Solutions to the exercises in the script

1 Groups

1.1 Proof of Proposition 1.2

1. Suppose u, v are both neutral. Then $u + v = u$ as v is neutral and at the same time $u + v = v$ as u is neutral. So $u = v$.
2. Suppose $g+h = e$ and $g+k = e$. Since g has an inverse, we have $(-g)+(g+h) = (-g)+e$ and $(-g)+(g+k) = (-g)+e$. Apply associativity to both of these then use that $((-g)+g) = e$ to get $e + h = e + k$ but since e is neutral we now have $h = k$.
3. In full detail (and the same with g on the right):

$$\begin{array}{rcl|l} g+h & = & g+k & \text{add } (-g) \text{ on left} \\ (-g)+(g+h) & = & (-g)+(g+k) & \text{assoc.} \\ ((-g)+g)+h & = & ((-g)+g)+k) & \text{inverses} \\ e+h & = & e+k & \text{neutral} \\ h & = & k & \text{QED.} \end{array}$$

1.2 Basic Groups

1. It has a neutral element 0 (well, some people don't include 0 in $\mathbb{N}$ but I do) and addition is associative. But there are no inverses of nonzero elements.
2. The neutral element is 1 as $1x = x$ for all x. But since $0x = 0$ for all x too, there cannot be an inverse a of 0 such that $(0a)1 = 1$ since $(0a)1 = 0(a1) = 0$ and $0 \neq 1$. Of course $\mathbb{Q}$ becomes a group under multiplication if we throw out 0.
3. A group has to have a neutral element.
4. Yes, $(\{e\}, +)$ with $e + e = e$. The one element is neutral and, like all neutral elements, its own inverse.
5. It must have two distinct elements $\{e, f\}$ of which one is neutral (by definition) and if e is the neutral one then $e + e = e$ and $e + f = f + e = f$ since e is neutral, that leaves $f + f$ which must be e. Otherwise, we'd have $f + e = f + f$ which would (with the last exercise) give us $e = f$. So the addition table is

$+$	e	f
e	e	f
f	f	e

1.3 Basic properties of groups

	$+$	$-$	$\times$	$\div$
associative	y	n	y	n
commutative	y	n	y	n
has neutral el.	y	y	y	n
has inverses	y	y	n	n
is group operation	y	n	n	n

1.4 Addition tables

The key to all of these is the "sudoku" rule: in any row or column an element cannot repeat. For example if you had $A + C = B$ and also $A + D = B$ then you could add the inverse of A to get $C = (-A) + B = D$ so $C = D$ which is a contradiction. Deriving this from the group axioms was an earlier exercise.

In the first table, since $\clubsuit + \spadesuit = \clubsuit$ then $\spadesuit$ must be the neutral element: there must be a neutral element e, and $\clubsuit + e = \clubsuit$ must hold, therefore $e = \spadesuit$ by the cancellation law. This gets us to the following partial table:

$+$	$\spadesuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$
$\spadesuit$	$\spadesuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$
$\clubsuit$	$\clubsuit$			
$\diamondsuit$	$\diamondsuit$		$\spadesuit$	
$\heartsuit$	$\heartsuit$			$\spadesuit$

From here on we can use the "sudoku" rule. For example the second row/column are immediate, which forces the remaining two elements as well.

$+$	$\spadesuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$
$\spadesuit$	$\spadesuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$
$\clubsuit$	$\clubsuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$
$\diamondsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$	$\clubsuit$
$\heartsuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$	$\spadesuit$

For the second one we have $C + B = C$ so B is neutral. Once we've filled in the B row/colums the "sudoku" rule gives us the rest.

$+$	A	B	C	D	E
A	D	A	B	E	C
B	A	B	C	D	E
C	B	C	E	A	D
D	E	D	A	C	B
E	C	E	D	B	A

1.5 Labelling with numbers

- The $ABCDE$ group has order 5 and we could use the following labelling(that we'll later call an "isomorphism"). While $B = 0$ is forced, we could set any of the other four elements to be 1 so there are four different valid labellings in total (because every nonzero element of $(\mathbb{Z}_5, +)$ is a generator).

A	B	C	D	E
1	0	4	2	3

The four-suits group has four elements but every element has order 2 (or 1 for the neutral element as always). Yet in $\mathbb{Z}_4$ the elements $1, 3$ have order 4. What we've actually shown is that the four-suits group and $\mathbb{Z}_4$ are not isomorphic; the four-suits one is in fact isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

1.6 Division with remainder

1. $17 \cdot 15 = 255$ so we have $256 = 17 \cdot 15 + 1$.
2. Take $n = 4$ and $a = 1, b = 3$. Then $[a + b]_n = [4]_n = 0$ but $[a]_n + [b]_n = 1 + 3 = 4$. The point is that $+$, unlike $+_n$, means plain old addition in $\mathbb{Z}$.
3. We have $(q, r) + +(q', r') := (q + q' + \delta, [r + r']_n)$ where $\delta = 1$ if $r + r' \geq n$ and 0 otherwise. If we think of a number in base n then r is the last digit and q all the other digits; δ is the carry from the r to the q component.

