MODEL ANSWERS TO THE FOURTH HOMEWORK

§14: 31. Let H_1 and H_2 be two normal subgroups of a group G. We already know that $H_1 \cap H_2$ is a subgroup of G. We check that it is normal. Pick $h \in H_1 \cap H_2$ and $g \in G$. As $h \in H_1$ and H_1 is normal,

$$ghg^{-1} \in H_1.$$

Similarly as $h \in H_2$ and H_2 is normal,

$$ghg^{-1} \in H_2.$$

But then

$$ghg^{-1} \in H_1 \cap H_2.$$

It follows that $H_1 \cap H_2$ is normal.
§15: 1. $(0, 1)$ generates the subgroup $\{0\} \times \mathbb{Z}_4$. The index of $\{0\} \times \mathbb{Z}_4$ inside $\mathbb{Z}_2 \times \mathbb{Z}_4$ is

$$\frac{2 \cdot 4}{4} = 2.$$

Thus the quotient is a finite abelian group of order 2. It must be isomorphic to $\mathbb{Z}_2$. We can also use the first isomorphism theorem. The projection map

$$\pi \colon \mathbb{Z}_2 \times \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \qquad \text{given by} \qquad (a, b) \longrightarrow a,$$

is a homomorphism, with image $\mathbb{Z}_2$. The kernel consists of all elements (a, b) of $\mathbb{Z}_2 \times \mathbb{Z}_4$ such that $a = 0$, so that the kernel is

$$\{0\} \times \mathbb{Z}_4.$$

It follows by the first isomorphism theorem that the quotient group

$$\frac{\mathbb{Z}_2 \times \mathbb{Z}_4}{\{0\} \times \mathbb{Z}_4}$$

is isomorphic to $\mathbb{Z}_2$.
6. $(0, 1)$ generates the subgroup $\{0\} \times \mathbb{Z}$. We use the first isomorphism theorem. The projection map

$$\pi \colon \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \qquad \text{given by} \qquad (a, b) \longrightarrow a,$$

is a homomorphism, with image $\mathbb{Z}$. The kernel consists of all elements (a, b) of $\mathbb{Z} \times \mathbb{Z}$ such that $a = 0$, so that the kernel is

$$\{0\} \times \mathbb{Z}.$$

It follows by the first isomorphism theorem that the quotient group

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\{0\} \times \mathbb{Z}}$$

is isomorphic to $\mathbb{Z}$.
§18: 2. $16 \cdot 3 = 48$. Modulo 32 this is 16.
7. $n\mathbb{Z}$ is indeed a ring, a subring of the integers $\mathbb{Z}$. It is commutative, there is no unity, unless $n = \pm 1$ or $n = 0$. If $n = 0$ then $1 = 0$ inside the ring $0\mathbb{Z} = \{0\}$ and it is not a field. It can only be a field if $n = \pm 1$ in which case $n\mathbb{Z} = \mathbb{Z}$. But even then 2 does not have a multiplicative inverse and so it is never a field.
8. $\mathbb{Z}^+$ is not a ring. The problem is that $\mathbb{Z}^+$ is not a group under addition; for example 1 does not have any additive inverse. If $n \geq 0$ then $n + 1 \geq 1 \neq 0$.
Challenge Problems §15. 39.
(a) $(1, 2, 3) = (1, 3)(1, 2) \in A_n$. By symmetry every 3-cycle belongs to A_n.
(b) We know that every element of A_n is a product of an even number of transpositions. If we arbitrarily pair together every term of the product, it is enough to show that the product of a pair of transpositions is a product of cycles. A pair of transpositions (a, b) and (c, d) comes in three different forms. The set

$$\{\, a, b\} \cap \{c, d\,\}$$

has 2, 1 or 0 elements. Up to symmetry, we therefore get three cases:

$$(a, b),\ (c, d) = \begin{cases} (1, 2) & (1, 2) \\ (1, 3) & (1, 2) \\ (1, 2) & (3, 4). \end{cases}$$

In the first case the product is the identity and there is nothing to prove. In the second case we have

$$(1, 3)(1, 2) = (1, 2, 3),$$

a 3-cycle. Finally in the third case we have

$$(1, 2)(3, 4) = (1, 3, 2)(1, 3, 4),$$

a product of two 3-cycles. It follows that every element of A_n is a product of 3-cycles.
(c) By symmetry we might as well assume that $r = 1$ and $s = 2$, and we want to show that A_n is generated by the set

$$\{\, (1, 2, i) \mid 3 \leq i \leq n \,\}.$$

It is enough to show we get every 3-cycle.

