exists a group $\mathbb{Z}_n$ for every finite group of order $n > 0$, and we know it is cyclic and therefore abelian.

f) False. The Klein 4 group V_4 is not cyclic yet has an order 4.

g) True. Elements of $\mathbb{Z}_{20}$ that are relatively prime with 20 are $\{3, 7, 11, 13, 17, 19\}$ which are all prime numbers. By Theorem 6.14 they are also generators.

h) False. The binary operation of $G \cap G'$ is ambiguous since G and G' might not have the same operation. Then $G \cap G'$ wouldn't even be well-defined as a group.

i) True. First $H \cap K \subseteq H \subseteq G$. Given $a, b \in H \cap K$,

   (i) Since H, K are subgroups of G, the identity $e_G \in H$ and K, which is equivalent to $e_G = H \cap K$.

   (ii) Since $a \in H \cap K$, a is in both H and K. So $a^{-1} \in H$ and K which is equivalent to $a^{-1} \in H \cap K$.

   (iii) Since H, k are subgroups, $a * b \in H$ and $a * b \in K$, which is equivalent to $a * b \in H \cap K$.

   Hence $H \cap K$ is a subgroup of G.

j) True. Consider all the finite cyclic groups. They are all isomorphic to $\mathbb{Z}_n$ which has at least 1 and a prime between 2 and $n - 1$ as generators for $n \geq 3$. Then for infinite cyclic groups, they are all isomorphic to $\mathbb{Z}$ which has at least 1 and -1 as generators. This covers all cyclic groups.