INTRO TO GROUP THEORY - APR. 4, 2012
SOLUTION SET 9 - GT13/14. ORDER 8/ SEMIDIRECT PRODUCTS

1. We can narrow the possibilities for each G by checking for abelian and counting elements of order 2:

(1) $G = \{1, 3, 5, 7, 9, 11, 13, 15\}$ is abelian with 3 elements of order 2, so $G \cong \mathbb{Z}/2 \times \mathbb{Z}/4$.
(2) First
$$(\mathbb{Z}/24)^* \cong (\mathbb{Z}/3)^* \times (\mathbb{Z}/8)^* \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$
Alternatively $G = \{1, 5, 7, 11, 13, 17, 19, 23\}$. Verify: each element satisfies $x^2 = 1$.
(3) Each element of $P(\{1, 2, 3\})$ satisfies $x^2 = \emptyset$, so $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.
(4) $G = \{(12)(34), (12), (34), (1324), (1423), (12), (34), (13)(24), (14)(23)\} \cong D_8$. Non-abelian with 5 elements of order 2.
(5) $G \cong D_8$ again.
(6) The generators have order 4 and distinct inverses. The product is another element of order 4, giving six elements of order 4, so $G \cong Q$. Of course, one should verify that the group generated has eight elements and construct the isomorphism.
(7) By GT12.1, $G \cong D_8$.
(8) By GT12.1, $G \cong (\mathbb{Z}/8)^*/\{\pm 1\} \times \mathbb{Z}/2$, so $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.
(9) By GT12.1, $G \cong D_8$.
(10) G is non-abelian and has 5 elements of order 2, so $G \cong D_8$. Of course, you should construct the isomorphism.

2. (a) If $\mathbb{Z}/3$ normal in G: the only homomorphism from $\mathbb{Z}/5$ to $(\mathbb{Z}/3)^* \cong \mathbb{Z}/2$ is trivial. Thus $G = \mathbb{Z}/5 \times \mathbb{Z}/3 \cong \mathbb{Z}/15$.

If $\mathbb{Z}/5$ normal in G: likewise, the only homomorphism from $\mathbb{Z}/3$ to $(\mathbb{Z}/5)^* \cong \mathbb{Z}/4$ is trivial. Thus $G \cong \mathbb{Z}/15$.

(b) If $\mathbb{Z}/4$ normal in G: the only homomorphism from $\mathbb{Z}/3$ to $(\mathbb{Z}/4)^* \cong \mathbb{Z}/2$ is trivial. Thus $G = \mathbb{Z}/3 \times \mathbb{Z}/4 \cong \mathbb{Z}/12$.

If $\mathbb{Z}/3$ normal in G: there is a non-trivial homomorphism from $\mathbb{Z}/4$ to $(\mathbb{Z}/3)^* \cong \mathbb{Z}/2$. That is, $\pi(1) = \pi(3) : 1 \mapsto 2, 2 \mapsto 1$.

This group is new! It is easier to describe with generators and relations:
$$y^4 = e,\ x^3 = e,\ yxy^{-1} = x^2.$$
Note that G is non-abelian and has four elements of order 4 (verify), so G is not A_4 or D_{12}.

(c) If we use a trivial homomorphism, $G = \mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \cong \mathbb{Z}/6 \times \mathbb{Z}/2$.

Date: April 6, 2012.

If $\mathbb{Z}/2 \times \mathbb{Z}/2$ normal in G: there are two non-trivial homomorphisms from $\mathbb{Z}/3$ to

$$Aut(\mathbb{Z}/2 \times \mathbb{Z}/2) \cong S_3.$$

It is enough to note that these automorphisms fix no labels in S_3 (or non-identity elements in $\mathbb{Z}/2 \times \mathbb{Z}/2$). For instance,

$$\pi(1,0) = (0,1),\ \pi(0,1) = (1,1),\ \pi(1,1) = (1,0).$$

Later we will see that either non-trivial automorphism leads to a group isomorphic to A_4, but of course you can convince yourself by computing orders of elements or constructing the isomorphism.

