Math 103A, Modern Algebra I, MT1

Monday, October 21st, 2019, 10-10:50am, APM B402A

- *Your Name*: SOLUTIONS.
- *ID Number*:
- *Section*:

B01 (5:00 PM) B02 (6:00 PM)

Problem #	Points (out of 10)
1	
2	
3	
4	

Total (out of 40):

Problem 1. Recall that $\mathbb{Z}_{13}$ denotes the additive group of all residue classes modulo 13.

(a) Find its cardinality $|\mathbb{Z}_{13}|$.

(b) Compute the following sums in $\mathbb{Z}_{13}$.

$$[7] + [11], \qquad [11] + [12], \qquad [-3] + [17].$$

(Express your answers in the form $[x]$ with x in the range $0 \le x < 13$.)

(c) Give the inverse class of $[6]$ in $\mathbb{Z}_{13}$. More precisely find the $x \in \mathbb{Z}$ in the range $0 \le x < 13$ satisfying the congruence $6 + x \equiv 0 \pmod{13}$.

(a) $|\mathbb{Z}_{13}| = \boxed{13.}$

(b) $\left.\begin{aligned} [7]+[11] &= [18] = [5] \\ [11]+[12] &= [23] = [10] \\ [-3]+[17] &= [14] = [1] \end{aligned}\right\}$ $\boxed{x = 5, 10, 1}$

(c) $-[6] = [-6] = [7]$, $\boxed{x = 7}$.

Problem 2. Recall that $\mathbb{Z}_{13}^{\times}$ denotes the multiplicative group of invertible residue classes modulo 13.

(a) Find its cardinality $|\mathbb{Z}_{13}^{\times}|$.

(b) Compute the following products in $\mathbb{Z}_{13}^{\times}$.

$$[3] \bullet [5], \qquad [5] \bullet [7], \qquad [7] \bullet [-11].$$

(Express your answers in the form $[x]$ with x in the range $0 \leq x < 13$.)

(c) Explain why $[11]$ belongs to $\mathbb{Z}_{13}^{\times}$ and find its inverse class: Find $x \in \mathbb{Z}$ in the range $0 \leq x < 13$ satisfying the congruence $11x \equiv 1 \pmod{13}$.

(a) $|\mathbb{Z}_{13}^{\times}| = \phi(13) = 13 - 1 = \boxed{12}$.

13 is a prime number.

(b)
$$[3] \bullet [5] = [15] = [2]$$
$$[5] \bullet [7] = [35] = [9]$$
$$[7] \bullet [-11] = [-77] = [1]$$
$\boxed{x = 2, 9, 1}$.

(c) $[11] \in \mathbb{Z}_{13}^{\times}$ since $GCD(11, 13) = 1$. We find its inverse using EUCLID:

$$\begin{cases} 13 = 1 \cdot 11 + 2 \\ 11 = 5 \cdot 2 + 1 \end{cases}$$

Back-substitution:

$1 = 11 - 5(13 - 11) = (-5)13 + 6 \cdot 11$

– shows: $11 \cdot 6 \equiv 1 \pmod{13}$

x.

Conclude $[11]^{-1} = [6]$.

– So, $\boxed{x = 6}$.

Problem 3. Let F denote the set of all numbers of the form $a + b\sqrt{3}$ with rational coefficients $a, b \in \mathbb{Q}$. Let $F^{\times} = F - \{0\}$ be the nonzero numbers.

(a) Explain why addition and multiplication $\bullet$ define composition laws on F.

(b) Check that $(F, +)$ and $(F^{\times}, \bullet)$ are groups. Give all details.

(c) Compute the multiplicative inverse of $1 + 2\sqrt{3}$. Find $a, b \in \mathbb{Q}$ such that

$$(1 + 2\sqrt{3})^{-1} = a + b\sqrt{3}.$$

(fractions)

(a) Let $x = a + b\sqrt{3}$ and $y = c + d\sqrt{3}$ with $a, b, c, d \in \mathbb{Q}$.

– Must show $x+y$ and xy have the <u>same</u> form:

- $x + y = \underbrace{(a+c)}_{\in\mathbb{Q}} + \underbrace{(b+d)}_{\in\mathbb{Q}}\sqrt{3}$, belongs to F ✓

- $xy = (a+b\sqrt{3})(c+d\sqrt{3}) = \underbrace{(ac+3bd)}_{\in\mathbb{Q}} + \underbrace{(ad+bc)}_{\in\mathbb{Q}}\sqrt{3}$

  – belongs to F ✓

(b) $(F, +)$ is a group:

- $(x+y)+z = x+(y+z)$
- $0 = 0 + 0\sqrt{3}$ is in F.
- $-x = \underbrace{(-a)}_{\in\mathbb{Q}} + \underbrace{(-b)}_{\in\mathbb{Q}}\sqrt{3}$ is in F.

