2.1.1 The symmetries of a non square rhombus is isomorphic to that of a (non-square) rectangle. It has four elements and is abelian. Denoting the 180° rotation by a and the reflection across one of the diagonals by β the elements of the group are: \{e, α, β, αβ\} with α² = β² = e, and αβ = βα.

2.1.6 Observe that the group of symmetries of the rectangle are the same as the group described in 2.1.1. Each element has square equal to the identity, e. But in \(\mathbb{Z}_4\) the elements \{1\} and \{3\} have squares \(2[1] = [2] \neq [0]\) and \(2[3] = [6] = [2] \neq [0]\). Note that in \(\mathbb{Z}_4\) the group operation is addition so the “square” of an element means to add it to itself, while in the group of symmetries of the rectangle the group operation is composition, so the “square” of an element is itself (written as juxtaposition).

2.1.7 We prove this by induction: Base case \(n = 1\) is clear: \(ϕ(g) = ϕ(g)^1\). Suppose \(ϕ(g^n) = ϕ(g)^n\) for some \(n ≥ 1\). Consider \(ϕ(g^{n+1}) = ϕ(g^n g) = ϕ(g)ϕ(g^n)\) since \(ϕ\) is a homomorphism. By the induction hypothesis we have \(ϕ(g)ϕ(g^n) = ϕ(g)ϕ(g^n)\) (the last equality being by definition) and the result follows by induction. Observe that \(ϕ(e) = e\), so the result implies that if \(g^n = e\) that \(ϕ(g^n) = e\).

2.1.8 Suppose \(G\) is abelian. Let \(h, h'\) be two elements in \(H\). Since \(ϕ\) is surjective, there exist \(g, g' ∈ G\) so that \(ϕ(g) = h\) and \(ϕ(g') = h'\). So \(hh' = ϕ(g)ϕ(g') = ϕ(gg') = ϕ(g')ϕ(g) = h'h\) and thus \(H\) is abelian. Assuming \(H\) is abelian one uses the fact that \(ϕ\) is injective (one-to-one) to show similarly that any two elements in \(G\) commute.

2.1.16 I will show first that (a) implies each of the other 4 statements, and then show that (c) ⇒ (a). So assume \(G\) is abelian. (b): \((ab)^{-1} = b^{-1}a^{-1}\) in any group but since \(G\) is abelian, \(b^{-1}a^{-1} = a^{-1}b^{-1}\). (c): Commute the element \(a\) past \(b\), cancel the \(aa^{-1}\) and then the \(bb^{-1}\), so \(aba^{-1}b^{-1} = e\). (d): \((ab)^2 = abab\) in any group, but since \(G\) is abelian one may switch the orders to obtain \(a^2b^2\). (e): the base case is trivial. Then observe that \((ab)^{n+1} = (ab)(ab)^n\) so assuming \((ab)^n = a^nb^n\) implies \((ab)^{n+1} = (ab)a^nb^n\), and using \(G\) abelian again we can move the \(a^n\) past the \(b\) to get \((ab)^{n+1} = a^n(b^n+1)\) and the result follows by induction. Finally, if \(aba^{-1}b^{-1} = e\) we can multiply both sides of this equation on the right by \(ba\) to obtain \(ab = ba\) so that (c) implies (a).

2.2.8 (a): I will prove \(a^k a^\ell = a^{k+\ell}\) for \(k, \ell ≥ 0\). Induction on \(k\): for \(k = 0\) there is nothing to prove, as \(a^0 = e\) by convention. The definition of \(a^\ell\) is on page 94 in the text: it is defined inductively as \(a^n = aa^{n-1}\). Assume \(a^{k-1}a^\ell = a^{k-1+\ell}\). Then \(a^k a^\ell = aa^{k-1}a^\ell = a(a^{k-1+\ell})\) by the induction hypothesis, but using the definition of powers in a group we get \(a^{1+k-1+\ell} = a^{k+\ell}\), (b) and (c) follow the same general procedure, using the definition of \(a^{-k} = (a^{-1})^k\).

2.2.10 We need to work out the orders of elements of \(Φ(14)\), and note that the elements of order 6 are the generators. Clearly the order of any element is the same as the order of its inverse, since \((aa^{-1})^k = a^k(a^{-1})^k = e\). \(Φ(14)\) is a multiplicative group consisting of \{1, [3], [5], [9], [11], [13]\}. The identity has order 1, while \([13] = [−1]\) obviously has order 2 since \([−1]^2 = [1]\) and \([1]\) too. The elements \{3\} and \{5\} are inverses of each other since \([15] = [1]\) while \([9]\) and \([11]\) are inverses of each other since \([1498] = [99] = [1]\). The order of \{3\}: \([3]^2 = [9] \neq [1]\), \([3]^3 = [27] = [−1]\) which has order 2, so \(o([3]) = o([5]) = 6\) and so \{3\} and \{5\} generate. Computing powers of \([9]\) = \([−5]\) we see that \(o([9]) = o([11]) = 3\).

