4.3 #3 Let $a, b \in G$, then $(ab)^2 = e$

so $abab = e$

Multiplying by $a$ on the left and $b$ on the right we get:

$aaabbb = aee$

$a^2 (ba) b^2 = agb$

$c (ba) e = ab$

$a ba = ab$ so $G$ is abelian

4.3 #4: closure holds since $a \ast b = ac^{-1}b \in G$

Associativity $(x \ast y) \ast z = (xc^{-1}y) \ast z = xc^{-1}y z$

$x \ast (y \ast z) = x c^{-1}(y \ast z) = x c^{-1}(yc^{-1}z) = (x \ast y) \ast z$

Identity $x \ast c = xc^{-1}c = x$ for all $x \in G$ so $c$ is the identity (Also $c \ast x = c c^{-1} x = ee = c$)

Inverse Given $x \in G$ take $z = cx^{-1}c$

Then $x \ast z = x c^{-1} c x^{-1} c = xx^{-1}c = ec = c$

and $z \ast x = cx^{-1} c^{-1} x = c x^{-1} ex = c x^{-1} x = ce = c$.

So $c x^{-1} c$ is the inverse of $x$.

So $G$ is a group under $\ast$.

4.3 #5 Let $J = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ then $G = \{aJ\}$ and $J = 3J$.

Let $X = xJ$ then $AX = aXJ = 3axJ = xJ$  

$3a = 1$ so $a = \frac{1}{3}$

We then get also $XA = x, \frac{1}{3}J = x, \frac{1}{3}J = xJ = X$.

So $A = \frac{1}{3} J$

$G$ satisfies closure and associativity since $aJ, bJ = abJ^2 = 3abJ \in G$ and matrix multiplication is associative, $A = \frac{1}{3} J$ is the identity and the inverse of $xJ$ is $\frac{1}{x}J$ since $xJ, \frac{1}{x}J = \frac{1}{x}J^2$

$= \frac{1}{3} J = \text{identity}$.
7. \( D(4) = \{ e, s, s^2, s^3, R, sR, s^2R, s^3R \mid R^2 = s^4 = e, R_s = s^3R \} \)

**Multiplication Table for \( D(4) \)**

<table>
<thead>
<tr>
<th></th>
<th>( e )</th>
<th>( s )</th>
<th>( s^2 )</th>
<th>( s^3 )</th>
<th>( R )</th>
<th>( sR )</th>
<th>( s^2R )</th>
<th>( s^3R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( e )</td>
<td>( e )</td>
<td>( s )</td>
<td>( s^2 )</td>
<td>( s^3 )</td>
<td>( R )</td>
<td>( sR )</td>
<td>( s^2R )</td>
<td>( s^3R )</td>
</tr>
<tr>
<td>( s )</td>
<td>( s )</td>
<td>( s^2 )</td>
<td>( s^3 )</td>
<td>( e )</td>
<td>( sR )</td>
<td>( s^2R )</td>
<td>( s^3R )</td>
<td>( R )</td>
</tr>
<tr>
<td>( s^2 )</td>
<td>( s^2 )</td>
<td>( s^3 )</td>
<td>( s )</td>
<td>( R )</td>
<td>( sR )</td>
<td>( s^2R )</td>
<td>( s^3R )</td>
<td>( e )</td>
</tr>
<tr>
<td>( s^3 )</td>
<td>( s^3 )</td>
<td>( e )</td>
<td>( s^2 )</td>
<td>( s^3R )</td>
<td>( sR )</td>
<td>( s^2R )</td>
<td>( e )</td>
<td>( R )</td>
</tr>
<tr>
<td>( R )</td>
<td>( R )</td>
<td>( R )</td>
<td>( R )</td>
<td>( R )</td>
<td>( R )</td>
<td>( R )</td>
<td>( R )</td>
<td>( R )</td>
</tr>
<tr>
<td>( sR )</td>
<td>( sR )</td>
<td>( sR )</td>
<td>( sR )</td>
<td>( sR )</td>
<td>( sR )</td>
<td>( sR )</td>
<td>( sR )</td>
<td>( sR )</td>
</tr>
<tr>
<td>( s^2R )</td>
<td>( s^2R )</td>
<td>( s^2R )</td>
<td>( s^2R )</td>
<td>( s^2R )</td>
<td>( s^2R )</td>
<td>( s^2R )</td>
<td>( s^2R )</td>
<td>( s^2R )</td>
</tr>
<tr>
<td>( s^3R )</td>
<td>( s^3R )</td>
<td>( s^3R )</td>
<td>( s^3R )</td>
<td>( s^3R )</td>
<td>( s^3R )</td>
<td>( s^3R )</td>
<td>( s^3R )</td>
<td>( s^3R )</td>
</tr>
</tbody>
</table>
4.4 #12  First notice that if \((r, s) \sim (t, u)\) then \(ru = ts\) and since \(s, u \neq 0\) \(r = 0 \iff t = 0\).

\(\sim\) is reflexive since \(rs = rs\) so \((r, s) \sim (r, s)\)

\(\sim\) is symmetric since \((r, s) \sim (t, u) \iff ru = st \iff ts = ur \iff (t, u) \sim (r, s)\)

\(\sim\) is transitive: Suppose \((r, s) \sim (t, u)\) and \((t, w) \sim (v, w)\).