If $\mathbb{Z}/3$ normal in G: there exists three non-trivial homomorphisms from $\mathbb{Z}/2 \times \mathbb{Z}/2$ to $(\mathbb{Z}/3)^* \cong \mathbb{Z}/2$. Each case leads to $S_3 \times \mathbb{Z}/2$, which is isomorphic to D_{12}.

(d) If $\mathbb{Z}/3$ is normal in G: the only homomorphism from $\mathbb{Z}/7$ to $(\mathbb{Z}/3)^* \cong \mathbb{Z}/2$ is trivial, so $G \cong \mathbb{Z}/21$ in this case.

If $\mathbb{Z}/7$ normal in G: there are two non-trivial homomorphisms from $\mathbb{Z}/3$ to $(\mathbb{Z}/7)^* \cong \mathbb{Z}/6$. The elements of order 3 in $(\mathbb{Z}/7)^*$ are 2 and 4 (verify), so we have two possibilities. Using generators and relations, these are given as:

$$y^3 = e,\ x^7 = e,\ yxy^{-1} = x^2, \qquad \text{and} \qquad t^3 = e,\ s^7 = e,\ tst^{-1} = s^4.$$

3. We have already seen that $|Aut(G)| = 24$, and $Inn(Q) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. The inner automorphisms are characterized as those that fix the labels i, j, k but possibly with an even number of sign changes. We can find automorphisms of order three given by

$$\pi :\ i \mapsto j,\ j \mapsto k,\ k \mapsto i, \qquad \text{and} \qquad \pi^{-1} : i \mapsto k,\ j \mapsto i,\ k \mapsto j,$$

and we have a subgroup of order 3. Computing shows that we have a subgroup H of $G = Aut(Q)$ isomorphic to A_4. One constructs the isomorphism as a semidirect product of $\mathbb{Z}/3$ and $\mathbb{Z}/2 \times \mathbb{Z}/2$, and this subgroup is characterized as the automorphisms that permute the set $\{i, j, k\}$ with an even number of sign changes.

Since $H \triangleleft G$ by the Index Two Theorem, we may consider the homomorphism

$$\omega : G \to Aut(H) \cong S_4$$

given by conjugation. Since $Z(H)$ is trivial, ω maps H onto $Inn(H) \cong A_4$. Thus one need only verify that one element not in $G \backslash H$, say $\pi' : i \mapsto -i,\ j \mapsto k,\ k \mapsto j$, is not in the kernel of ω. We leave this to the reader.

Since $Out(G) = Aut(G)/Inn(G) \cong S_3$, the elements of a given coset are the automorphisms that yield the same permutation of $\{i, j, k\}$ when the signs are removed.

4. (a) As a set, the semidirect product equals $\mathbb{Z}/3 \times \mathbb{Z}/7$ and is generated by $(1, 0)$ (order 3) and $(0, 1)$ (order 7), and we build the multiplication using the automorphism $\pi(m) = 2m$:

$$(1,0)(0,1)(2,0) = (0,2) \quad \text{or} \quad (0,1)(2,0) = (2,2).$$

To construct an isomorphism, we define

$$\pi(1,0) = y, \qquad \pi(0,1) = x$$

and extend homomorphically. Note

$$yxy^{-1} = \pi(1,0)\pi(0,1)\pi(2,0) = \pi((1,0)(0,1)(2,0))\pi((1,0)(2,2)) = \pi(0,2) = x^2.$$

This map is a bijection preserving the relations, so π is an isomorphism.

(b) If we show there are fourteen elements of order 3, then the remaining seven elements are clearly identitfied. Now

$$(yx^k)^3 = yx^kyx^kyx^k = yx^ky^2x^{2k}x^k = y^3x^{4k}x^{3k} = ex^{7k} = e,$$

but this element cannot have order 2 since $|G| = 21$. A similar computation holds for elements of the form x^2y^k. This gives $2 \times 7 = 14$ elements of order 3.

