Solution Outlines for Chapter 6

 # 1: Find an isomorphism from the group of integers under addition to the group of even integers under addition.

Let $\phi : \mathbb{Z} \to 2\mathbb{Z}$ be defined by $x \mapsto x + x = 2x$. Then $\phi(x + y) = 2(x + y) = 2x + 2y = \phi(x) + \phi(y)$, so ϕ is a homomorphism. Now, $\phi(x) = \phi(y)$ if and only if $2x = 2y$, which holds if and only if $x = y$. Thus ϕ is one-to-one. Finally, let $y \in 2\mathbb{Z}$. Then $y = 2k$ for some $k \in \mathbb{Z}$. Since $k \in \mathbb{Z}$ and $\phi(k) = 2k = y$, ϕ is onto.

 # 3: Let $\mathbb{R}^+$ be the group of positive real numbers under multiplication. Show that the mapping $\phi(x) = \sqrt{x}$ is an automorphism of $\mathbb{R}^+$.

Let $\phi : \mathbb{R}^+ \to \mathbb{R}^+$ be defined by $\phi(x) = \sqrt{x}$. Since $\sqrt{x}$ will be in the positive reals, and the positive reals is an appropriate domain for ϕ, ϕ is an automorphism. Now, $\phi(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = \phi(x)\phi(y)$, so ϕ is a homomorphism. Notice that $Ker\ \phi = \{x \big| \sqrt{x} = 1\} = \{1\}$, so ϕ is one to one. Finally, let $y \in \mathbb{R}^+$. Then $y^2 = x$ is also in $\mathbb{R}^+$. Moreover, $\phi(x) = \phi(y^2) = \sqrt{y^2} = y$, so ϕ is onto.

 # 4: Show that $U(8)$ is not isomorphic to $U(10)$.

Observe that $U(10)$ is cyclic while $U(8)$ is not.

 # 5: Show that $U(8)$ is isomorphic to $U(10)$.

First notice that $U(8) = \{1, 3, 5, 7\}$, $U(12) = \{1, 5, 7, 11\}$ and all elements of both $U(8)$ and $U(12)$ square to the identity. Let ϕ be defined by $\phi(1) = 1$, $\phi(3) = 5$, $\phi(5) = 7$, and $\phi(7) = 11$. You can check the multiplications of $\phi(1a)$, $\phi(3 \cdot 5)$, $\phi(3 \cdot 7)$ and $\phi(5 \cdot 7)$ in order to see that ϕ indeed is a homomorphism. It is clear by construction that ϕ is onto and one to one.

 # 6: Prove that isomorphism is an equivalence relation.

Proof. To show that isomorphism is an equivalence relation, I must show reflexive, symmetric and transitive. First, notice that $G \approx G$ by the identity map. Thus the isomorphism relation is reflexive. Suppose that $G \approx H$. Then there exists an isomorphism $\phi : G \to H$. But this implies that $\phi^{-1} : H \to G$ is also an isomorphism. Thus $H \approx G$ and the relation is symmetric. Finally, supposes that $G \approx H$ and $H \approx K$. Then there exist two isomorphisms: $\phi : G \to H$ and $\sigma : H \to K$. Then $\sigma\phi : G \to k$ is also an isomorphism (you have previously shown that the composition of bijections is a bijection; you should argue that the composition is still a homomorphism if you have not done so yet). Thus, the relation is transitive. □

 # 10: Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is Abelian.

Define α as above. Suppose that α is an automorphism. Then $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in G$. This implies that $(ab)^{-1} = a^{-1}b^{-1}$. But this means that $b^{-1}a^{-1} = a^{-1}b^{-1}$

and multiplying we see that $ab = ba$. Now suppose instead that G is Abelian. Then reversing the previous argument shows that α must be a homomorphism. The kernel of α is $\{g|g^{-1} = e\} = \{e\}$ so α is one-to-one. Finally, let $a \in G$. Then a^{-1} is also in G since G is a group. Moreover, $\alpha(a^{-1}) = (a^{-1})^{-1} = a$ so α is onto. (Note: You should recognize most of this problem from an earlier chapter).

 # 11: If g and h are elements from a group, prove that $\phi_g\phi_h = \phi_{gh}$.

Proof. Let $x \in G$. Then $(\phi_g\phi_h)(x) = \phi_g(\phi_h(x)) = \phi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \phi_{gh}(x)$. Thus, $\phi_g\phi_h = \phi_{gh}$. □

 # 12: Find two groups G and H such that $G \not\approx H$, but $\mathrm{Aut}(G) \approx \mathrm{Aut}(H)$.

Consider $G = \mathbb{Z}_6$ and $H = \mathbb{Z}_3$. Since $|\mathbb{Z}_6| \neq |\mathbb{Z}_3|$, $G \not\approx H$. But
$\mathrm{Aut}(\mathbb{Z}_6) \approx U(6) = \{1, 5\} =< 5 >\approx \mathbb{Z}_2$ and $\mathrm{Aut}(\mathbb{Z}_3) \approx U(3) = \{1, 2\} =< 2 >\approx \mathbb{Z}_2$. Thus $\mathrm{Aut}(G) \approx \mathrm{Aut}(H)$.

