Exercise 10

Discrete Mathematics

December 17, 2020

Exercise 91

Task: Let (e, n) and (d, n) be Bob's public and private RSA key, respectively. Suppose that Bob sends an encrypted message c and Alice wants to find out the original message m. She has the idea to send Bob a message and ask him to sign it. How can she find out m? Hint: Pick a random integer r and consider the message $r^e c \mod n$.

Exercise discussion: Tutor mentions it should probably be "Somebody sends a message with Bob's public key to Bob that you should decrypt.

Solution: The encrypted message was calculated with $c = m^e \mod n$.

Alice sends message $x = r^e c \mod n$ to Bob and asks him to sign it. Bob calculates the signed message $D_B(x) = x^d \mod n$ and sends $D_B(x)$ to Alice.

Usually, Alice would now calculate $E_B(D_B(x)) = x$. We don't do that. Instead, we notice that as $D_B(E_B(r)) = r$ we have

$$D_B(x) = x^d \equiv (r^e c)^d \equiv (r^e)^d c^d \equiv r c^d \mod n$$

So Alice has to calculate

$$D_B(x) r^{-1} \equiv c^d \mod n$$

to get the original message

$$m = D_B(c) = c^d \mod n.$$

Notes:

- Encrypting for Bob is $E_B(x) = x^e \mod n$ and analog for Alice $E_A(x)$
- Bob decrypts doing $D_B(x) = x^d \mod n$ and analog for Alice $D_A(x)$
- It is required that the modular inverse $r^{-1} \in \mathbb{Z}_n$ exists. We know from the lecture that it exists if and only if $\gcd(r, n) = 1$. This means we can just choose r accordingly.

- Bob should encrypt $D_B(x)$, that means calculate $E_A(D_B(x))$, when he sends the message ot Alice. She can then directly decrypt it $D_A(E_A(D_B(x))) = D_B(x)$, so this part is non-essential for us.
- In asymmetric cryptagraphy encryption is done with the recipient key. So Bob probably *received* the message c (instead of sending) because it was calculated with his public key (or he sent it to himself).

Exercise 92

Task: Let G be a finite group and $a \in G$ an element for which $ord_G(a)$ is maximal. Prove that for all $b \in G$, the order $ord_G(b)$ is a divisor of $ord_G(a)$.

Should be a commutative group according to exercise discussion.

Solution: There is no solution. The statement is false.

Consider the dihedral group D_3. It has order 6. It is (the smallest possible) non-abelian group. It has the following multiplication table:

D_3	1	A	B	C	D	E
1	1	A	B	C	D	E
A	A	B	1	D	E	C
B	B	1	A	E	C	D
C	C	E	D	1	B	A
D	D	C	E	A	1	B
E	E	D	C	B	A	1

From that we can read off the order $ord_{D_3}(x) = \min\{k \geq 1 : x^k = 1\}$ of each element:

- $ord_{D_3}(1) = 1$
- $ord_{D_3}(A) = 3$
- $ord_{D_3}(B) = 3$
- $ord_{D_3}(C) = 2$
- $ord_{D_3}(D) = 2$
- $ord_{D_3}(E) = 2$

$ord_{D_3}(A)$ is maximal, but $ord_{D_3}(C) = 2 \nmid 3 = ord_{D_3}(A)$.

Example: The permutation on three objects 123 is an example of D_3. There are 3! permutations/elements:

1. Identity $RGB \to RGB$ has order 1
2. Shifting right $RGB \to BRG \to GBR \to RGB$ has order 3
3. Shifting left $RGB \to GBR \to BRG \to RGB$ has order 3
4. Exchanging first two elements $RGB \to GRB \to RGB$ has order 2

5. Exchanging first and last elements $RGB \to BGR \to RGB$ has order 2
6. Exchanging last two elements $RGB \to RBG \to RGB$ has order 2

The group is not abelian

- Permutations 4. & 6. give $RGB \to GRB \to GBR$
- Permutations 6. & 4. give $RGB \to RBG \to BRG$

See also definition of D_3 on Mathworld and explanation as permutation of three objects on Wikipedia.

Suppose the group is also abelian.
Then the following lemma holds:

Lemma: If the orders $|x|, |y|$ for $x, y \in G$ are coprime then the order of xy is $|x||y|$.
Proof: If $(xy)^m = 1$ then

$$1 = (xy)^m = ((xy)^m)^{|y|} = (xy)^{m|y|} = x^{m|y|} \underbrace{y^{m|y|}}_{1} = x^{m|y|}$$

because $y^{|y|} = 1 \implies y^{m|y|} = 1$. As a consequence $|x|$ divides $m|y|$.

Since $|x|$ and $|y|$ are coprime, this implies $|x|$ divides m. Similarly $|y|$ divides m, so by coprimality their product divides m. This concludes the proof of the lemma.

