Daniel Gardiner
Math 122, PSET 2 Answer Key (With many thanks to Sam Lewallen and Yiyi Deng, whose excellent proofs and code are presented here with their permission mostly unchanged.)

1. Take $\varphi : G \to G'$ and $x \in G$ with order r. Then, if φ is a homomorphism, $\varphi(x)^r = \varphi(x^r) = \varphi(e_G) = e_{G'}$, so the order of $\varphi(x)$ is less than or equal to r. In fact, this order, k, must be a factor of r. For, assume not. Then, $\exists\ c \in \mathbb{N} \neq 0$, $c < k$, s.t. $r = kn + c$ for some positive $n \in \mathbb{N}$. Then we have

$$e_{G'} = \varphi(x^r) = \varphi(x^{kn})\varphi(x^c) = \varphi(x^k)^n\varphi(x^c) = \varphi(x^c)$$

$$\Rightarrow \varphi(x)^c = e_{G'}$$

   But k, not c, is the order of $\varphi(x)$, and $c < k$, so we have a contradiction.

2. (a) Let $\varphi : G \to G'$ be a surjective homomorpism. Assume that G is abelian, that is, $xy = yx$ for all elements $x, y \in G$. Now, φ being surjective implies that every element of G' can be written as $\varphi(x)$ for some $x \in G$. Thus, to show G' is abelian, we need only show that $\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$ for all $x, y \in G$. However, φ is a homomorphism, so this reduces to $\varphi(xy) = \varphi(yx)$, which is clearly true because xy and yx are the same element in G.

   (b) Now assume G is the cyclic group on x, that is, that every element of G can be written as x^r for some $r \in \mathbb{N}$. Then, the surjectivity of φ again gives us that every element $z \in G'$ can be written as $\varphi(y)$ for some $y \in G \Rightarrow z = \varphi(x^r)$ for some r, $\Rightarrow z = \varphi(x)^r$ $\forall z \in G'$. Thus, G' is the cyclic group on the element $\varphi(x) \in G'$.

3. Aut$G$ is closed under composition: the composition of two bijective maps $\rho_1, \rho_2 : G \to G'$ is a bijective map; $\rho_2 \circ \rho_1$ also satisfies the homomorphism property. Associativity follows because we are composing functions: $((\rho_1 \circ \rho_2) \circ \rho_3)(x) = (\rho_1 \circ \rho_2)(\rho_3(x)) = \rho_1(\rho_2(\rho_3(a))) = \rho_1(\rho_2 \circ \rho_3)(x) = (\rho_1 \circ (\rho_2 \circ \rho_3)(x)$. Identity Element: $I : G \to G'$ such that $I(a) = a$ for all $a \in G$ is an automorphism and is the identity on Aut$G$ because $I(\rho(a)) = \rho(a) = \rho(I(a))$. Inverses: each $\rho \in$ Aut$G$ is an automorphism, so $\exists$ a bijective map $\rho^{-1} : G \to G'$ such that $\rho^{-1}(\rho(a)) = a$ and preserves group multiplication. In other words, $\rho \circ \rho^{-1} = I$, the identity automorphism. Hence, Aut$G$ is a group.

4. Take a generator x of G, the cyclic group of order 10. Then any automorphism φ of G is completely determined by $\varphi(x)$. Moreover, in order to be injective, and hence bijective, it is clear that $\varphi(x)$ must have order 10, Hence, checking the various options for $\varphi(x)$, we have four distinct choices: $\varphi(x) = x$, $\varphi(x) = x^3$, $\varphi(x) = x^7$, and $\varphi(x) = x^9$. These four choices correpond to the four members of AutG. Now, by φ_n, we mean the automorphism sending x to x^n, We thus have $AutG = \{\varphi_n(x)\}$, where $n = 3, 5, 7$, or 9, and since a brief computation shows that $\varphi_3(x)$ generates the other members of the group, $AutG$ is the cyclic group of order 4.

   Note: By far the most common error on this set was a failure to specify the group structure of $AutG$. When being asked to determine a group, it is insufficent to simply list the group as a set. You should at least comment on its group structure (i.e. the order of every element

involved), and now that we have a notion of isomoprhisms, it is probably better to say exactly what the group is.

5. (a) Let φ_x be conjugation by x. Then clearly, $a \sim a$ because $a = aaa^{-1} = \varphi_a(a)$. For the symmetric property, it's clear that $a = \varphi_x(b) \Rightarrow b = \varphi_{x^{-1}}(a)$. For transitivity, $y^{-1}x^{-1}$ is the inverse of xy, so if $a = \varphi_x(b)$, and $b = \varphi_y(c)$, then, by substitution, we get $a = \varphi_{xy}(c)$.