2.2.14 Just use Prop. 2.2.33: the order of \(a^2\) has order \(o(a)/gcd(s, o(a))\). We know that \((ab)^{o(ab)} = a^{o(ab)}b^{o(ab)} = e\). So \(a^{o(ab)}\) and \(b^{o(ab)}\) are inverses of each other, hence each have the same order (check this!). But the order of \(a^{o(ab)}\) is a divisor of \(o(a)\), and similarly the order of \(b^{o(ab)}\) is a divisor of \(o(b)\), thus the order of each is a common divisor of \(o(a)\) and \(o(b)\). But since \(gcd(o(a), o(b)) = 1\), this means that \(a^{o(ab)} = e\) and \(b^{o(ab)} = e\) (as they must have order 1), and one can show from this (using the usual division algorithm trick) that \(o(a)\) is a divisor of \(o(a)\) and \(o(b)\). Since \(o(a)\) and \(o(b)\) are relatively prime, \(o(a)\) and \(o(b)\) are coprime. But one may also show (using the division algorithm trick) that \(o(ab)\) is a divisor of \((ab)^{o(ab)} = e\) by commutativity of \(a\) and \(b\). Thus \(o(ab) = o(a)\) or \(o(b)\).

2.4.5 It is clear that \(gAg^{-1}\) is a subset of \(G\). So we check: \(gag^{-1}gbg^{-1} = gabg^{-1} ∈ gAg^{-1}\) and \((gag^{-1})^{-1} = ga^{-1}g^{-1} ∈ gAg^{-1}\)
2.4.6 Let $H$ be any subgroup of an abelian group $G$. Let $g \in G$ and $h \in H$. It is enough to show that $ghg^{-1} \in H$. But $ghg^{-1} = ggg^{-1}h = h \in H$ since $G$ is abelian.

2.4.7 Let $a, x \in G$. $\varphi(a) = \varphi(x)$ if $\varphi(a^{-1})\varphi(x) = e$ if $\varphi(a^{-1}x) = e$ if $a^{-1}x \in N$, (as $N$ is the kernel of $\varphi$). Observe that if $aN \neq xN$ then $an = xn'$ for some $n, n' \in N$. But this implies $a^{-1}x = n'n' \in N$. For the other direction of the last implication we assume $a^{-1}x = n \in N$, so that $an = x$. But then for any element $xn' \in xN$ we see that $xn' = a(nn') \in aN$ since $nn' \in N$. Now suppose $an'' \in aN$. Then $an'' = xn^{-1}n'' \in xN$. Observe that we can’t appeal to Prop. 2.5.3 since it is in the next section!

2.4.9 We have defined $D_n$ to be a group generated by a reflection $a$ and a rotation $r$ which satisfy the relations $a^2 = r^n = e$ and $ar = r^{-1}a$. By the definition of $e a \rightarrow -1$ while $r \rightarrow 1$. The elements in $D_n$ are of the form $r^k$ or $ar^k$ for $0 \leq k \leq n-1$. The elements that exchange the top and bottom of the n-gon are those of the form $ar^k$, since $a$ does exchange top and bottom and $r$ does not. So $\varepsilon(ak) = -1$ and $\varepsilon(r^k) = 1$. We just need to check that this satisfies the homomorphism property. Using the relation $ar = r^{-1}a$ for $\ell = 1$ we compute $\varepsilon(a^{rj}a^{r^k}) = (-1)^{j} = \varepsilon(a^{rj}) \varepsilon(a^{r^k})$.

2.5.12 It is clear that (c) implies (b) taking $b = a$. Moreover, (a) iff (c) is easy: fix $a \in G$, and assume $aN^{-1} = N$. Then for every $n \in N$, $an = ana^{-1}a = n'a$ for some $n'$, so that $aN \subset Na$ the other containment is similar. If $aN = Na$ then for any $n \in N$, $an = n'a$ for some $n' \in N$. But then $ana^{-1} = n' \notin N$, so that $aN^{-1} \subset N$ and the other containment is similar, so is normal. Thus all three statements imply each other.

2.6.2 We must show that the relation on a group G “a is conjugate to b” satisfies reflexivity, symmetry and transitivity. Let $a \in G$. Then $ae^{-1} = a$, so that $a$ is conjugate to itself. Now assume $a$ is conjugate to $b$ so that there exists a $g \in G$ such that $gbg^{-1} = a$. Multiplying on the left by $g^{-1}$ and on the right by $g$ we get $b = g^{-1}ag$, so that $b$ is conjugate to $a$. Now suppose $a$ is conjugate to $b$, $a = gbg^{-1}$ and $b$ is conjugate to $c$, $b = hch^{-1}$. Then $a = g(hch^{-1})g^{-1} = (gh)c(gh)^{-1}$ so that $a$ is conjugate to $c$, proving transitivity.