We compute the indicated products:

$$(1,2,i)^2 = (1,i,2) = (2,1,i).$$

so that

$$(1,2,j)(1,2,i)^2 = (1,2,j)(2,1,i) = (1,i,j)$$

and

$$(1,2,j)^2(1,2,i) = (2,1,j)(1,2,i) = (2,i,j).$$

It follows that

$$(1,2,i)^2(1,2,k)(1,2,j)^2(1,2,i) = (2,k,i)(2,i,j) = (i,j,k).$$

Suppose that (a,b,c) is an arbitrary 3-cycle. Consider the cardinality of the intersection

$$\{\,a,b,c\} \cap \{1,2\,\}.$$

If it is two then we have either $(1,2,i)$ or $(2,1,i)$ and we are okay. If it is one then we have either $(1,i,j)$ or $(2,i,j)$ are we are okay. If it is zero we have (i,j,k) and we are okay.

(d) By symmetry we may assume that $(1,2,3) \in N$. Let $g = (1,2)(3,i)$ and $h = (1,2,3)^2 \in N$. Since N is a normal subgroup we have $ghg^{-1} \in N$. Now $(1,2,3)^2 = (2,1,3)$ and so ghg^{-1} is equal to

$$(1,2,i) \in N.$$

By part (c) $N = A_n$.

(e) As N is non-trivial, we may pick $\sigma \in N$ such that σ is not the identity. Consider the cycle type of σ. We may always write σ as a product of disjoint cycles, where the length of the cycles is increasing (so first transpositions, then 3-cycles, etc). If the length of the longest cycle is greater than 3 we are in case II. Otherwise σ is a product of disjoint transpositions and 3-cycles. If there is more than one 3-cycle then we are in case III. If there is one 3-cycle there are either no transposition and we are in case I or we are in case IV. Otherwise σ is a product of transpositions, of which there are least two since σ is even, and we are in case V.

We now check that if we are in one of these five cases then $N = A_n$. Observe that if ρ is in A_n then

$$\sigma^{-1}\rho\sigma\rho^{-1} = \sigma^{-1}(\rho\sigma\rho^{-1}) \in N$$

as N is a normal subgroup. In what follows it is convenient to first compute

$$\sigma^{-1}\rho\sigma$$

and multiply the result by ρ^{-1}. Note that to compute $\sigma^{-1}\rho\sigma$ we conjugate ρ by σ^{-1}.

Case I: $N = A_n$ by part (d).

Case II: Now suppose σ has a cycle of length greater than 3. Then σ has the form

$$\mu(a_1, a_2, \dots, a_r),$$

where $r > 3$ and μ fixes $a_1, a_2, \dots, a_r$. As $\rho = (a_1, a_2, a_3) \in A_n$ we must have

$$\sigma^{-1}\rho\sigma\rho^{-1} = (a_r, a_1, a_2)(a_1, a_3, a_2) = (a_1, a_3, a_r) \in N.$$

But then we are in case I and $N = A_n$.

Case III: Now suppose that σ has no cycle of length greater than 4 but it is a product of at least two 3-cycles. As the 3-cycles at the end we have

$$\sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3),$$

where μ fixes $a_1, a_2, \dots, a_6$. As $\rho = (a_1, a_2, a_4) \in A_n$ we must have

$$\sigma^{-1}\rho\sigma\rho^{-1} = (a_3, a_1, a_6)(a_2, a_1, a_4) = (a_1, a_4, a_2, a_6, a_3) \in N.$$

Thus N contains a 5-cycle and so we are in case II. But then $N = A_n$.

Case IV: Now suppose that σ is a product of transpositions and one 3-cycle. As the 3-cycle is at the end

$$\sigma = \mu(a_1, a_2, a_3),$$

where μ is a product of disjoint transpositions, which fix a_1, a_2 and a_3. Then

$$\begin{aligned}\sigma^2 &= \mu(a_1, a_2, a_3)\mu(a_1, a_2, a_3)\\ &= \mu^2(a_1, a_2, a_3)^2\\ &= (a_2, a_1, a_3) \in N.\end{aligned}$$

Thus N contains a 3-cycle and we are in case I. But then $N = A_n$.

Case V: Now we suppose that σ is a product of an even number of disjoint transpositions. We may write

$$\sigma = \mu(a_3, a_4)(a_1, a_2),$$

where μ is a product of an even number of disjoint transpositions, which fix a_1, a_2, a_3 and a_4. As $\rho = (a_1, a_2, a_3) \in A_n$ we must have

$$\sigma^{-1}\rho\sigma\rho^{-1} = (a_2, a_1, a_4)(a_2, a_1, a_3) = (a_1, a_3)(a_2, a_4) \in N.$$

Thus $\alpha = (a_1, a_3)(a_2, a_4) \in N$. As $n \geq 5$, we may pick

$$i \notin \{\, a_1, a_2, a_3, a_4 \,\} \qquad \text{where} \qquad i \leq n.$$

Let $\beta = (a_1, a_3, i) \in A_n$. Then

$$\alpha\beta\alpha^{-1}\beta^{-1} = (a_3, a_1, i)(a_3, a_1, i) = (a_1, a_3, i) \in N.$$

But then we are in case I and $N = A_n$.