 # 14: Find $\mathrm{Aut}(\mathbb{Z}_6)$.

As above, $\mathrm{Aut}(\mathbb{Z}_6) \approx U(6) =< 5 >\approx \mathbb{Z}_2$. Thus there are only two elements in $\mathrm{Aut}(\mathbb{Z}_6)$. Clearly one is the identity map. Also, since the inverse map is an automorphism, this must be the second map. Thus $Aut(\mathbb{Z}_6) \approx \{id, \phi\}$ where $\phi(g) = -g$.

Alternately: The generators of $\mathbb{Z}_6$ are 1 and 5. Thus $\mathrm{Aut}(\mathbb{Z}_6) = \{\phi_1, \phi_5\}$ where ϕ_i is defined as the map that sends 1 to i. Since $\phi_1(1) = 1$, ϕ_1 is just the identity. Similarly, we can see that $\phi_5(1) = 5$ implies that 2 maps to 4 and 3 maps to 3. Thus ϕ_5 is the inverse map that sends g to $-g$.

 # 15: If G is a group, prove that $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups.

Proof. Clearly both $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are associative because function composition is associative. Now consider $\phi_1, \phi_2 \in \mathrm{Aut}(G)$. Since the composition of an isomorphism is an isomorphism (if you don't remember this, prove it to yourself), $\phi_1\phi_2 \in \mathrm{Aut}(G)$, giving closure. Let ϕ_e be the automorphism defined by $\phi_e(x) = x$. Then $\phi_1\phi_e(x) = \phi_1(x) = \phi_e\phi_1(x)$ so this is the identity map. Finally, by Theorem 6.1, property 1, we know that the inverse of an isomorphism is also an isomorphism, thus $\mathrm{Aut}(G)$ contains inverses. This completes the proof that $\mathrm{Aut}(G)$ is a group.

Now, let $\phi_g, \phi_h \in \mathrm{Inn}(G)$. By homework problem 11, we know that $\phi_g\phi_h \in \mathrm{Inn}(G)$ so it is closed. Using the same calculation (in problem 11), $\phi_g\phi_e = \phi_{ge} = \phi_g = \phi_{eg} = \phi_e\phi_g$, so the group identity is indeed ϕ_e, which is in $\mathrm{Inn}(G)$. Similarly, we see $\phi_g\phi_{g^{-1}} = \phi_{gg^{-1}} = \phi_e = \phi_{g^{-1}g} = \phi_{g^{-1}}\phi_g$ and inverses exist in $\mathrm{Inn}(G)$. Thus $\mathrm{Inn}(G)$ is also a group. □

 # 20: Show that $\mathbb{Z}$ has infinitely many subgroups isomorphic to $\mathbb{Z}$.

Consider $a\mathbb{Z}$ where $a \in \mathbb{Z}$. If $a = \pm 1$, $a\mathbb{Z} = \mathbb{Z}$, and if $a = 0$, $a\mathbb{Z} = \{0\}$. For all other a, $a\mathbb{Z}$ is a proper, non-trivial subgroup of $\mathbb{Z}$ (as shown previously). Consider

$\phi : a\mathbb{Z} \to \mathbb{Z}$ defined by $az \mapsto z$ (Note: ϕ clearly maps to $\mathbb{Z}$ by construction). Then $\phi(az_1 + az_2) = \phi(a(z_1 + z_2)) = z_1 + z_2 = \phi(az_1) + \phi(az_2)$, so ϕ is a homomorphism. Now, $\phi(az_1) = \phi(az_2)$ implies that $z_1 = z_2$. But, since $a = a$, this means $az_1 = az_2$ thus ϕ is one to one. Finally, for any $z \in \mathbb{Z}$, $az \in aZ$ thus our map is onto. Since there are an infinite number of $a \neq -1, 0, 1$, there are an infinite number of subgroups isomorphic to $\mathbb{Z}$.

 # 35: Show that the mapping $\phi(a+bi) = a-bi$ is an automorphism of the group of complex numbers under addition. Show that ϕ preserves complex multiplication as well.

First, we show ϕ is a homomorphism: $\phi((a+bi)+(c+di)) = \phi((a+c)+(b+d)i) = (a+c)-(b+d)i = (a-bi)+(c-di) = \phi(a+bi)+\phi(c+di)$. Now suppose that $\phi(a+bi) = \phi(c+di)$. Then $a-bi = c-di$. But this implies that $a = c$ and $b = d$. Hence, $a+bi = c+di$, and ϕ is 1-1. Finally, let $a+bi$ be any element of $\mathbb{C}$. Then $a-bi$ is also in $\mathbb{C}$ and $\phi(a-bi) = a-(-b)i = a+bi$. Thus ϕ is onto.