(c) If π is an automorphism, it is determined by values on x and y. There are 6 choices for x and 14 choices for y based on order. So there is a maximum of 84 automorphisms. In fact, we show that there are 42 automorphisms. To restrict these choices, π must preserve the relation

$$yxy^{-1} = x^2, \qquad \text{or} \qquad \pi(y)\pi(x)\pi(y^{-1}) = \pi(x^2).$$

If we choose $\pi(y) = y^ix^j$ and $\pi(x) = x^k$, then

$$y^ix^jx^kx^{-j}y^{-i} = x^{2k} \qquad \text{or} \qquad y^ix^ky^{-i} = x^{2k}.$$

If $i = 1$, this is always true. On the other hand, if $i = 2$, then $x^{4k} = x^{2k}$, or $x^{2k} = e$. Since $|x| = 7$, k is a multiple of 7, which does not work. This gives $7 \times 6 = 42$ automorphisms.

If one shows that $Z(G) = \{e\}$, then $Inn(G) \cong G$, and $Out(G) \cong \mathbb{Z}/2$. More later.

5. (a) We consider all homomorphisms $\pi : \mathbb{Z}/p \to (\mathbb{Z}/q)^* \cong \mathbb{Z}/(q-1)$. If trivial, then $G \cong \mathbb{Z}/pq$.

To be non-trivial, p must divide $q-1$, or $q = kp+1$ for some integer k, and, in this case, we need to identify the elements of order p in $(\mathbb{Z}/q)^*$. In the group $\mathbb{Z}/(q-1)$, these lie in the subgroup $\langle (q-1)/p \rangle$. If these are given by $\{l\}$ in $(\mathbb{Z}/q)^*$, then $\pi_l(m) = lm$. Then one may follow the argument in Problem 4(a): the key identity is

$$(1,0)(0,1)(p-1,0) = (0,l) \quad \text{or} \quad (0,1)(p-1,0) = (p-1,l).$$

(b) As before, the semidirect product has elements $\mathbb{Z}/p \times \mathbb{Z}/q$ with generators $(1,0)$ (order p) and $(0,1)$ (order q). We build the multiplication using $(1,0)(0,1)(p-1,0) = (0,l)$ or $(0,1)(p-1,0) = (p-1,l)$. To construct an isomorphism, we define

$$\pi(1,0) = y, \qquad \pi(0,1) = x$$

and extend homomorphically. Note

$$yxy^{-1} = \pi(1,0)\pi(0,1)\pi(p-1,0) = \pi((1,0)(0,1)(p-1,0))\pi((1,0)(p-1,l)) = \pi(0,l) = x^l.$$

This map is a bijection preserving the relations, so π is an isomorphism.

(c) As before, we show the elements $y^i x^j$ have order p. Now

$$(yx^k)^p = yx^k \dots yx^k yx^k = yx^k \dots y^2 x^{kl} x^k = y^p x^{k+lk+l^2k+l^3k+\cdots+l^{p-1}k} = ex^E = e,$$

where

$$E = k(1 + l + l^2 + \cdots + l^{p-1}) = k(1 - l^p)/(1 - l) = 0.$$

This holds since l is an element of order p. For general $y^i x^k$ $(0 < i \leq p-1)$, we modify

$$E = k + kl^i + kl^{2i} + \cdots + kl^{i(p-1)} = k(1 - l^{ip})/(1 - l^i) = 0.$$

Thus there are $q(p-1)$ elements of order p, and the result follows.

(d) As before, with $q-1$ choices for x and $q(p-1)$ choices for y, there are at most $q(q-1)(p-1)$ automorphisms of G. Suppose $\pi(y) = y^i x^j$ and $\pi(x) = x^k$ $(0 < i \leq p-1,\ 0 < k \leq q-1)$. We limit these choices by using the relation

$$\pi(y)\pi(x)\pi(y^{-1}) = \pi(x^l), \quad \text{or} \quad y^i x^j x^k x^{-j} y^{-i} = y^i x^k y^{-i} = x^{lk}, \quad \text{or} \quad x^{kl^i} = x^{lk}.$$

Now we need to solve $kl^i = lk \pmod q$. If $i = 1$, any k works, and we have $q(q-1)$ automorphisms. Otherwise k is in $(\mathbb{Z}/q)^*$ and we solve $l^i = l \pmod q$, or $l^{i-1} = 1 \pmod q$. Since l has order p in $(\mathbb{Z}/q)^*$, $i-1$ is a multiple of p, or $i = pk+1$. Thus $\pi(y) = y$, which is just the case $i = 1$. Thus there are $q(q-1)$ automorphisms of G.

