MATH1530, HOMEWORK 3

Section 1.7

2. Let $z_1, z_2 \in \mathbb{Z}$. We need to check the following:
(i) $z_1 \cdot (z_2 \cdot a) = (z_1 z_2) \cdot a$ for all $z_1, z_2, a \in \mathbb{Z}$
(ii) $0 \cdot a = a$ for all $a \in \mathbb{Z}$ since 0 is the identity of $\mathbb{Z}$.
First, (i) is saying $z_1 + (z_2 + a) = (z_1 + z_2) + a$ which is simply associativity of addition in $\mathbb{Z}$ and (ii) is saying $0 + a = a$, which is obvious.

4. Kernel of an action: $\{g \in G : gb = b \text{ for all } b \in B\}$
Given a group G, let S be a subset of G. Then S is a subgroup if and only if for any elements $a, b \in S$, $ab^{-1} \in S$. Using this principle, first look at (a). Let a, b in the Kernel. Then for any $x \in A$, we have $b \cdot x = x$ so $x = e \cdot x = b^{-1} b \cdot x = b^{-1} \cdot x$ so we have b^{-1} in the Kernel. Now, $(ab^{-1}) \cdot x = a \cdot (b^{-1} \cdot x) = a \cdot x = x$ for all $x \in A$, which shows that ab^{-1} is in the Kernel. Hence we are done.

Let us set $S = \{g \in G : g \cdot a = a\}$ where a is a fixed element in A.
If $g \in S$, $g \cdot a = a$ and we have $a = g^{-1} \cdot a$ which means $g^{-1} \in S$. Also if $h, g \in S$ then $(hg^{-1}) \cdot a = h \cdot (g^{-1} \cdot a) = h \cdot a = a$ so hg^{-1} is also in S, which shows the stabilizer of a in G is a subgroup.

16. We need to check two things;
(i) $(hg) \cdot x = h \cdot (g \cdot x)$ for all $h, g, x \in G$
(ii) $1 \cdot g = g$ for all $g \in G$.
First, we compute $(hg)x(hg)^{-1} = (hg)x(g^{-1}h^{-1}) = h(gxg^{-1})h^{-1} = h \cdot (gxg^{-1}) = h \cdot (g \cdot x)$ to obtain (i) and (ii) is simply $1g1^{-1} = g$.

17. We denote $\sigma_g : G \to G$ as the conjugation by g, $\sigma_g(h) = ghg^{-1}$. We prove it is injective. Assume $ghg^{-1} = gkg^{-1}$. Then $h = k$, so σ_g is injective. Now given any element h, $\sigma_g(g^{-1}hg) = g(g^{-1}hg)g^{-1} = h$, so σ_g is surjective. Finally, $\sigma_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = \sigma_g(h)\sigma_g(k)$, so σ_g is an automorphism.
It is in general true that if $\phi : G \to G$ is an automorphism, then $x \in G$ and $\phi(x)$ has the same order. In particular, x and gxg^{-1} will have the same order. And since σ_g is bijective, if A is a subset of G and we denote $\sigma_g(A)$ be the image of A under σ_g then $|\sigma_g(A)| = |A| = |gAg^{-1}|$.

18. Recall that a relation $\sim$ on a set A is an equivalence relation if
(i) $a \sim a$ for all $a \in A$.
(ii) $a \sim b$ then $b \sim a$ for all $a, b \in A$
(iii) $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$.
Since $a = 1 \cdot a$ for all a, (i) is satisfied. If $a \sim b$, it means by definition, there exists $h \in H$ such that $a = hb$. But then $b = h^{-1}a$ where $h^{-1} \in H$. So $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, it implies $a = hb$ and $b = h'c$, so we have $a = h(h'c) = (hh')c$, where $hh' \in H$, so $a \sim c$.

19. We have defined a map $\phi_x : H \to \mathcal{O}$ by $h \mapsto hx$. We need to show that this is injective and surjective. First, assume that $\phi(h) = \phi(k)$. It means $hx = kx$, or $h = k$. (injectivity) Now let $y \in \mathcal{O}$. Then by definition of the orbit of x, $y \sim x$ and $y = hx$ for some $h \in H$. So $\phi(h) = y$, showing that ϕ is surjective.
That is, we have shown that $|H| = |\mathcal{O}|$ and in particular, for any element $x \in G$, the size of its orbit is equal to $|H|$. But since $\sim$ is an equivalence relation on G, its equivalence classes (orbits) partition the set G which are shown to have equal number of elements. Let N be the number of distinct orbits = equivalent classes. Then $|G| = |H| \cdot N$, from which we deduce Lagrange's Theorem.

Section 2.1

3. A standard way to check whether a subset of a group is indeed a subgroup is the following: Verify that $ab^{-1} \in S$ for all $a, b \in S$. However, when the subset is finite, it suffices to check $ab \in S$ for all $a, b \in S$.

(a). $\{1, r^2, s, sr^2\}$. Check all possible pairs: $r^2s = r(rs) = r(sr^{-1}) = (rs)r^{-1} = sr^{-1}r^{-1} = sr^{-2} = sr^2 \in S$, $r^2(sr^2) = r^2sr^2 = sr^2r^2 = s \in S$, $s(sr^2) = s^2r^2 = r^2 \in S$, so we are done.

(b). $\{1, r^2, sr, sr^3\}$. Again, $r^2sr = sr^2r = sr^3$, $r^2sr^3 = sr^2r^3 = sr$, $srsr^3 = ssr^{-1}r^3 = r^2$, which are all inside S.

5. If $n = |G| > 2$, $n - 1$ does not divide n. From Lagrange's theorem, it is impossible to have a subgroup of order $n - 1$.

8. Let H and K be subgroups of G. Then show that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Proof. Assume that the conclusion is false. That is, $H \subsetneq K$ and $K \subsetneq H$. Equivalently, there exists $h \in H$ which is not contained in K and $k \in K$ which is not contained in H. Since $H \cup K$ is assumed to be a subgroup, $hk \in H \cup K$. For a moment, assume that $hk \in H$. Since $h^{-1} \in H$, $h^{-1}hk = k \in H$, which is a contradiction. On the other hand, if we assume $hk \in K$, $hkk^{-1} = h \in K$, which is another contradiction. Therefore, it must happen that either $H \subseteq K$ or $K \subseteq H$. ☐

11.

(a),(b). $S = \{(a, 1) : a \in A\}$. To show that S is a subgroup, let us assume $x, y \in S$. Then $x = (a, 1)$, $y = (b, 1)$ for some elements $a, b \in A$. We have $y^{-1} = (b^{-1}, 1^{-1}) = (b^{-1}, 1)$ and $xy^{-1} = (ab^{-1}, 1)$, which is in S as $ab^{-1} \in A$. That is, S is a subgroup. From symmetry, it should be clear that (b) is also a subgroup.

(c). $S = \{(a, a) : a \in A\}$. Assume $x, y \in S$. Then $x = (a, a)$ and $y = (b, b)$ for some $a, b \in A$. We see that $y^{-1} = (b^{-1}, b^{-1})$ and $xy^{-1} = (ab^{-1}, ab^{-1})$. Since $ab^{-1} \in A$, we have $xy^{-1} \in S$, which shows that S is a subgroup.