Tutorial Sheet 1

1 (a) Assume $[a]=[a']$ and $[b]=[b']$. That is, there are $s,t\in\mathbb{Z}$ with $a'=a+sn$ and $b'=b+tn$. Thus $[a+b]=[a'+b']$ since $a+b-(a'+b')=-(s+t)n$ is divisible by n.

(b) Associativity: inherited from $+$ for $\mathbb{Z}$: $([a]+[b])+[c]=[(a+b)+c]=[a+(b+c)]=[a]+([b]+[c])$

Unit: $[0]+[a]=[0+a]=[a]$ for all $a\in\mathbb{Z}$.

Inverses: $[a]+[-a]=[a+(-a)]=[0]$ for all $a\in\mathbb{Z}$.

(Commutativity: $[a]+[b]=[a+b]=[b+a]=[b]+[a]$)

(c) Since $a=\underbrace{1+1+\cdots+1}_{a \text{ summands}}$, we have $[a]=\underbrace{[1]+\cdots+[1]}_{a \text{ summands}}$.

2. (a) Let n be prime, i.e. the only divisors are 1 and n. Then for all $1\le m<n$ we have $\gcd(m,n)=1$ because otherwise the gcd were a non-trivial divisor of n. Thus $\phi(n)=n-1$.

Assume now $\phi(n)=n-1$. This means, that for all $1\le m<n$ we have $\gcd(m,n)=1$, in particular, no element $1<m<n$ is a divisor of n and thus n is prime.

(b) The unique factorisation of p^k is p^k, p is the only prime dividing p^k.

Among $\{1,\dots,p^k-1\}$ every p-th element is divisible by p and thus has gcd >1 with p^k.

Thus, there are p^k-p^{k-1} numbers in the set with $\gcd(m,p^k)=1 \Rightarrow \phi(p^k)=p^k-p^{k-1}$

(c) Denote by "$a \bmod n$" the remainder of a divided by n such that $0\le a \bmod n<n$.

Claim: The map $\pi:\{0,1,\dots,m\cdot n-1\}\longrightarrow\{0,1,\dots,m-1\}\times\{0,1,\dots,n-1\}$

$$a \longmapsto (a \bmod m,\ a \bmod n)$$

is a well-defined bijection.

Proof: Well-defined is clear, both sets have $m\cdot n$ elements.

Assume $a,b\in\{0,1,\dots,m\cdot n-1\}$ and $\pi(a)=\pi(b)$. This means:

$a\equiv b \bmod m$ and $a\equiv b \bmod n$ and thus: $a-b$ is divisible by m and n. Since $\gcd(m,n)=1$ it follows that $a-b$ is divisible by $m\cdot n$. But since $|a-b|\le mn-1$ we must have $a-b=0$ and thus $a=b$.

An injective map between two finite sets of the same cardinality is surjective. □

Note: $\gcd(x,y) = \gcd(x, y+kx)$ for $k \in \mathbb{Z}$, $a \bmod m = a + km$

Claim?: $\gcd(a, mn) = 1$ iff $\gcd(a, m) = 1$ and $\gcd(a \bmod n, n) = 1$.

Proof: Assume $\gcd(mn, a) = 1$ then $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$ ($s \mid m \Rightarrow s \mid mn$).

Assume $\gcd(a \bmod m, m) = 1 = \gcd(a \bmod n, n) \Rightarrow \gcd(a, m) = 1 = \gcd(a, n)$

$\Rightarrow$ No prime divisor of a divides either m or n $\Rightarrow$ no prime divisor of a divides $m \cdot n$.

$\Rightarrow \gcd(a, mn) = 1$.

$$\Rightarrow \phi(mn) = \#\{a \in \{0, 1, \dots, mn-1\} \mid \gcd(a, mn) = 1\}$$
$$= \left|\{a \in \{1, 2, \dots, m-1\} \mid \gcd(a, m) = 1\}\right| \cdot \left|\{a \in \{1, 2, \dots, n-1\} \mid \gcd(a, n) = 1\}\right|$$
$$= \phi(m) \cdot \phi(n).$$

(d) $$\phi(n) = \prod_{i=1}^{r} \phi\left(p_i^{k_i}\right) = \prod_{i=1}^{r} \left(p_i^{q_i} - p_i^{q_i - 1}\right) = \prod_{i=1}^{r} p_i^{q_i} \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

3. (a) $G = \{e, a, a^2, \dots, a^{m-1}\}$

(b) If $d \mid m$ then ~~$\{e, a, \dots, a^{(d-1)m}\} = \langle a \rangle$~~

$\langle a^{m/d} \rangle = \{e, a^{m/d}, a^{2m/d}, \dots, a^{(d-1)m/d}\}$ which has d elements $\Rightarrow$ index $\frac{m}{d}$

$\langle a^d \rangle = \{e, a^d, a^{2d}, \dots, a^{(\frac{m}{d}-1)d}\}$ which has $\frac{m}{d}$ elements $\Rightarrow$ index d

Note: $a^{id} \cdot a^{jd} = a^{(i+j)d} = a^{((i+j) \bmod \frac{m}{d})d}$

Cosets are exactly $a^i \langle a^d \rangle = \{a^{i+jd} \mid 0 \le j < \frac{m}{d}\}$ for $0 \le i < d$, each of which has $\frac{m}{d}$ elements $\Rightarrow d$ cosets.