   Since $(q, r) = q \cdot n + r$ we always have $(q \cdot n + r) + (q' \cdot n + r') = (q + q') \cdot n + (r + r')$ but the value of $r + r'$ can itself be greater or equal to n in which case it is no longer the remainder and we need to carry one over to the q part.

   The neutral element is $(0, 0) = 0$ and the inverse of (a, b) is $((-a), n - b)$ since $(a \cdot n + b) + ((-a) \cdot n + (n - b)) = 0$.

2 Subgroups

2.1 Generators of $\mathbb{Z}$

The other generator is (-1) since $(-1) \cdot (-1) = 1$.

2.2 Small orders and small groups

1. In $(\mathbb{Z}_4, +_4)$ the identity 0 has order 1, the element 2 has order 2 and elements $\{1, 3\}$ have order 4.

   In $(\mathbb{Z}_5, +_5)$ the identity 0 still has order 1 but all other elements $\{1, 2, 3, 4\}$ have order 5.

   In $(\mathbb{Z}_6, +_6)$ the identity 0 also has order 1 (as it does in *any* group), the element 3 has order 2, elements $\{2, 4\}$ have order 3 and $\{1, 5\}$ have order 6.

2. If x has order 1 in $(G, +)$ then $\langle x \rangle = (\{x\}, +)$ since we know that x is in this subgroup and we know it contains only one element. But we also know that a subgroup contains the neutral element e of G, hence $x = e$.

3. By Lagrange, the order of an element x must divide the order of the group. If the group order is a prime p then the divisors are $\{1, p\}$; the only element of order 1 is the identity as we have just established above. So any other element must have order p and therefore generate the whole group. For example, in $(\mathbb{Z}_7, +_7)$ the elements $\{1, 2, 3, 4, 5, 6\}$ all have order 7 and are generators.

2.3 The L block

1. There are obviously exaclty four elements in this group. A possible set of representatives is $\{\varepsilon, A, AA, AAA\}$ with ε the empty string; another one is $\{\varepsilon, A, AA, B\}$. Any set of four elements that covers all four rotations will do.

2. The cancellation rules are:

   a) Four of the same in a row cancel, so $AAAA \Rightarrow \varepsilon$ and $BBBB \Rightarrow \varepsilon$.

   b) AB and BA both cancel to ε.

   c) $B \Rightarrow AAA$. Alternatively one could use $A \Rightarrow BBB$ or $AAA \Rightarrow B$ depending on which representative set one has chosen.

   If we take these rules (with the first alternative for the third one) then any fully reduced word will be in the set $\{\varepsilon, A, AA, AAA\}$. First of all, a fully reduced word cannot contain both As and Bs as we could reduce further with rule 2. If we only have As left then by rule 1 we have at most three of them. If we have nothing left

at all (e.g. the original word was AB) then we are also done. The remaining case is that there are only Bs left but we could reduce these by applying rule 3 and then we are back in the case of only As.

Under these rules, $AAA \stackrel{*}{\Rightarrow} AAA$, $ABABA \stackrel{*}{\Rightarrow} A$, $AAAA \stackrel{*}{\Rightarrow} \varepsilon$ and $BBBBA \stackrel{*}{\Rightarrow} A$. Here the $(*)$ means that there is a sequence of $\Rightarrow$ steps that turns the original word into the final one.

3. Just take the number of As: $\varepsilon = 0$, $A = 1$, $AA = 2$, $AAA = 3$.

4. There are now 8 elements, the four from before and four rotations for the mirrored block. As representatives we could chose $\{\varepsilon, A, AA, B, X, AX, AAX, BX\}$ for example. We get new reduction rules $XX \Rightarrow \varepsilon$ and $AX \Leftrightarrow XB, BX \Leftrightarrow XA$ which we can use to make sure every word contains at most one X and if so, then the X is the last character in the word.

   The only candidate $\mathbb{Z}_n$ group is $(\mathbb{Z}_8, +_8)$ but this has elements of order 8, for example 1. If we compute the orders of all elements in our group, the highest one is 4. So there's no element that we can map to 1 in $\mathbb{Z}_8$ without wrecking the addition property.

5. We can use one bit x to record if the block is "standing" (3 blocks high, $x = 1$) or "sitting" (2 blocks high, $x = 0$) and one bit y that is 1 if it is a Z (mirrored) and 0 if it is a S. Then we represent a position of the block as xy. Our transformations are now:

00	do nothing
01	reflect around a vertical axis
10	rotate 90 degrees
11	rotate then reflect

   And we can see that for any two transformations, composing them results in the bitwise XOR of their codes.

