3ZWYL

$GL(n, \mathbb{F})$: matrices of size $n \times n$ w/ elements from $\mathbb{F}$

$GL(2, \mathbb{R}) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc \neq 0$

$SL(n, \mathbb{F})$ = $GL(n, \mathbb{F})$, but only matrices w/ determinant 1
$ad - bc = 1$

negate

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

switch

Aside: [matrix] | det | $\begin{bmatrix} a \\ b \end{bmatrix}$ (a, b) / $\langle a, b \rangle$

$[c, d] = \begin{bmatrix} c \\ d \end{bmatrix}^T$ $[a, b]$

Prop's of Groups

1) Identity is unique
2) Cancellation is OK

$ab = ac$ Consider $a^{-1} \in G$

$\underbrace{a^{-1}a}b = \underbrace{a^{-1}a}c$

$eb = ec$

$b = c$ ✓

If group operation is not known to be abelian then operation is written as:

ab or $a \cdot b$

if abelian $a + b$

3) Inverses are unique

③

$(1-2)-3 = -4$

#2 $a-b-c$

$(a-b)-(c)$

$(a)-(b-c)$

$-1-(-2+3) = -2$

#5 $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}^{-1}$ in $\underline{GL(2, \mathbb{Z}_{11})}$

$\dfrac{1}{\underline{2\cdot 5 - 3\cdot 6}} \cdot \begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix} = -\dfrac{1}{8} \begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix}$

$-8 \equiv 3 \pmod{11}$

$3+8 = 11 \equiv 0 \pmod{11}$

#8 Show that $\{5, 15, 25, 35\}$ is a group with mult. mod 40

identity

$35^2 \bmod 40 \equiv 35$

$5 \cdot 35 = 175 = 15$

#9 Ans (e)

Aside If the gcd $(m, n) = d$ then it is always possible to write $d = am + nb$

If p, q are prime, then $1 = ap + qb$

12) $n > 2$ Show that there are at least 2 elements in $U(n)$ $\ni$ $x^2 = 1$

Claim: 2 elements are $1, n-1$

$(n-1)^2 = \cancel{n^2} - 2\cancel{n} + 1 \equiv 1 \pmod{n}$

#16 $(ab)^{-1} = ?$ $\quad \begin{cases} a^{-1}b^{-1} \\ \underline{b^{-1}a^{-1}} \end{cases} ?$

$(ab)(a^{-1}b^{-1}) = e$

$(ab)(b^{-1}a^{-1}) = a(\underbrace{bb^{-1}}_{e})a^{-1} = \underbrace{aa^{-1}}_{e} = e$

If $\langle G, * \rangle$ is a group

order of G (elements in G) written $|G|$

$|\{g : g \in G\}| = n$

Elements have their own orders:

$g^n = e$ we say $|g| = n$ if n is smallest integer for which this true