Let $H \le G$ and a^d be the smallest power of a with $a^d \in H$. Then $\langle a^d \rangle \le H$

Claim: $=$. Let $a^i \in H \setminus \langle a^d \rangle$, then $i = qd + r$ with $0 < r < d$.

But then $a^i \cdot (a^d)^{-q} = a^r \in H \Rightarrow r = 0$ since d was minimal $\Rightarrow$ ↯.

4 (a) We already know that $\mathbb{Z}$ is a commutative ring with identity. Since 2 is not invertible, it is not a field. For integral domain missing: no zero divisors. But since $\mathbb{Z} \subseteq \mathbb{Q}$ is a subring, it does not have zero-divisors.

(b) It is clear that $\mathbb{R}^{2\times 2}$ is an abelian group w.r.t. $+$ since this is inherited from $\mathbb{R}$.
The identity matrix $\begin{bmatrix}1&0\\0&1\end{bmatrix}$ is an identity. We need associativity of the matrix product:

$$\left(\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}\cdot\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix}\right)\cdot\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix} = \begin{bmatrix}a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22}\\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22}\end{bmatrix}\cdot\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix}$$

$$= \begin{bmatrix}a_{11}b_{11}c_{11}+a_{12}b_{21}c_{11}+a_{11}b_{12}c_{21}+a_{12}b_{22}c_{21} & a_{11}b_{11}c_{12}+a_{12}b_{21}c_{12}+a_{11}b_{12}c_{22}+a_{12}b_{22}c_{22}\\ a_{21}b_{11}c_{11}+a_{22}b_{21}c_{11}+a_{21}b_{12}c_{21}+a_{22}b_{22}c_{21} & a_{21}b_{11}c_{12}+a_{22}b_{21}c_{12}+a_{21}b_{12}c_{22}+a_{22}b_{22}c_{22}\end{bmatrix}$$

$$= \begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}\cdot\begin{bmatrix}b_{11}c_{11}+b_{12}c_{21} & b_{11}c_{12}+b_{12}c_{22}\\ b_{21}c_{11}+b_{22}c_{21} & b_{21}c_{12}+b_{22}c_{22}\end{bmatrix} = \begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}\left(\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix}\cdot\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix}\right)$$

Or: cite from linear algebra: "matrix of a linear map".

Distributive laws: $\left(\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}+\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix}\right)\cdot\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix} = \dots$

$$\dots = \begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}\cdot\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix} + \begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix}\cdot\begin{bmatrix}c_{11}&c_{12}\\c_{21}&c_{22}\end{bmatrix}$$

simply compute!

...and the other way round.

The product is not commutative: $\begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&2\\3&4\end{bmatrix} = \begin{bmatrix}4&6\\3&4\end{bmatrix}$

$$\begin{bmatrix}1&2\\3&4\end{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix} = \begin{bmatrix}1&3\\3&7\end{bmatrix}$$

(c) Already shown: $+$ is well-defined.
$\cdot$ is well-defined: $a' = a + kn$, $b' = b + \ell n \Rightarrow a'b' = ab + akn + b\ell n + k\ell n^2$
$= ab + n(ab + b\ell + k\ell n)$
$\Rightarrow a'b' - ab$ is divisible by n.
Already shown $(\mathbb{Z}_n, +)$ is an abelian group.
$[1]$ is an identity since $[a]\cdot[1] = [a]$ $\forall a$
Associativity is inherited from $\mathbb{Z}$, $\cdot$ is commutative and the distributive law follows from that of $\mathbb{Z}$.

5. (a) $\mathbb{Z}$ is a subring of $\mathbb{Q}$, since sum and product (operation of $\mathbb{Q}$) of two integers and the negative of an integer are integers again.

(b) $\mathbb{Z}$ is no ideal of $\mathbb{Q}$ since for example $2 \cdot \frac{1}{4} = \frac{1}{2} \in \mathbb{Z}$ but $2 \in \mathbb{Z}$.

6. If $I = \{0\}$ then $I = (0)$. Otherwise let m be the smallest positive element of I. (there are positive ones because with x there is $-x$ in I). For any $a \in I$ with

$a = m \cdot q + r$ with $0 \leq r < m$.

$\Rightarrow a - mq = r \in I \Rightarrow r = 0$ by the minimality of m.

7. If $n = a \cdot b$ with $1 < a, b < n$ then $[0] = [n] = [a][b]$ and $\mathbb{Z}/(n)$ has zero-divisors.

8.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

9. $\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i+1)}{1 \cdot 2 \cdot 3 \cdot 4 \cdots i}$ Since $1 \leq i < p$ the numerator is divisible by p but the denominator is not.