6. (a) Brute force to be done at least once in a lifetime. First show associativity for the 27 triple products from $\{i, j, k\}$, and then extend to sums.

(b) This follows from the rules for the group Q extended to sums.

(c) $N(\alpha\beta) = \alpha\beta(\overline{\alpha\beta}) = \alpha\beta\overline{\beta}\overline{\alpha} = \alpha N(\beta)\overline{\alpha} = N(\alpha)N(\beta)$.

(d) Since $\alpha\overline{\alpha} = N(\alpha) \neq 0$, define $\alpha^{-1} = \overline{\alpha}/N(\alpha)$.

(e) Closure: if $\alpha, \beta \neq 0$, then $N(\alpha\beta) = N(\alpha)N(\beta) \neq 0$. So $\alpha\beta \neq 0$. Associativity: 6(a). Identity: $e = 1$, and $N(e) = 1 \neq 0$. Inverse: 6(d), noting that $N(\alpha^{-1}) = N(\alpha)^{-1} \neq 0$.. Non-abelian: $ij = -ji$.

(f) Closure: If u, v are in U, then $N(uv) = N(u)N(v) = 1$. So uv is in U. Inverse: since $N(u) = 1$, $u^{-1} = \overline{u}$ is in U since $N(\overline{u}) = 1$. The set $x^2 + y^2 + z^2 + w^2 = 1$ in $\mathbb{R}^4$ is the unit three-sphere S^3. Not abelian since $ij = -ji$.

(g) Considering elements that commute with i, j, k, we have $Z(\mathbb{H}) = \mathbb{R}$, and $Z(U) = \{\pm 1\}$.

7. Let $\alpha = 1 + 2i - 2k, \beta = 3j + 4k$, and $\gamma = 1 - i + j - k$.

(a)

$$((1-2k)(3j-4k))(1+j) = (-8 + 6i + 3j - 4k)(1+j) = -11 + 10i - 5j + 2k,$$

$$(1-2k)((3j-4k)(1+j)) = (1-2k)(-3 + 4i + 3j - 4k) = -11 + 10i - 5j + 2k.$$

(b)

$$\overline{(1-2k)(3j-4k)} = \overline{-8+6i+3j-4k} = -8-6i-3j+4k,$$

$$\overline{(3j-4k)}\ \overline{(1-2k)} = (-3j+4k)(1+2k) = -8-6i-3j+4k,$$

$$\overline{(1-2k)}\ \overline{(3j-4k)} = (1+2k)(-3j+4k) = -8+6i-3j+4k.$$

(b) $N(\alpha) = 1^2+2^2 = 5$, so $\alpha^{-1} = (1/5)(1+2k) = 1/5+(1/5)k$. Then

$$\alpha\alpha^{-1} = (1-2k)(1/5+(2/5)k) = 1.$$

$N(\beta) = 3^2+4^2 = 25$, so $\beta^{-1} = (1/25)(-3j+4k) = (-3/25)j+(4/25)k$.

$$(\alpha\beta)^{-1} = (1/125)(-8-6i-3j+4k),$$

$$\beta^{-1}\alpha^{-1} = (1/125)(-3j+4k)(1+2k) = (1/125)(-8-6i-3j+4k),$$

$$\alpha^{-1}\beta^{-1} = (1/125)(1+2k)(-3j+4k) = (1/125)(-8+6i-3j+4k).$$

(d) $N(\alpha\beta) = N(-8+6i+3j-4k) = 64+36+9+16 = 125$. $N(\alpha)N(\beta) = 5\times 25 = 125$.