2.4 Free groups

1. The neutral element is the empty string which we can write ε.

2. It is associative since $(x+y)+z$ and $x+(y+z)$ both involve writing out the string xyz and then reducing. If we didn't reduce then associativity would be obvious. The property that we really need here is that whatever order we reduce in, we get the same result. The proof is beyond the scope of this unit.

   It has a neutral element as we observed above. It also has inverses: the inverse of a word w is w reversed with each letter replaced by its anti-letter. Call this $\overline{\overline{w}}$. If $w = c_1 \ldots c_n$ then $w + \overline{\overline{w}} = [c_1 \ldots c_n \overline{c_n} \ldots \overline{c_1}]$ which reduces to ε in n steps (a full proof would use induction). Therefore we have a group.

3. The group generated by the original letters $\{A, B, C, \ldots\}$ is the set of all elements that we can make by forming strings of these letters *and their inverses*, which gives us all the words in the free group.
4. $A + B \neq B + A$ for example as the strings AB and BA are different and both fully reduced.
5. Set $\varepsilon = 0, A = 1, AA = 2, \ldots, \overline{A} = (-1)$ and so on. The number is simply the number of As (where anti-As count negatively).

2.5 Free groups via equivalence relations

- $w \sim w$ for any word w, by performing zero changes. So $\sim$ is reflexive.
- $w \sim u$ implies $u \sim w$ by performing the opposite steps (add becomes remove and vice versa) in opposite order. So $\sim$ is symmetric.
- $w \sim u$ and $u \sim v$ imply $w \sim v$, you can first perform the steps to turn w into u and then the steps to turn u into v.

This gives us an equivalence relation. Each equivalence class obviously contains at least one word as that's the way we defined the classes. If a class contains a word w of length n then we can repeatedly remove the first instance in w where a letter is paired with its anti-letter; this process will terminate after at most n steps because each step can only shorten the word. This is also called *fully reducing* the word w.

2.6 Permutations — the case $n = 3$

1. There are 6 of them:
$$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$
2. For example,
$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$
3. We have
$$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = () \quad \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} = (01) \quad \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = (021)$$
$$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix} = (12) \quad \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = (012) \quad \begin{pmatrix} 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix} = (02)$$

4. The addition table is the following with pq the element in row p and column q.

+	()	(01)	(02)	(12)	(012)	(021)
()	()	(01)	(02)	(12)	(012)	(021)
(01)	(01)	()	(021)	(012)	(12)	(02)
(02)	(02)	(012)	()	(021)	(01)	(12)
(12)	(12)	(021)	(012)	()	(02)	(01)
(012)	(012)	(02)	(12)	(01)	(021)	()
(021)	(021)	(12)	(01)	(02)	()	(012)

5. Any S_n for $n \geq 3$ contains S_3 as a subgroup. A group that contains a non-commutative subgroup contains two elements a, b with $ab \neq ba$ (in the subgroup) so it cannot be commutative.

   S_1 is the group with one element and S_2 is the group with two elements $\{(), (01)\}$ with $(01)(01) = ()$. Both of these are commutative.

2.7 Permutations in general

- $pq = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}$ and $qp = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix}$.
- pq has order 4 (cycle of order 4) and qp has order 4 too.
- $pq = (2354)$ and $qp = (1453)$.
- $(154) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}$, $(12)(54) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ and $(1254)(4531) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$.

3 Rings and Multiplication

3.1 Arithmetic modulo primes

1. 702
2. 1009 is a prime so the order of 7 (and any other nonzero element) is 1009.

3.2 Addition and multiplication tables

- $(\mathbb{Z}_5, +, \cdot)$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- $(\mathbb{Z}_4, +, \cdot)$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- $(\mathbb{Z}_4^\times, \cdot)$: We see in the last example that the only elements left are $\{1, 3\}$.

·	1	3
1	1	3
3	3	1

3.3 Arithmetic modulo n

1. $\{13\}$. We have $5 \cdot 13 = 65 = 4 \cdot 16 + 1$.
2. $\{\}$. The value $6 \cdot y$ is even modulo 16 for all y.
3. $\{0, 2, 4, 6, 8, 10, 12, 14\}$. Since $8 \cdot 2 = 0$ the same must hold for all its multiples.

3.4 Euler's ϕ function

1. 1008 since $\phi(p) = p - 1$ for primes p.

2. $64 = 2^6$ so $\phi(64) = 2^5 = 32$. Indeed, the elements of $\mathbb{Z}_{64}^{\times}$ are exactly the odd numbers less than 64.
3. $60 = 2^2 \cdot 3 \cdot 5$ so $\phi(60) = 16$.