10. A reducible polynomial of degree 4 either has a root in $\mathbb{F}_2$ or an irreducible factor of degree 2, which can only be: $x^2 + x + 1$. If both is not the case, it is irreducible. This leaves only $x^4 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x^3 + x^2 + x + 1$, since $(x^2 + x + 1)^2 = x^4 + x^2 + 1$

11. Assume r_1 and r_2 have degree $< \deg f$ and $[r_1] - [r_2] = [0]$. Then $r_1 - r_2$ is divisible by f, but since $\deg(r_1 - r_2) < \deg f$ it follows, that $r_1 = r_2$

12. (a) (i) is a field since $x^3 - x - 1$ is irreducible (ii) not a field since 1 is root of $x^3 - x^2 + x - 1$

(b) Yes, use hom. $\Pi : \mathbb{F}_3[x] \longrightarrow \mathbb{F}_3[x]/(x^3 - x + 1)$ mapping $x \longmapsto (-x)$

Then $\Pi(x^3 - x - 1) = -x^3 + x - 1 + (x^3 - x + 1) = 0 + (x^3 - x + 1) \Rightarrow \ker \Pi = (x^3 - x - 1)$

$\Rightarrow$ By the First Isomorphism Theorem and the surjectivity of $\tilde{\pi}$ we get

$$\mathbb{F}_3[x]/(x^3-x-1) \cong \mathbb{F}_3[x]/(x^3-x+1)$$

since $\ker\tilde{\pi} = (x^3-x-1)$ because x^3-x-1 is irreducible.

(c) The order must be a divisor of $3^3-1 = 26$ since $\left|\mathbb{F}_3[x]/(x^3-x-1)\right| = 27$.
Thus it can only be 1, 2, 13 or 26. It is not 1 or 2.
In $K := \mathbb{F}_3[x]/(x^3-x-1)$ we have for $\Theta := [x] = x + (x^3-x-1)$: $\Theta^3 = \Theta+1$

$\Rightarrow \Theta^9 = (\Theta+1)^3 = \Theta^3+1^3 = \Theta+2$

$\Rightarrow \Theta^{13} = \Theta\cdot(\Theta+1)(\Theta+2) = \Theta^1\cdot\Theta^3\cdot\Theta^9 = \Theta^3 + \underbrace{3\Theta^2}_{=0} + 2\Theta = \Theta+1$ (since $3\Theta+1 = 1$)

Thus the order is 13.

13. (a)

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x	2x+1	2x+2
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x	1	2	0	x+1	x+2	x
2x+2	2x+2	2x	2x+1	2	0	1	x+2	x	x+1

•	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	0	x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	0	x+2	2x+1	2x+2	1	x	x+1	2x+1	2
2x	0	2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	0	2x+1	x+2	x+1	2	2x+1	2x+2	x	1
2x+2	0	2x+2	x+1	2x+1	x	2	x+2	1	2x

this is a field, also: x^2+1 is irreducible

13. (b) x^3+1 has 1 as a root, thus $\mathbb{F}_2[x]/(f)$ is not a field!
Write abc for ax^2+bx+c with $a,b,c \in \{0,1\}$:

+	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

•	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	001	011	101	111
011	000	011	110	101	101	110	011	000
100	000	100	001	101	010	110	011	111
101	000	101	011	110	110	011	101	000
110	000	110	101	011	011	101	110	000
111	000	111	111	000	111	000	000	111

zero-divisors!

note: $x\cdot(1+x+x^2) = x+x^2+x^3 = 1+x+x^2$

$(1+x)^2 = 1+2x+x^2 = 1+x^2$

$(1+x)(1+x^2) = 1+x+x^2+x^3 = x+x^2$

$(1+x)(x+x^2) = x(1+x)^2 = x+x^3 = x+1$

$(1+x)(1+x+x^2) = 1+x+x^2+x+x^2+x^3$
$= 0$

$(1+x^2)^2 = 1+x^4 = 1+x$

$(1+x^2)(x^2+x) = x(1+x^2)(1+x) = 1+x^2$

$(x+x^2)^2 = x^2+x^4 = x^2+x$

14 (a)+(b)
Write $f = (x-a)^k \cdot g$ with $g(a) \neq 0$. If $k=0$ then a is not a root of f.
Assume $k \geq 2$ that is, f has a as a multiple root, then:

$$f' = k(x-a)^{k-1}\cdot g + (x-a)^k \cdot g' \Rightarrow f'(a) = 0 \text{ since } k-1 \geq 1$$
$$= (x-a)^{k-1}\left(k\cdot g + (x-a)\cdot g'\right)$$

Otherwise, if $k=1$ (simple root a), then with the same computation:

$$f'(a) = k\cdot g^{k}(a) \neq 0 \quad \text{since } 1 = (x-a)^{k-1} = (x-a)^0$$