We see that ϕ also preserves multiplication since $\phi((a+bi)(c+di)) = \phi((ac-bd)+(ad+bc)i) = (ac-bd)-(ad+bc)i$, which is the same as $\phi(a+bi)\phi(c+di) = (a-bi)(c-di) = (ac-bd)-(bc+ad)$.

 # 36: Let $G = \{a + b\sqrt{2} | a, b$ are rational$\}$ and $H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} | a, b \text{ are rational} \right\}$. Show that G and H are isomorphic under addition. Prove that G and H are closed under multiplication. Does your isomorphism preserve multiplication as well as addition?

To show G is isomorphic to H under addition, define $\phi : G \to H$ by the map $a + b\sqrt{2} \mapsto \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$. Then $\phi(a + b\sqrt{2} + c + d\sqrt{2}) = \phi((a+c) + (b+d)\sqrt{2}) = \begin{bmatrix} a+c & 2b+2d \\ b+d & a+c \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2})$. It is clear that ϕ is onto since $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ is mapped to by $a + b\sqrt{2}$ and in both cases $a, b \in \mathbb{Q}$. Finally we see that ϕ is onto since $Ker\ \phi = \left\{ a + b\sqrt{2} | \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\} = \{a + b\sqrt{2} | a = 0 = b\} = \{0\}$.

Because $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(bc+ad)\sqrt{2}$ and the rationals are closed under multiplication, G is closed under multiplication. We similarly see that H is closed under multiplication: $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} ac+2bd & 2ad+2bd \\ bc+ad & 2bd+ac \end{bmatrix} = \begin{bmatrix} (ac+2bd) & 2(ad+bc) \\ (ad+bc) & (ac+2bd) \end{bmatrix}$.

Finally, we also see that ϕ preserves multiplication since $\phi((a + b\sqrt{2})(c + d\sqrt{2})) = \phi((ac + 2bd) + (bc + ad)\sqrt{2}) = \begin{bmatrix} ac+2bd & 2(bc+ad) \\ bc+ad & ac+2bd \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \phi(a + b\sqrt{2})\phi(c + d\sqrt{2})$.

 # 37: Prove that $\mathbb{Z}$ under addition is not isomorphic to $\mathbb{Q}$ under addition.

The proof is simply that $\mathbb{Z}$ is cyclic while $\mathbb{Q}$ is not cyclic. We have already shown $\mathbb{Z} =< 1 >$ but, for completeness, we should argue that $\mathbb{Q}$ is not cyclic. Assume that it is cyclic. Then $\mathbb{Q} =< \frac{p}{q} >$ for some reduced rational (note: $p, q \in \mathbb{Z}$). But $\frac{p}{2q} \neq (\frac{p}{q})^i$ for any i [there is one case $q = 2$ that has to be considered separate, but clearly $\mathbb{Q}$ is not generated by $\frac{p}{2}$ since you can't get a third]. But this means that $\frac{p}{2q} \notin \mathbb{Q}$, which is a contradiction.

 # 40: Let $\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) | a_i \in \mathbb{R}\}$. Show that the mapping $\phi : (a_1, a_2, \ldots, a_n) \to (-a_1, -a_2, \ldots, -a_n)$ is an automorphism of the group $\mathbb{R}^n$ under component wise addition. This automorphism is called inversion. Describe the action of ϕ geometrically.

Clearly, $(a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$ implies that $(-a_1, -a_2, \ldots, -a_n)$ is also in $\mathbb{R}^n$, thus $\phi : \mathbb{R}^n \to \mathbb{R}^n$. Now, $\phi((a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n)) = \phi((a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)) = (-(a_1 + b_1), -(a_2 + b_2), \ldots, -(a_n + b_n)) = (-a_1 - b_1, -a_2 - b_2, \ldots, -a_n - b_n) = (-a_1, -a_2, \ldots, -a_n) + (-b_1, -b_2, \ldots, -b_n) = \phi((a_1, a_2, \ldots, a_n)) + \phi((b_1, b_2, \ldots, b_n))$. thus ϕ is a homomorphism. The $\ker \phi = \{(a_1, a_2, \ldots, a_n) \big| (-a_1, -a_2, \ldots, -a_n) = (0, 0, \ldots, 0)\} = \{(a_1, a_2, \ldots, a_n) \big| -a_i = 0 \forall i\} = \{(a_1, a_2, \ldots, a_n) \big| a_i = 0 \forall i\} = \{(0, 0, \ldots, 0)\}$. Thus, ϕ is one-to-one. Finally, we need to show ϕ is onto. Let $(a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$. Then $(-a_1, -a_2, \ldots, -a_n)$ is also in $\mathbb{R}$ and $\phi((-a_1, -a_2, \ldots, -a_n)) = (a_1, a_2, \ldots, a_n)$.