3.5 Euclid's algorithm

1. We perform the extended Euclidean algorithm:

q	r	a	b
64	0	1	0
13	0	0	1
0	13	1	0
4	12	-4	1
1	1	5	-1
12	0	-64	13

   So $5 \cdot 13 + (-1) \cdot 64 = 1$.

2. We compute the extended Euclidean algorithm on 1009 and 5:

q	r	a	b
1009	0	1	0
5	0	0	1
201	4	1	-201
1	1	-1	202
4	0	5	-1009

   This gives us $(-1) \cdot 1009 + 202 \cdot 5 = 1$ which means $202 \cdot 5 \equiv 1 \pmod{1009}$.

3. Another extended Euclidean algorithm gives us $101 \cdot 10 \equiv 1 \pmod{1009}$ — which we could also find just by observing that $101 \cdot 10 = 1010 = 1009 + 1$.

   For the second equation we first find that $25 \cdot 444 \equiv 1 \pmod{1009}$. This means that $y = (98 - 6) \cdot 444 = 488$.

3.6 Classification of ring elements

1. 0 is zero, everything else is a unit.
2. 0 is zero, the nonzero even numbers are zero-divisors, the odd ones are units.
3. 0 is still zero, the elements $\{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}$ are coprime to 60 so they are units, the rest are zero-divisors.
4. 0 is zero, $\{(-1), 1\}$ are units and the rest are neither.

3.7 Fields modulo primes

We know that any $(\mathbb{Z}_n, +, \cdot)$ is a finite commutative ring so every nonzero element is either a unit or a zero-divisor. When n is prime, there cannot be any zero-divisors as $\gcd(a, n) = 1$ for any $a \neq 0$ when n is a prime. So they are all units.

3.8 Exponentiation modulo n

We compute modulo 1009:

$2^2 = 4$
$2^4 = (2^2) \cdot (2^2) = 4 \cdot 4 = 16$
$2^8 = (2^4) \cdot (2^4) = 16 \cdot 16 = 256$
$2^{16} = 256 \cdot 256 = 960$
$2^{32} = 960 \cdot 960 = 383$
$2^{64} = 383 \cdot 383 = 384$
$2^{128} = 384 \cdot 384 = 142$

So our solution is 141.

4 Polynomials

4.1 Polynomials modulo 7

1. $3X^3 + 2X^2 + 5$
2. $3X^5 + 6X^4 + 3X^3 + 2X^2 + 6X + 4$

4.2 Division with remainder

- quotient $X^3 + 3X + 1$, remainder $5X + 3$
- quotient $X^2 + 4$, remainder 0
- quotient $5X^2 + 6$, remainder 0

4.3 Division without remainder

1. The roots are 4 and 5. The first two linear factors match these roots since $2 = (-5)$ and $3 = (-4)$. The next three are just multiples: $(2X + 4) = 2(X + 2)$ and so on, similar to what we get over the rationals where e.g. $(X + 1)(X - 1) = (2X + 2)(X/2 - 1/2)$. The difference over a finite field is that for example $2 = 1/4$ so our "fractions" are "integers" too. Finally, $(3X - 1) = (3X + 6)$ modulo 7.
2. Over the rationals or reals, $(X+1)(X-1) = (2X+2)(X/2-1/2) = (aX+a)(X/a-1/a)$ for any nonzero a, for example.

4.4 The relation $\sim_p$

Over a field $\mathbb{F}$ with a polynomial $p \in \mathbb{F}[X]$, for such polynomials a, b, c we have

- $a \sim_p a$ since $a + 0 \cdot p = a$, so it's reflexive.
- If $a \sim_p b$ then $a + p \cdot q = b$ for some q therefore $b + p \cdot (-q) = a$ so $b \sim_p a$ too and it's symmetric.
- From $a \sim_p b$ and $b \sim_p c$ we get values q, r such that $a + pq = b$ and $b + pr = c$ therefore $a + p(q + r) = c$ and $a \sim_p c$ so it's transitive.

Since we never had to divide by anything, this must also hold over rings.

5 Homomorphisms

5.1 Trivial homomorphisms

- There is exactly one homomorphism $\mathbb{Z}_n \to \{0\}$ and it sends all elements to 0 since that is the only element in its range. In the other direction, since homomorphisms must map the neutral element to the neutral element, there is exactly one homomorphism and it maps 0 to 0.
- The condition that it maps neutral to neutral is obviously satisfied. As for $f(a +_G b) = f(a) +_H f(b)$, the left hand side is e_H and the right hand side is $e_H +_H e_H = e_H$ too. Similarly $e_H = f(-a) = -f(a) = e_H$ for all $a \in G$.
- The other trivial one is the identity map. (If the group has only one element then this is the same as the one that maps everything to the neutral element.)