(for any three $x, y, z \in F$).

– continued →

$(F^\times, \bullet)$ is a group:

- $(xy)z = x(yz)$
- $1 = 1 + 0\sqrt{3}$ is in F.

The KEY POINT $\to$ When $x = a + b\sqrt{3} \in F$ is nonzero, $\frac{1}{x} \in F$:

Indeed,

$$\frac{1}{x} = \frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{(a+b\sqrt{3})(a-b\sqrt{3})} = \frac{a-b\sqrt{3}}{a^2-3b^2}$$

$$= \underbrace{\frac{a}{a^2-3b^2}}_{\in \mathbb{Q}} + \underbrace{\frac{-b}{a^2-3b^2}}_{\in \mathbb{Q}}\sqrt{3}$$

rational coefficients.

visibly belongs to F.

(c) For instance,

$$(1+2\sqrt{3})^{-1} = \frac{1-2\sqrt{3}}{(1+2\sqrt{3})(1-2\sqrt{3})} = \frac{1-2\sqrt{3}}{1-3\cdot 4}$$

$$= \frac{-1}{11} + \frac{2}{11}\sqrt{3}.$$

a   b

$$\boxed{a = \frac{-1}{11} \quad b = \frac{2}{11}}.$$

Problem 4. Let $(G, *)$ be a group. Two elements $a, b \in G$ are *conjugate* when one can write $b = g * a * g^{-1}$ for some $g \in G$. If so we write $a \sim b$.

(a) Find all $a \in G$ satisfying $a \sim e$ (where e is the neutral element).

(b) Prove that $\sim$ gives an equivalence relation on G. Check these properties:

(i) $a \sim a$

(ii) $a \sim b \Longleftrightarrow b \sim a$

(iii) $a \sim b$ and $b \sim c \Longrightarrow a \sim c$

for any three elements $a, b, c \in G$.

(c) Are the two matrices $\left(\begin{smallmatrix} 1 & 2 \\ 3 & \pi \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \pi & 1 \\ 2 & 3 \end{smallmatrix}\right)$ conjugate in $\mathrm{GL}_2(\mathbb{R})$?

(a) $a \sim e$ means $a = \underbrace{g * e * g^{-1}}_{\text{equals } g * g^{-1} = e.}$ for some $g \in G$.

— conclude: Only $\boxed{a = e}$ satisfies $a \sim e$.

(b) (i) $a \sim a$ since $a = e * a * e^{-1}$ (take $g = e$)

(ii) $a \sim b$ means $b = g * a * g^{-1}$ for some $g \in G$.

Then $a = g^{-1} * b * g = g^{-1} * b * (g^{-1})^{-1}$.

(and vice versa) "new" g.

(iii) $a \sim b$ and $b \sim c$ means $\exists g, h \in G$:

$b = g * a * g^{-1}$ and $c = h * \underset{b}{a} * h^{-1}$.

— Combined:

~~$b = g *$~~

$c = h * (g * a * g^{-1}) * h^{-1}$

By "socks & shoes" $(h * g)^{-1} = g^{-1} * h^{-1}$.

$= \underbrace{(h * g)} * a * \underbrace{(h * g)}^{-1}$

~ continued →

(c) No, $\overset{\displaystyle a}{\overset{\|}{\begin{pmatrix} 1 & 2 \\ 3 & \pi \end{pmatrix}}}$ and $\overset{\displaystyle b}{\overset{\|}{\begin{pmatrix} \pi & 1 \\ 2 & 3 \end{pmatrix}}}$ are <u>not</u> conjugate in $GL_2(\mathbb{R})$ since they have different <u>traces</u>:

$$\mathrm{tr}(a) = 1+\pi \neq \mathrm{tr}(b) = \pi + 3.$$

[Recall from <u>linear</u> <u>algebra</u>: $\forall g \in GL_N(\mathbb{R})$

$$\mathrm{tr}(gag^{-1}) = \mathrm{tr}(a)$$

– represent the same linear transformation with respect to different <u>bases</u>.

conjugation $\longleftrightarrow$ change-of-basis.]