Geometrically, this is a reflection through the origin.

 # 42: Suppose that G is a finite Abelian group and G has no element of order 2. Show that the mapping $g \to g^2$ is an automorphism of G. Show, by example, that there is an infinite Abelian group for which the mapping $g \to g^2$ is one-to-one and operation-preserving but not an automorphism.

Since G is closed under the operation, $g^2 \in G$ for all $g \in G$. Thus ϕ, defined as above, maps G to G. Now, for $g, h \in G$, $\phi(gh) = (gh)^2 = g^2h^2 = \phi(g)\phi(h)$ so ϕ is a homomorphism. [Recall, $(gh)^2 = g^2h^2$ because G is Abelian.] Let $\phi(g) = \phi(h)$. Then $g^2 = h^2$, which implies $g^2h^{-2} = (gh^-1)^2 = e$. Since G has no elements of order two, this means that $gh^{-1} = e$ so $g = h$ and ϕ is one-to-one. [Alternatively, $\ker \phi = \{g | g^2 = e\} = \{g | g = e\} = \{e\}$ since there are no elements of order 2.] Since G is finite and ϕ is one-to-one, we know ϕ is onto. Thus ϕ is an automorphism.

Let $G = \mathbb{Z}_{\geq 0}$. Then ϕ is still 1-1 and a homomorphism. However, ϕ is not onto. For example, nothing maps to 3. Thus ϕ is not an automorphism.

 # 43: Let G be a group and let $g \in G$. If $z \in Z(G)$, show that the inner automorphism induced by g is the same as the inner automorphism induced by zg.

Let $g \in G$ and $z \in Z(G)$. Then $\phi_{zg}(x) = (zg)x(zg)^{-1} = zgxg^{-1}z^{-1} = zz^{-1}gxg^{-1}$. This last step is true because z is in the center, and the center is a group so z^{-1} is also in the center. Now $zz^{-1}gxg^{-1} = gxg^{-1} = \phi_g(x)$.

 # 45: Suppose that g and h induce the same inner automorphism of a group G. Prove that $h^{-1}g \in Z(G)$.

Proof. Suppose that g and h induce the same inner automorphism of a group G. Then for all $x \in G$, $\phi_g(x) = \phi_h(x)$. Hence, $gxg^{-1} = hxh^{-1}$. Multiplying on the right of each side of the equation by g, we have $gx = hxh^{-1}g$. Now we multiply each side on the left by h^{-1}. this gives $h^{-1}gx = xh^{-1}g$. Thus $h^{-1}g$ commutes with x for all $x \in G$ so $h^{-1}g \in Z(G)$. □

 # 48: Let ϕ be an isomorphism from a group G to a group $\overline{G}$ and let a belong to G. Prove that $\phi(C(a)) = C(\phi(a))$.

We know that $ab = ba$ if and only if $\phi(a)\phi(b) = \phi(b)\phi(a)$. Let $g \in C(a)$. Then $ga = ag$ which implies $\phi(g)\phi(a) = \phi(a)\phi(g)$. Hence, $\phi(g) \in C(\phi(a))$, illustrating the first containment. Now let $h \in C(\phi(a))$. Then $h\phi(a) = \phi(a)h$. But ϕ is onto so there exists a $g \in G$ such that $h = \phi(g)$. Further, $ga = ag$ because h and $\phi(a)$ commute. Thus $h \in \phi(C(a))$. Since both containments hold, $\phi(C(a)) = C(\phi(a))$.

 # 52: Given a group G, define a new group G^* that has the same elements as G with the operation $*$ defined by $a * b = ba$ for all a and b in G^*. Prove that the mapping from G to G^* defined by $\phi(x) = x^{-1}$ for all x in G is an isomorphism from G onto G^*.

Since G^* contains the same elements of G, and G is closed under inverses, ϕ maps from G to G^*. Now for $g, h \in G$, $\phi(gh) = (gh)^{-1} = h^{-1}g^{-1} = \phi(h)\phi(g) = \phi(g) * \phi(h)$. Thus ϕ is a homomorphism. The kernel of ϕ is $\{g \in G | \phi(g) = g^{-1} = e\} = \{g \in G | g^{-1}g = eg\} = \{g \in G | e = g\} = \{e\}$. Hence, ϕ is also one to one. [Note: If G is finite, we are done since this implies ϕ is onto.] Now let $h \in G^*$. Then $h^-1 \in G^*$, and hence in G. Farther, $\phi(h^{-1}) = (h^{-1})^{-1} = h$. Thus, ϕ is onto, which completes the proof that ϕ is an isomorphism.