5.2 Group homomorphisms and orders

- In $(\mathbb{Z}_2, +_2)$ the element 1 has the property that $1 + 1 = 0$ so for any homomorphism we'd have $f(1) +_3 f(1) = f(1 +_2 1) = 0$ too. But the only element of $\mathbb{Z}_3$ with this property is 0. In the other direction one can make the same argument using $1 + 1 + 1 = 0$.
- There is a homomorphism $\mathbb{Z}_2 \to \mathbb{Z}_4$ that sends $0 \mapsto 0, 1 \mapsto 2$ and in the other direction, for example one could map $\{0, 2\}$ to 0 and $\{1, 3\}$ to 1.
- We have $f(g +_G \ldots +_G g) = f(g) +_H \ldots +_H f(g) = h +_H \ldots +_H h$. To be exact, we should show this by induction over the number of copies of g in the addition. But the left-hand side is $f(0_G)$ which must be 0_H.
- The map $f : (\mathbb{Z}_n, +_n) \to (\{0\}, +_1)$ sends everything to 0 which has order 1, including the element 1 that originally had order n. For a non-trivial example, the map $\mathbb{Z}_4 \to \mathbb{Z}_2$ considered above sends $1 \mapsto 1$ but in $\mathbb{Z}_4$ the element 1 had order 4 but in $\mathbb{Z}_2$ it has order 2.

It is convenient to write $n \star g$ for $\underbrace{g + \ldots + g}_{n \text{ times}}$ when $n > 0$ and to set $0 \star g := e_G$ and $z \star g := (-z) \star (-g)$ for $z < 0$. Note that $\star$ is a map $\mathbb{Z} \times G \to G$, so not a "multiplication" in the usual sense because its operands some from different spaces. It is however very similar to scalar multiplication in a vector space. It satisfies $n \star (m \star g) = (n \cdot m) \star g$ and $(m + n) \star g = m \star g + n \star g$ and, for any elements $g, k \in G$ with $g + k = k + g$ also $n \star (g + k) = n \star g + n \star k$.

Suppose that $f : (G, +_G) \to (H, +_H)$ is a homomorphism and that $g \in G$ has order n and $h = f(g) \in H$ has order m. We already know that $n \star h = 0$ so $m \leq n$, in particular if n is finite then m is finite too.

We can find integers a, b with $an + bm = \gcd(n, m)$ with the extended Euclidean algorithm. We compute $(an + bm) \star h = (a \star (n \star h)) + (b \star (m \star h))$ but $m \star h$ and $n \star h$ are both e_H, the former because m is the order of h and the latter because it is the order of g and we discussed this case above. Therefore $\gcd(m, n) \star h = e_H$. Since we defined m to be the order of h this means that m is the smallest nonzero integer satisfying $m \star h = e_H$ therefore $m = gcd(m, n)$ as the gcd of two integers cannot be bigger than any of the two. Since the gcd of two integers divides both these integers, we conclude that m divides n.

5.3 Isomorphisms preserve group orders

The order of an element g is the smallest positive integer n such that $g + \ldots + g$ (repeated n times) is the neutral element. We will write this sum as $n \star g$ and define $0 \star g$ to be the neutral element e_G, this gives us a map $\star : \mathbb{N} \times G \to G$.

Claim: if f is an isomorphism then $n \star f(g) = e_H$ if and only if $n \star g = e_G$. This is enough to conclude that the orders are the same. Proof: if $n \star g = e_G$ then $f(n \star g) = f(e_G) = e_H$ and $f(n \star g) = f(g +_G \ldots +_G g) = f(g) +_H \ldots +_H f(g) = n \star f(g)$ since f is a homomorphism. In the other direction, since f is an isomorphism there is another isomorphism u such that $u(f(g)) = g$ and we can do the same calculation again: $u(n \star f(g)) = n \star u(f(g)) = n \star g$.

To be really precise, the arguments involving ... would have to be done by induction (this holds generally in mathematics for most arguments involving ... symbols) and we should have defined two separate maps $\star_G$ and $\star_H$.

5.4 Isomorphisms between additive and multiplicative groups

- The subgroup is $\langle 2 \rangle = \{2, 4, 1\}$ where 1 is the neutral element. One isomorphism is $1 \mapsto 0, 2 \mapsto 1$ and $4 \mapsto 2$. This map is certainly bijective; to show that it (and its inverse) are homomorphisms we write out the operation tables and check that the map transforms one table into the other one.

$\cdot_7$	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

- The other isomorphism is the map $1 \mapsto 0$, $2 \mapsto 2$ and $4 \mapsto 1$. This is forced as the old neutral element 1 must become the new one 0 and that leaves only one other possibility (which we can again check is really an isomorphism by writing out the operation tables).
- Since $f(1) = 2$ we must have $f(1+1) = 2 \cdot_{11} 2 = 4$, $f(3) = 8$, $f(4) = 5$ (which is 16 mod 11) and so on. The formula is $f(x) = 2^x \pmod{11}$ and it is a homomorphism

because of the law $2^a \cdot 2^b = 2^{a+b}$ which still holds when we reduce modulo a positive integer. It is an isomorphism because it has an inverse and the inverse is also a homomorphism.