By the remark at the beginning we know that \(r = 0 \iff t = 0 \iff v = 0\).

Case 1: \(r = 0\) then \(t = 0\), \(v = 0\) so \(rw = sv = 0\) and \((r, s) \sim (v, w)\).

Case 2: \(r \neq 0\) then \(t \neq 0\) and \(v \neq 0\). We also have \(s \neq 0\), \(u \neq 0\).

Since \((r, s) \sim (t, u)\) we get \(ru = st\)

Since \((t, u) \sim (v, w)\) we get \(tw = uv\)

So \(ru + tw = st + uv\)

By the axioms of arithmetic \((rw - sv) = 0\) and since we are in an integral domain there are no zero divisors and since \(u \neq 0\), \(t \neq 0\)

\(rw - sv = 0 \Rightarrow rw = sv \Rightarrow (r, s) \sim (v, w)\).

Since the relation \(\sim\) is reflexive, symmetric and transitive it is an equivalence relation.

**Addition of equivalence classes is well defined**

We need to show \((r, s) \sim (r', s')\) and \((t, u) \sim (t', u')\)

\((r, s) + (t, u) \sim (r', s') + (t', u')\)

1. \((ru + st, su) \sim (ru' + st', s'u')\)
2. \((ru + st) s'u' = su\ (ru' + st')\)
3. \(rus'u' + st s'u' = su(r'u' + s't')\)

We know \(rs' = r's\) and \(tu' = ut'\)

So \(rus'u' + st s'u' = (rs')uu' + (tu')ss' = r's uu' + ut'ss' = su r'u' + su s't'\)
Multiplication of equivalence classes is well defined

We need to show \((r, s) \sim (r', s')\) and \((t, u) \sim (t', u')\) \(\Rightarrow\)

\((r, s)(t, u) = (r', s')(t', u')\) or

\((rt, sw) = (r't', s'u')\) \(\Rightarrow \) \(rt's'u' = su'r'\)

But we know \(rs' = rs\) and \(tu' = ut'\) so

\(rt's'u' = (rs')(tu') = (rs)(ut') = su'r'\)

Addition is associative

\([\{(r, s) + (t, u)\} + (v, w)] = (ru + st, su) + (v, w) =\]

\((ru + st, su + vs)\) \(\Rightarrow \)

\((r, s) + \{(t, u) + (v, w)\} = (r, s) + \{(tu + uv, uw)\} =\]

\((ru + st, su + uv, suw) = [(ru + st, sw) + vs + uv, suw]\)

Addition is commutative

\((r, s) + (t, u) = (ru + st, su) = (ts + ur, us) = (tu) + (rs)\)

\((0, 1)\) is an identity for addition

\((r, s) + (0, 1) = (r + 1 + s, 0, s, 1) = (r, s)\)

\((-r, s)\) is the additive inverse for \((r, s)\)

\((r, s) + (-r, s) = (rs - sr, s^2) = (0, s^3) = (0, 1)\) since \(0 = 0\).

Multiplication is associative

\[\{(r, s)(t, u)\} \{(v, w)\} = (rt, su) \{(v, w)\} = (rtv, suw)\]

\[\{(t, u) \{(v, w)\}\} = (r, s) \{(tv, uw)\} = (rtv, suw)\]

Multiplication is commutative

\((r, s)(t, u) = (rt, su) = (tr, us) = (t, u)(r, s)\)

Multiplication is distributive with respect to addition

(Since multiplication is commutative we need to check only one distributive law.)
\[(r, s)(t, w + (r, s)w) = (r, s)(tw + uv, sw) = r(tw + uv), sww) = (rtw + ruv, sww)\]

\[(r, s)(t, w) + (r, s)(r, s)w = (rt, sw) + (rv, sw) = \]
\[\begin{align*}
    (rtsw + surv, s^2uw) &\sim (rtw + ruv, sww) \sim uv \\
    (rtsw + surv) sww &\sim s^2uw (rtw + ruv) \\
    rts^2uw^2 + s^2utvw + rvw &\sim s^2rtuw^2 + ru^2s^2vw
\end{align*}\]

\((1, 1)\) is a multiplicative identity

\((r, s)(1, 1) = (r, 1, s, 1) = (r, s)\)

So \(Q\) is a commutative ring with identity under

\[\text{the operation}\]

\[\text{Inverse: Let } (r, s) \neq (0, 1), r \neq 0 \]

\[\text{then } (r, s)(s^{-1}) = (rs, sr) \sim (1, 1)\]

So every non-zero element of \(Q\) has an inverse.

\(Q\) is a field.

\[\text{Note that if } R = \mathbb{Z} \text{ we get the set of all fractions } \frac{r}{s} \text{ where } s \neq 0 \text{ with } \sim \text{ meaning that the fractions are equivalent and } + \text{ and multiplication in } Q \text{ are ordinary addition and multiplication of fractions.}\]

If \(R = \mathbb{Z}[x]\) the set of polynomials with integer coefficients then \(Q\) is the field of rational fractions \(\frac{p(x)}{q(x)}\).