12.21

Group 4 [Th 11.20]: K Hwang; L Jones; L Kenny; A Leeman (with special guest BRIAN D.)

Define $\varphi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

Then $\varphi((a+bi)(c+di)) = \varphi((ac-bd)+(ad+bc)i) = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$

$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \varphi(a+bi)\varphi(c+di)$$

From this we know the relation is homomorphic.

Next, to prove 1:1 relationship, suppose $a+bi = c+di$.

But, we know $\varphi(a+bi)\varphi(c+di)$.

Then $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$.

Therefore $a = c$ & $b = d$ so that $a+bi = c+di$, but this is a contradiction.

Thus, the relation is 1:1.

Next, for any $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in H$ there exists some $a+bi \in G$ such that

$$\varphi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Thus, the relation is onto.

Group 6: Problem 12.29 (taken in steps)

Let $G = \langle a \rangle$, $|G| = p$, a prime

For $1 \le n \le p-1$, consider $\phi_n : G \to G$ with $\phi(x) = x^n$

Claim 1: ϕ_n is an automorphism, since $(n, |G|) = 1$. (Exer 12.20).

Claim 2: If $1 \le m, n \le p-1$ and $m \neq n$, $\phi_n \neq \phi_m$.

Pf: Just suppose $\phi_n = \phi_m$, so $\phi_n(a) = \phi_m(a)$.

Therefore $a^n = a^m$, and by Theorem 4.5, $m \equiv n \pmod{p}$,

but $1 \le m, n \le p-1$. ※. Thus $\phi_n \neq \phi_m$.

Claim 3: If $\phi : G \to G$ is an automorphism, then $\phi = \phi_n$ for some $1 \le n \le p-1$.

Pf: Fix the elements of $G = \{e, a, a^2, \cdots a^{p-1}\}$.

Consider $\phi : G \to G$ such that $\phi(a) = a^n$, $1 \le n \le p-1$.

Fix $a^j \in G$, $1 \le j \le p-1$. Consider $\phi(a^j) = (\phi(a))^j$ by 12.4(ii).

$(\phi(a))^j = (a^n)^j = (a^j)^n$, and since a^j is an arbitrary element of G.

$\phi = \phi_n$. Now just suppose $\phi(a) = e = a^0$, but then ϕ sends every element to e and ϕ is not an automorphism.

So, a cyclic group, G, of order p a prime has