For this particular example we can just write out the operation tables (or get a computer to do it for us) and then check all 100 cases. In general, the inverse of the map $x \mapsto a^x \pmod n$ is called the *discrete logarithm* to base a and written $x = \log_a(y) \pmod n$, satisfying the usual laws such as $\log_a(u \cdot v) \pmod n = \log_a(u) + \log_a(v) \pmod n$ which is what we need to show that the other direction is a homomorphism too. As expected we have $2^0 = 1 \pmod{11}$) and $\log_2(1) = 0 \pmod{11}$; we can't take a logarithm of 0 because 0 is not in $\mathbb{Z}_{11}^\times$.

5.5 Another decomposition

$0 = (0,0)$ $1 = (1,1)$ $2 = (2,2)$ $3 = (3,0)$
$4 = (0,1)$ $5 = (1,2)$ $6 = (2,0)$ $7 = (3,1)$
$8 = (0,2)$ $9 = (1,0)$ $10 = (2,1)$ $11 = (3,2)$

5.6 Group automorphisms

- Since 0 has to map to 0 that leaves $0 \mapsto 0, 1 \mapsto 2, 2 \mapsto 1$ as the only option which we can check is really an automorphism by writing out the operation table.
- $(\mathbb{Z}_5, +_5)$ is a prime-order group so every nonzero element is a generator and the automorphisms are the maps $x \mapsto cx$ for $c \in \{1,2,3,4\}$:
  - $0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3, 4 \mapsto 4$
  - $0 \mapsto 0, 1 \mapsto 2, 2 \mapsto 4, 3 \mapsto 2, 4 \mapsto 3$
  - $0 \mapsto 0, 1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 4, 4 \mapsto 2$
  - $0 \mapsto 0, 1 \mapsto 4, 2 \mapsto 3, 3 \mapsto 2, 4 \mapsto 1$

  These are homomorphisms since $c(x+y) = cx + cy$ and these are the only automorphisms since if $f(1) = c$ then $f(2) = f(1+1) = c + c = 2c$ and so on, making the map $f(x) = cx$.

  The automorphism group of $\mathbb{Z}_5$ is therefore isomorphic to $\mathbb{Z}_4$ since it has 4 elements, two of which have order 4. An explicit isomorphism is for example

$Aut(\mathbb{Z}_5)$	$f(x) = x$	$f(x) = 2x$	$f(x) = 3x$	$f(x) = 4x$
$\mathbb{Z}_4$	0	1	3	2

  For $(\mathbb{Z}_6, +_6)$ the element 3 has order 2, $\{2,4\}$ have order 3 and $\{1,5\}$ have order 6. Again if we know $f(1) = c$ then $f(x) = cx$ for all x since we can write x as a sum of 1s. But the only elements c that we can possibly map 1 to are $\{1,5\}$ so we get these two:

- The identity $f(x) = x$
- $f(x) = 5x$, which is actually another way of saying $f(x) = (-x)$.

and the automorphism group is isomorphic to $\mathbb{Z}_2$.

- All 3 nonzero elements have order 2 so there are 6 bijective functions with signature $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ that send $(0, 0)$ to $(0, 0)$ namely

x	(0,0)	(0,1)	(1,0)	(1,1)
$f_1(x)$	(0,0)	(0,1)	(1,0)	(1,1)
$f_2(x)$	(0,0)	(0,1)	(1,1)	(1,0)
$f_3(x)$	(0,0)	(1,0)	(0,0)	(1,1)
$f_4(x)$	(0,0)	(1,0)	(1,1)	(0,0)
$f_5(x)$	(0,0)	(1,1)	(1,0)	(0,1)
$f_6(x)$	(0,0)	(1,1)	(0,1)	(1,0)

All of these are automorphisms. If we write the nonzero elements as a, b, c then another way to think of $\mathbb{Z}_2 \times \mathbb{Z}_2$ is as the group defined by the following three rules: $x + x = 0$ for any x; $x + 0 = x$ for any x and in the remaining case the sum of two distinct nonzero elements is the third one i.e. $a + b = c$ etc. None of a, b, c are in any way distinguished from the others. The 6 maps are just the permutations of the set $\{a, b, c\}$ so $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$, the permutation group on 3 elements.

5.7 Finite field inversion

Since $p = 1033$ is prime, the order of the multiplicative group modulo p is $p - 1 = 1032$ (which is $\phi(p)$). Therefore $3^{1032} = 1 \pmod{p}$ and so $a = 3^{1031} \pmod{p}$ is the multiplicative inverse since it satisfies the equation $3a = 1 \pmod{p}$.