2.6.4 Recall that $D_4 = \{a^r : 0 \leq i \leq 2\}$ as a set with the rules $a^2 = r^4 = e$ and $ra = ar^{-1}$ (which is equivalent to the condition $ar = r^{-1}a$ and implies $r^2a = ar^{-1}$). First we know that $[e] = \{e\}$. Also, if we compute $ar^2a^{-1} = (ar)(ra) = (r^{-1}a)(ar^{-1}) = r^{-2}r = r^2$, so acommutes with $r^2$. Obviously $r$ commutes with $r^2$, so $r^2$ is in the center of $D_4$ so its conjugacy class is just $[r^2] = \{r^2\}$. Let us compute the elements of $[a]$. First, $a \in [a]$. Next, we compute that $(ar)(a^{-1}) = r^{-1} = (a^{-1})(ar^{-1}) = a^{-1}ar^{-1}a^{-1} = a^{-1}ar^{-2}a^{-1}$. Since $r^{-2} = e$ or $r^2$, both of which commute with $a$ we see that $(a^{-1})(ar^{-1}a^{-1}) = ar^{-2}$ which is either $a$ or $ar^2$. So $[a] = \{a, ar^2\}$. Next we compute $[r] = \{r, ara = r^{-1}\}$ using the fact that powers of $r$ commute to save some work. This leaves only two elements: $ar$ and $ar^{-1}$. It is easy to see that they are conjugate to each other by computing $a’(ar)a = ra = ar^{-1}$.

2.6.5 We use the same basic technique to compute conjugates in $D_5$ with the relations $a^2 = r^5 = e$ and $ar^2 = r^{-1}a$. Two facts are useful: the number of elements in a conjugacy class divides the order (10) of $D_5$, and conjugacy classes partition the group. First $[e] = \{e\}$. Next we compute some conjugates of $a$: $rar^{-1} = ar^{-2} = ar^3, r^2ar^{-2} = r^{-3} = ar, r^3ar^{-3} = ar^{-2} = r^4$ and of course $eae = a$. So we have at least $\{a, ar, ar^2, ar^3, ar^4\} \subset [a]$. But the number of conjugates of $a$ must divide 10, and $e$ is not conjugate to $a$, so there can be no more! There are just 4 elements of the group remaining, and
so their conjugacy classes must have either 1 or 2 elements in them. We compute \(ара^{-1} = r^{-1} = r^4\) and \(ара^2a^{-1} = r^{-2} = r^3\), so the conjugacy classes are: \(\{e\}\), \(\{a, ar, ar^2, ar^3, ar^4\}\), \(\{r, r^4\}\), and \(\{r^2, r^3\}\).

2.7.11 Let \(G\) be an abelian group, and \(N\) any subgroup. Since \(G\) is abelian, \(N\) is normal. Consider two elements \(gN\) and \(hN\) in the quotient group \(G/N := \{gN : g \in G\}\). The products of these two elements in both orders are \(gNhN = (gh)N\) and \(hNgN = (hg)N\). Our job is to show that these are equal (as sets!) since this implies that the elements \(gN\) and \(hN\) in \(G/N\) commute. Observe that \(ghe = gh \in (gh)N\). But \(ghe = hge\) since \(G\) is abelian, so \(ghe = hge \in (hg)N\). By Prop. 2.5.4(a) the fact that the cosets \((gh)N\) and \((hg)N\) share an element implies that the are equal. Thus \(G/N\) is abelian.

2.7.12 Recall that the center of \(G\) is \(Z(G) := \{z \in G : zg = gz \ \forall g \in G\}\). If \(G/Z(G)\) is cyclic then there exists some coset \(gZ(G)\) such that every coset \(aZ(G) = (g^k)Z(G)\) for some \(k \in \mathbb{Z}\). Now cosets of \(Z(G)\) partition the group \(G\), so that every element is in some coset, i.e. \(a \in aZ(G)\) and \(b \in bZ(G)\). So take two arbitrary elements of \(G\), say \(a\) and \(b\). We must show that \(ab = ba\). Now \(aZ(G) = (g^k)Z(G)\) and \(bZ(G) = (g^\ell)Z(G)\) for some \(k, \ell \in \mathbb{Z}\), so \(a = g^kz_1\) and \(b = g^\ell z_2\). Using the fact that \(z_1, z_2 \in Z(G)\) and powers of \(g\) commute with each other we have: \(ab = (g^kz_1g^\ell z_2 = g^\ell z_2 g^k z_1 = ba\), and we have shown \(G\) is abelian.