# Math 3140 - Assignment 2

Due January 31, 2024

(1) Use the Euclidean algorithm to find $\gcd(a, b)$ and Bezout's coefficients $u, v \in \mathbb{Z}$ such that

$$u \cdot a + v \cdot b = \gcd(a, b)$$

for $a = 51, b = 36$.

**Solution:** Starting with the first two lines, iteratively subtract multiples of one line from the previous to get the next

$$\begin{array}{rcll}
& 51 = & 1 * 51 + 0 * 36 & \\
& 36 = & 0 * 51 + 1 * 36 & / * 1 \\
\hline
& 15 = & 1 * 51 - 1 * 36 & / * 2 \\
& 6 = & -2 * 51 + 3 * 36 & / * 2 \\
\gcd(51, 36) = & 3 = & 5 * 51 - 7 * 36 & / * 2 \\
& 0 & \text{remainder} &
\end{array}$$

Bezout's identity occurs in the penultimate line before we get to remainder 0.

(2) Compute the following multiplicative inverses in $\mathbb{Z}_n$ if possible:
(a) $[12]^{-1}$ in $\mathbb{Z}_{35}$
(b) $[14]^{-1}$ in $\mathbb{Z}_{35}$
Hint: Use the Euclidean Algorithm to compute Bezout's coefficients.

**Solution:** In $\mathbb{Z}_{35}$ we get $[12]^{-1} = [3]$ but $[14]^{-1}$ does not exist since $\gcd(14, 35) = 7 \neq 1$.

(3) For $n \in \mathbb{N}$, let $\mathbb{Z}_n^*$ denote the set of elements in $\mathbb{Z}_n$ that have a multiplicative inverse. Show that $(\mathbb{Z}_n^*, \cdot)$ is a group.
Hint: Don't forget to show that $\cdot$ is an operation on $\mathbb{Z}_n^*$, i.e., that the product of invertible elements is invertible again.

**Solution:** (a) $\mathbb{Z}_n^*$ is closed under multiplication: Let $a, b \in \mathbb{Z}_n^*$ have multiplicative inverses $a^{-1}, b^{-1}$, respectively. Then $ab$ has the inverse $b^{-1}a^{-1}$, hence is in $\mathbb{Z}_n^*$ as well.
(b) $\mathbb{Z}_n^* \neq \emptyset$ since it contains the identity [1].
(c) $(\mathbb{Z}_n^*, \cdot)$ is associative because $(\mathbb{Z}, \cdot)$ is (mentioned in class).
(d) For every $a \in \mathbb{Z}_n^*$ there exists $a^{-1} \in \mathbb{Z}_n^*$ since $a$ is the multiplicative inverse of $a^{-1}$.

(4) Let $A, B$ be subgroups of a group $(G, \cdot)$. Show that $A \cap B$ is a subgroup as well.

**Solution:** (a) $A \cap B \neq \emptyset$: Note $1 \in A \cap B$ since $A, B$ are subgroups hence both contain 1.

(b) $A \cap B$ is closed under multiplication: Let $x, y \in A \cap B$. Then $xy \in A$ and $xy \in B$ since both are subgroups. So $xy \in A \cap B$.

(c) $A \cap B$ is closed under inverses: as above.

(5) Determine the center of $\mathrm{GL}(2, \mathbb{R})$.

Hint: Let $E_{ij}$ be the $2 \times 2$ matrix whose $ij$-entry is 1 and all other entries are 0. This is not invertible but their sum with the identity matrix $I + E_{ij}$ is.

Note that $A(I + E_{ij}) = (I + E_{ij})A$ iff $AE_{ij} = E_{ij}A$. Check the latter equations to determine conditions on $a, b, c, d$ such that $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(\mathrm{GL}(2, \mathbb{R}))$.

**Solution:** Following the hint consider $A \cdot E_{12} = E_{12} \cdot A$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}.$$

Equality yields that $a = d$ and $c = 0$.

Dually, multiplying $A$ and $E_{21}$ yields that $a = d$ and $b = 0$.

So any $A$ in $Z(\mathrm{GL}(2, \mathbb{R}))$ is a multiple of the identity matrix $aI_2$ for $a \in \mathbb{R}$. Conversely every $aI_2$ clearly commutes with all matrices. So

$$Z(\mathrm{GL}(2, \mathbb{R})) = \{aI_2 \ : \ a \in \mathbb{R}\}.$$

(6) Prove that every group of even order has an element of order 2.

**Solution:** $A := \{x \in G \ : \ x^{-1} \neq x\}$ can be partitioned into pairs $x, x^{-1}$, hence $|A|$ is even.

Now $G$ is the disjoint union $1 \cup A \cup \{x \in G \ : \ x \text{ has order } 2\}$. Hence

$$|G| \equiv 1 + |\{x \in G \ : \ x \text{ has order } 2\}| \mod 2$$

yields that a group $G$ of even order has an odd number of elements of order 2.

(7) Which of the following groups are cyclic? For those that are, list all their generators. For those that are not, explain why.

$A = (\mathbb{Q}, +)$
$B = (\mathbb{Z}_{12}, +)$
$C = (\mathbb{Z}_7^*, \cdot)$
$D = \{\pi^z \; : \; z \in \mathbb{Z}\}$ under multiplication
$E = \mathbb{Z}^2 = \{(a, b) \; : \; a, b \in \mathbb{Z}\}$ under addition

**Solution:** $A$ is not cyclic: For any $\frac{a}{b} \in \mathbb{Q}$ we have $\langle \frac{a}{b} \rangle = \{\frac{az}{b} \; : \; z \in \mathbb{Z}\} \neq \mathbb{Q}$ since it does not contain e.g. $\frac{a}{2b}$.

$B$ is cyclic with generators $1, 5, 7, 11$.

$C$ is cyclic with generators $3, 5$

$D$ is cyclic with generators $\pi, \pi^{-1}$

$E$ is not cyclic: For any $(a, b) \in \mathbb{Z}^2$ we have $\langle (a, b) \rangle = \{z(a, b) \; : \; z \in \mathbb{Z}\} \neq \mathbb{Z}^2$ since it is contained in a 1-dimensional subspace of $\mathbb{R}^2$.

(8) How many subgroups does $(\mathbb{Z}_{20}, +)$ have? List a generator for each subgroup. Draw a diagram showing the containments between the subgroups.

**Solution:** The subgroup lattice looks like the lattice of divisors of 20 upside down (discussed in class). Something like

$$\langle 1 \rangle$$
$$\langle 2 \rangle \qquad \qquad \langle 5 \rangle$$
$$\langle 4 \rangle \qquad \qquad \langle 10 \rangle$$
$$\langle 0 \rangle$$

There are 6 subgroups (same as the number of divisors of 20).