We expand the exponent in binary to get (modulo 1033)

$$a = 3^{(2^{10}+2^2+2^1+2^0)}$$

We compute the following chain by squaring and reducing

$3^{(2^0)}$	3	
$3^{(2^1)}$	9	
$3^{(2^2)}$	81	
$3^{(2^3)}$	363	$(= 81 \cdot 81 \pmod{1033})$
$3^{(2^4)}$	578	
$3^{(2^5)}$	425	
$3^{(2^6)}$	883	
$3^{(2^7)}$	807	
$3^{(2^8)}$	459	
$3^{(2^9)}$	982	
$3^{(2^{10})}$	535	

So we have

$$a = 3 \cdot 9 \cdot 81 \cdot 535 = 689$$

and indeed, $3 \cdot 689 = 1 \pmod{1033}$.

6 Finite Fields

6.1 Irreducibles and units

If both a and b are units then there are values u, v with $au = ua = 1$ and $bv = vb = 1$. But now $abvu = a(bv)u = a1u = au = 1$ and similarly $vuab = 1$ so ab is a unit too.

6.2 Irreducible polynomials

1. Degree 2 has only one: X^2+X+1. In degree 3 we have X^3+X+1 and X^3+X^2+1. One way to find these is for each candidate polynomial p to check that $p(0)$ and $p(1)$ are both nozero — which means $p(0) = p(1) = 1$ over $GF(2)$.
2. For example X^4+X+1. There are two more, X^4+X^3+1 and $X^4+X^3+X^2+X+1$ which can be found with the same idea as above.

   Additional remark: since $1^n = 1$ for any $n > 0$ and since the constant term must be 1 to make $p(0) = 1$, an irreducible polynomial over $GF(2)[X]$ must have an odd number of nonzero coefficients in order that $p(1) = 1$. For degrees 2 and 3, this condition is necessary and sufficient as such a polynomial can only be reducible if it has a linear factor. From degree 4 onwards the condition is only necessary, not sufficient: $X^4 + X^2 + 1$ is not irreducible, it is the square of the degree-2 irreducible $X^2 + X + 1$.
3. $X^2 + 1, X^2 + X + 2, X^2 + 2X + 2, 2X^2 + 2, 2X^2 + X + 1, 2X^2 + 2X + 1$.

   Remark: the first three with leading coefficient 1 are monic irreducibles, the other three are the monic ones multiplied by 2. In general, one can find the monic irreducibles first, then the irreducibles with leading coefficient a (for a a unit) are the monic ones multiplied by a. This is because multiplying with a unit does not change whether a polynomial is irreducible or not.

   For the monic ones, we can again test all degree-3 candidates to see when $p(0)$, $p(1)$ and $p(2)$ are all nonzero.
4. For example $X^3 + X + 1$. (There are 40 in total of which 10 are monic.)

6.3 Not an automorphism

If $v = 0$ then all 49 elements $\{a + bX \mid a, b \in GF(7)\}$ get mapped to the 7-element set $GF(7)$ as the map "removes the Xes". This cannot be bijective, so it's not an isomorphism.

6.4 The field $GF(5^2)$

1. $(a, b) \cdot (c, d) = (ac + 2bd, ad + bc + 3bd)$.
2. $(a, b) \cdot (c, d) = (ac + 2bd, ad + bc + 3bd)$. The formula is the same because this polynomial is 2 times the last one (and 2 is a unit).
3. One of the isomorphisms is the identity map since the multiplication is the same in both cases. The other is $X \mapsto 4Y + 3$ which is $(a, b) \mapsto (a + 3b, 4b)$.

   There are three ways to find these isomorphisms. One can calculate them by hand as in the example above (which should give $u = 0, v = 1$ and $u = 3, v = 4$), one can use the factoring approach given at the end of the section or one can note that the two irreducible polynomials are the same up to a unit, so it's really an automorphism and the second one must be the Frobenius map.

6.5 Computation in $GF(2^8)$

- $X^6 + X^5 + 1$
- What we really want to do is divide $(X^3 + X + 1)$ by $(X^5 + 1)$, or rather multiply it by the inverse of $(X^5 + 1)$. Since there are $255 = 2^8 = 1$ nonzero elements, each one must satisfy $a^{255} = 1$ and therefore $a^{-1} = a^{254}$. We calculate that $(X^5 + 1)^{254} = X^6 + X^5 + X^3 + X^2 + X$ and our solution is $(X^6 + X^5 + X^3 + X^2 + X)(X^3 + X + 1) = X^7 + X^6 + X^5 + X^3 + X^2 + X + 1$.

  The point of this question is that solving linear equations in finite fields is exactly the same process as solving linear equations in the real numbers: subtract/divide until the variable stands alone on one side of the equation. It's only the "numbers" that work differently.
- The powers are the following. Note that $\phi^3(Z)$ means $\phi(\phi(\phi(Z)))$, not $\phi(Z)^3$.

