Midterm 1 MAT4233.001 Sp. 2013

1. $\det \begin{bmatrix} 7 & 1 \\ 4 & 5 \end{bmatrix} = 35-4 = 31 \equiv 9 \bmod 11$

$\gcd(9, 11) = 1$, so 9 is invertible in $\mathbb{Z}_{11}$, so the matrix is invertible

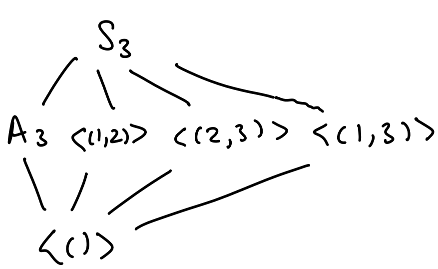
We need 9^{-1} in $\mathbb{Z}_{11}$: Euclid's algorithm:

Div. alg.	Solve for remainders
$11 = 9 + 2$	$2 = 11 - 9$
$9 = 4 \cdot 2 + 1$	$1 = 9 - 4 \cdot 2 = 9 - 4(11-9) = 5 \cdot 9 - 4 \cdot 11$

$\therefore\ 9^{-1} \equiv 5 \bmod 11$

$$\therefore \begin{bmatrix} 7 & 1 \\ 4 & 5 \end{bmatrix} = 5 \cdot \begin{bmatrix} 5 & -1 \\ -4 & 7 \end{bmatrix} = \begin{bmatrix} 25 & -5 \\ -20 & 35 \end{bmatrix} = \begin{bmatrix} 3 & 6 \\ 2 & 2 \end{bmatrix}$$

2. Subgroups: $\langle () \rangle = \{ () \}$ (trivial)



$\langle (1,2) \rangle = \{ (), (1,2) \}$

+ 2 other similar ones

$A_3 = \langle (1,2,3) \rangle = \{ (), (1,2,3), (1,3,2) \}$

Non-trivial left cosets of $\langle (1,2) \rangle$

$(1,3)\langle (1,2) \rangle = \{ (1,3), (1,3)(1,2) \} = \{ (1,3), (1,2,3) \}$

$(2,3)\langle (1,2) \rangle = \{ (2,3), (2,3)(1,2) \} = \{ (2,3), (1,3,2) \}$

Right:

$\langle (1,2) \rangle (1,3) = \{ (1,3), (1,2)(1,3) \} = \{ (1,3), (1,3,2) \}$

$\langle (1,2) \rangle (2,3) = \{ (2,3), (1,2)(2,3) \} = \{ (2,3), (1,2,3) \}$

3. First assume $n \geq 0$. Induction on n:

Basis $n=0$: $(ab)^0 = e$ $\quad a^0 b^0 = e \cdot e = e$

If $n > 1$ $\quad (ab)^n = (ab)^{n-1}\, ab =$

$$\underset{\text{By induction}}{=} a^{n-1} b^{n-1} ab \underset{\text{abelian}}{=} a^{n-1} a\, b^{n-1} b = a^n b^n$$

If $n < 0$, Let $n = -k$, where $k > 0$.

Then $(ab)^n = (ab)^{-k} = ((ab)^{-1})^k \overset{\text{socks/shoes}}{=} (b^{-1}a^{-1})^k =$

$$= (b^{-1})^k (a^{-1})^k \underset{\text{previous case}}{=} b^{-k} a^{-k} \underset{\text{abelian}}{=} a^{-k} b^{-k} = a^n b^n$$

<u>Counterexample</u>.

Let $G = S_3$ $\quad a = (1,2)$ $\quad b = (2,3)$

then $(ab)^2 = ((1,2)(2,3))^2 = (1,2,3)^2 = (1,3,2)$

but $a^2 b^2 = () \cdot () = ()$

4. Suppose $p \neq q$ are primes in H.

Then $\gcd(p,q) = 1$, so $\exists s,t \in \mathbb{Z}$ $\quad sp + tq = 1$

$\therefore 1 \in H$ $\quad \therefore \forall n \in \mathbb{Z}$ $\quad n \cdot 1 \in H$

5. hom: $\varphi(j+k) = a^{j+k} = a^j \cdot a^k = \varphi(j)\varphi(k)$

Since $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$, by inspection φ is surjective.

φ is injective $\Leftrightarrow$ $\ker \varphi$ is trivial $\Leftrightarrow$ $\forall n \neq 0$ $\varphi(n) \neq e$ $\Leftrightarrow$

$\Leftrightarrow$ $\forall n \neq 0$ $a^n \neq e$ $\Leftrightarrow$ $|a| = \infty$