8. Identifying (y,z,w) with $\alpha = yi+zj+wk$, we compute

$$(y_1,z_1,w_1)\times(y_2,z_2,w_2) = (z_1w_2-z_2w_1, y_2w_1-y_1w_2, y_1z_2-y_2z_1),$$

$$\begin{aligned} Im(\alpha\beta) &= Im((y_1i+z_1j+w_1k)(y_2i+z_2j+w_2k)) \\ &= Im(-(y_1y_2-z_1z_2+w_1w_2)+(z_1w_2-z_2w_1)i+(y_2w_1-y_1w_2)j+(y_1z_2-y_2z_1)k) \\ &= (z_1w_2-z_2w_1)i+(y_2w_1-y_1w_2)j+(y_1z_2-y_2z_1)k \end{aligned}$$

Now $Im(\alpha) = (\alpha-\overline{\alpha})/2$, so

$$Im(\alpha\beta) = (\alpha\beta-\overline{\alpha\beta})/2 = (\alpha\beta-\overline{\beta}\overline{\alpha})/2 = (\alpha\beta-(-\beta)(-\alpha))/2 = (\alpha\beta-\beta\alpha)/2.$$

9. (a) $T_\alpha(r\beta) = \alpha(r\beta) = r(\alpha\beta) = rT_\alpha(\beta)$, and

$$T_\alpha(\beta+\gamma) = \alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma = T_\alpha(\beta)+T_\alpha(\gamma).$$

(1) $T_\alpha(1) = \alpha\cdot 1 = \alpha = x+yi+zj+wk$,
(2) $T_\alpha(i) = \alpha\cdot i = -y+xi+wj-zk$,
(3) $T_\alpha(j) = \alpha\cdot j = -z-wi+xj+yk$,
(4) $T_\alpha(k) = \alpha\cdot k = -w+zi-yj+xk$.

So, with respect to this basis,

$$A_\alpha = \begin{pmatrix} x & -y & -z & -w \\ y & x & -w & z \\ z & w & x & -y \\ w & -z & y & x \end{pmatrix}.$$

(b) $T_\alpha(\beta c) = \alpha(\beta c) = (\alpha\beta)c = T_\alpha(\beta)c$, and

$$T_\alpha(\beta+\gamma) = \alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma = T_\alpha(\beta) + T_\alpha(\gamma).$$

(1) $T_\alpha(1) = \alpha \cdot 1 = x + yi + zj + wk = 1(x+yi) + j(z-wi)$,
(2) $T_\alpha(j) = \alpha \cdot j = -z - wi + xj + yk = 1(-z-wi) + j(x-yi)$.

So, with respect to this basis,

$$B_\alpha = \begin{pmatrix} x+yi & -z-wi \\ z-wi & x-yi \end{pmatrix}.$$

(c) By observation, $A_\alpha^T = A_{\overline{\alpha}}$, $B_\alpha^* = B_{\overline{\alpha}}$ (careful), $A_\alpha^T A_\alpha = N(\alpha)I$, and $B_\alpha^* B_\alpha = N(\alpha)I$.

(d) One could check directly, but, if this holds at the level of linear transformations, it also follows for the associated matrices. Note that

$$T_\alpha T_\beta(\gamma) = \alpha\beta\gamma = T_{\alpha\beta}(\gamma).$$

(e) Same as (d).

(f) Closed: Suppose A, B are in $SU(2)$. Then

$$det(AB) = det(A)det(B) = 1,$$

and

$$AB(AB)^* = ABB^*A^* = ABB^{-1}A^{-1} = I.$$

Associative follows from matrix multiplication. Identity: $II^* = I$. Inverse: By definition, $A^{-1} = A^*$, and

$$A^{-1}(A^{-1})^* = A^{-1}(A^*)^{-1} = (A^*A)^{-1} = I.$$

When restricted to U, $\alpha \mapsto B_\alpha$ is a homomorphism into $SU(2)$ by (c) and (e), and the bijective property is straightforward.