  $\phi\ (Z) = Z^2$
  $\phi^2(Z) = Z^4$
  $\phi^3(Z) = Z^7 + Z^2 + Z + 1$
  $\phi^4(Z) = Z^6 + Z^5 + Z^3 + Z^2 + Z + 1$
  $\phi^5(Z) = Z^4 + Z^3 + Z^2 + 1$
  $\phi^6(Z) = Z^7 + Z^6 + Z^4 + Z^2 + Z$
  $\phi^7(Z) = Z^5 + Z^4 + Z^2$
  $\phi^8(Z) = Z$
- Using the factoring approach: one of the isomorphisms sends $Z \mapsto X^5 + X^2 + X + 1$. (There are 8 in total.)

6.6 Computation in $GF(2^3)$

1. $X+1$, X^2+X, Y^2+1 and Y^2+Y+1.
2. It has 3 elements (the extension degree is 3) and they are the identity, the Frobenius map and the inverse Frobenius map (which is also ϕ^2).
3. $\phi(X) = X^2$ and $\phi(X^2) = X^2+X$ so $\phi(aX^2+bX+c) = (a+b)X^2+aX+c$.

   $\phi(Y) = Y^2$ and $\phi(Y^2) = Y^2+Y+1$ so $\phi(aY^2+bY+c) = (a+b)Y^2+aY+(a+c)$.
4. $\phi^2(aX^2+bX+c) = bX^2+(a+b)X+c$ and $\phi^2(aY^2+bY+c) = bY^2+(a+b)Y+(b+c)$. ϕ^3 is the identity in both cases.
5. There are three isomorphisms:

$f(X)$	$f(aX^2+bX+c)$
$Y+1$	$aY^2+bY+(a+b+c)$
Y^2+1	$(a+b)Y^2+aY+(b+c)$
Y^2+Y	$bY^2+(a+b)Y+(a+c)$

6. $$(aX^2+bX+c)(dX^2+eX+f) =$$
   $$(af+be+cd+ad)X^2+(bf+ce+ae+bd)X+(cf+ae+bd)$$

   and

   $$(aY^2+bY+c)(dY^2+eY+f) =$$
   $$(af+be+cd+ae+bd+ad)Y^2+(bf+ce+ad)Y+(cf+ae+bd+ad)$$

7 Vector spaces

7.1 The rest of the example

- From the formula $f_3 = f_2\phi$:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

  So $f_3(X) = 1+Y$, $f_3(X^2) = 1+Y^2$ and $f_3(a+bX+cX^2) = (a+b+c)+bY+cY^2$.

- Using row operations:

$$\begin{array}{c|ccc|ccc|l} 1 & 1 & 1 & 0 & 1 & 0 & 0 & \\ 2 & 0 & 0 & 1 & 0 & 1 & 0 & \\ 3 & 0 & 1 & 1 & 0 & 0 & 1 & \\ 4 & 1 & 0 & 1 & 1 & 0 & 1 & 1+3 \\ 5 & 1 & 0 & 0 & 1 & 1 & 1 & 2+4 \\ 6 & 0 & 1 & 0 & 0 & 1 & 1 & 2+3 \\ 7 & 0 & 0 & 1 & 0 & 1 & 0 & =2 \end{array}$$

  we can read off the inverse

$$f_1^{(-1)} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

7.2 More finite fields

1. We have $\phi(X) = [X^3] = X+2$ and $\phi(X^2) = (X+2)(X+2) = X^2+X+1$ so the matrix is

$$\phi = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

2. The powers are

$$\phi^2 = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$\phi^3 = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

as we would expect since the extension degree is 3.

3. The first row is fixed, the second we read off the exercise and the third we compute by $(2Y^2 + 2Y)^2 = [Y^4 + 2Y^3 + Y^2] = 2Y$.

$$f_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 2 & 0 \end{pmatrix}$$

4. We compute the inverse (we could do this in SAGE but let's do it by hand for once):

1	1	0	0	1	0	0	
2	0	2	2	0	1	0	
3	0	2	0	0	0	1	
4	0	0	2	0	1	1	$2 + 3$
5	0	1	0	0	0	2	[2·]3
6	0	0	1	0	2	2	[2·]4
7	1	0	0	1	0	0	$= 1$
8	0	1	0	0	0	2	$= 5$
9	0	0	1	0	2	2	$= 6$

so

$$f_1^{(-1)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 2 \end{pmatrix}$$

5. The extension degree is 3 so there are three isomorphisms.

6.

$$f_2 = f_1\phi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 1 \\ 0 & 2 & 2 \end{pmatrix}$$

$$f_3 = f_2\phi = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 1 \\ 0 & 2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 2 & 1 \end{pmatrix}$$

7.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$