   (b) If a is the only element of its conjugacy class, then $xax^{-1} = a$ for all x, $\Leftrightarrow xa = ax$. Thus, the elements that are alone in their conjugacy class are those that commute with all the other elements of the group.

6. The fibres of φ are the sets $\varphi^{-1}(x)$ for all $x \in G'$. Choose a particular $\varphi^{-1}(x)$. Take two elements, $y, y' \in \varphi^{-1}(x)$, and let $z = y'^{-1}y, \Rightarrow (*)\ y = y'z$. Thus, $y \equiv y'$, implies they are in the same coset of a subgroup that contains z. Now take φ of both sides of $(*)$, which gives us $\varphi(y) = \varphi(y'z) \Rightarrow \varphi(y) = \varphi(y')\varphi(z) \Rightarrow x = x\varphi(z) \Rightarrow \varphi(z) = e_{G'} \Rightarrow z \in K = \ker \varphi$. Thus, y and y' are in the same coset of $K \Rightarrow \varphi^{-1}(x) \subset yK$ for any $y \in \varphi^{-1}(x)$ (we have just showed that all these sets are the same). To show the reverse inclusion, take two elements z, z' in the coset yK, $y \in \varphi^{-1}(x)$. Then, $z = z'h$, for some $h \in K, \Rightarrow \varphi(z) = \varphi(z'h) \Rightarrow \varphi(z) = \varphi(z')\varphi(h), \Rightarrow \varphi(z) = \varphi(z')$, because h is in the kernal of φ. Thus, all the elements of yK are in the same fibre, and because $y \in yK$, it is precisely the fibre that contains y, that is, the fibre of $x \Rightarrow yK \subset \varphi^{-1}(x)$. Thus, $yK = \varphi^{-1}(x)$, which shows that every fibre corresponds to one coset of the kernal. Because every element of G is contained in some fibre, this shows that there is a 1-1 correspondence between cosets and fibres.

7. By Lagrange's Theorem, the order of every subgroup of G must divide the order of G. In particular, in the case that the order of G is p^k for some prime p and $k \in \mathbb{N}$, it is clear that the order of every subgroup must also be a power of that same prime p. Now, given any element $g \in G$, we can construct the subgroup H_g that is the cyclic group generated by the element g, with the order of H_g equal to the order of g. Thus, the order of every element g must be p^r for some $r \in \mathbb{N}$, $r \leq k$. If, for some element g, $r \neq 0$, we have $g^{p^r} = e = (g^{p^{r-1}})^p$, and therefore $g^{p^{r-1}}$ is our desired element of order p. (If it were to have order less than p, that would clearly also imply a smaller order for g as well, as it is just a product of g's.). If, on the other hand, $r = 0$ for all g, then every element is the identity and we are dealing with the group of order one, and the statement is trivially true.

8. **Claim**: Every subgroup of index 2 is normal. **Proof**: Let H be a subgroup of index 2 and partition G into two cosets of H. THen $G - H$ is a single left or right coset of H. Let $g \in G$. If $g \in H$, then $gH = H = Hg$. If $g \notin H$, then $gH \neq H$ so $gH = G - H$. Similarly, $Hg = G - H$ so for all $g \in G$, $gH = Hg$, so $gHg^{-1} = H$, and thus H is normal in G.

9. We know that $|G|$=|im φ| |ker φ|, so |im φ| divides $|G|$. But we also know that Im(φ) is a subgroup of G', and so |im φ| divides G'. Thus, since $|G|$ and $|G'|$ have no common factors |im φ| must equal 1. Hence, the image of φ is trivial, and so φ is the trivial homomorphism sending every element to the identity in G'.

10. **Claim**: If $H \cap K = 1$ then $HK = G$. **Proof**: We must show that $\rho : H \times K$ is surjective. But because the order of $G = \mid H \times K \mid = ab$, it is enough to show that ρ is injective. Let

$hk = h'k'$ for some $h, h' \in H$ and $k, kk' \in K$, so $h'h^{-1} = k(k')^{-1}$. Hence, $h'h^{-1}$ and $k(k')^{-1}$ are in $H \cap K = 1 \rightarrow h = h'$ and $k = k'$ so ρ is injective.
Claim: G is not isomorphic to the product group $H \times K$.
Proof: By counterexample. Consider $G = S_3$, and take $H = \{e, (12)\}$, $K = \{e, (123), (132)\}$. Then certainly the order of HK is the same as the order of G, but the product group $H \times K$ contains the element $((12), (123))$, an element of order 6, while S_3 has no elements of order 6 because it is not cyclic.

Note: Many people pointed out that H and K needed to be normal in G, and cited Artin as well, but really the best method here is just a clear, concise, counter-example. Also, while I gave credit to what were essentially proofs straight out of Artin, for your own practice make sure you at least write out the proofs on your own without referring to the book to make sure that you understand them.