Example cyclic group $\mathbb{Z}_6 = \{e, x, x^2, x^3, x^4, x^5\}$ using multiplicative notation. Then $|x^2| = 3, |x^3| = 2$ and $m = 1$.

$$e = (x^2 \cdot x^3)^1 = ((x^2 \cdot x^3)^1)^2 = (x^2 \cdot x^3)^{1\cdot 2} = (x^2)^{1\cdot 2} \cdot \underbrace{(x^3)^{1\cdot 2}}_{1} = (x^2)^{1\cdot 2}$$

Wee see that in our previous example D_3 which is not abelian, we have $|A| = 3$ coprime to $|C| = 2$ but $|AC| = |D| = 2 \neq 3 \cdot 2$. For such groups

Now let $a \in G$ be an element of maximal order and $b \in G$ arbitrary. Suppose p is a prime dividing $|b|$ to a higher power than $|a|$. We denote this as $|a| = p^i m$ and $|b| = p^j n$ where $j > i$ and p divides neither m nor n. Then a^{p^i} and b^n have coprime orders, so $a^{p^i} b^n$ has order $p^j m > |a|$. Contradiction.

Example $\mathbb{Z}_6$ with addition: $|1| = 6, |2| = 3, |3| = 2$. We see that taking a to the power of the first factor gives as order the second factor $a = 1, p^i = 2^1, m = 3$, so $|1| = 6 = 2^1 \cdot 3$ and $|1^{2^1}| = |2| = 3 = m$.

Exercise 93

Task: List all irreducible polynomials up to degree 3 in $\mathbb{Z}_3$.

Should be 3 linear, 3 squared and 8 for 3? This is just what I had with always 1 as leading coefficient?

Solution: We defined reducible for polynomials over fields. As 3 is prime, $\mathbb{Z}_3$ is a field. $p(x)$ is irreducible if $p(x) \neq a(x) \cdot b(x)$ with $\deg a(x) < \deg p(x)$ and $\deg b(x) < \deg p(x)$.

A factorization of polynomials of degree 1 would have a factor of degree smaller than 0. Polynomials of degree 0 are just non-zero constants. Hence, polynomials of degree 1 are irreducible.

A polynomial $p = ax^2 + bx + c$ of degree 2 cannot have any factors of degree 2 in its factorization. Hence, there must be a linear factor. That factor shows a root. There is a root if $p(0) \equiv 0 \mod 3 \vee p(1) \equiv 0 \mod 3 \vee p(2) \equiv 0 \mod 3$ because we're in $\mathbb{Z}_3$. If $c = 0$ then 0 is certainly a root and then p is reducible.

A degree 3 polynomial $p = ax^3 + bx^2 + cx + d$ cannot have 2 degree 2 factors in its factorization. Hence, there must a one linear factor. We can then apply the same reasoning as for polynomials of degree 2. For example:

- $p(x) = x^3 + 1 = (x + 1)(x^2 - x + 1)$ has as root $x = -1 \in \mathbb{Z}_3$ because $-1 \equiv 2 \mod 3$. Equivalently, $p(2) \equiv 2^3 + 1 \equiv (-1)^3 + 1 \equiv 0 \mod 3$. Hence, it is reducible.
- $p(x) = x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$ has as root $x = -1 \in \mathbb{Z}_3$. Hence, it is reducible.
- $p(x) = x^3 + 2x^2 + 1 = (x + 2)x^2 + 1$ has as root $x \approx -2.2056 \notin \mathbb{Z}_3$. Equivalently, $p(1) \equiv 1 \mod 3, p(2) \equiv 2 \mod 3$. Hence, it is irreducible.
- $p(x) = x^3 + 2x^2 + x + 1 = x(x + 1)^2 + 1$ has as root $x \approx -1.7549 \notin \mathbb{Z}_3$. Hence, it is irreducible.

In the lecture we had something similar: $x^2 + 1 = (x + 1)(x + 1)$ over $\mathbb{Z}_2$. We see -1 is a root and $(-1)^2 + 1 \equiv 0 \mod 2$.

				0	1	2		
a	b	c	d	f(0)	f(1)	f(2)		
0	0	0	0					constant
0	0	0	1					constant
0	0	0	2					constant
0	0	1	0				TRUE	Degree 1 => Irreducible
0	0	1	1				TRUE	Degree 1 => Irreducible
0	0	1	2				TRUE	Degree 1 => Irreducible
0	0	2	0				TRUE	Degree 1 => Irreducible
0	0	2	1				TRUE	Degree 1 => Irreducible
0	0	2	2				TRUE	Degree 1 => Irreducible
0	1	0	0	0	1	1	FALSE	If the constant of the polynomi
0	1	0	1	1	2	2	TRUE	true means irreducible
0	1	0	2	2	0	0	FALSE	
0	1	1	0	0	2	0	FALSE	
0	1	1	1	1	0	1	FALSE	
0	1	1	2	2	1	2	TRUE	x^2+x+2 has no roots
0	1	2	0	0	0	2	FALSE	
0	1	2	1	1	1	0	FALSE	x^2+2x+1 has as root 2
0	1	2	2	2	2	1	TRUE	
0	2	0	0	0	2	2	FALSE	
0	2	0	1	1	0	0	FALSE	
0	2	0	2	2	1	1	TRUE	
0	2	1	0	0	0	1	FALSE	
0	2	1	1	1	1	2	TRUE	
0	2	1	2	2	2	0	FALSE	
0	2	2	0	0	1	0	FALSE	
0	2	2	1	1	2	1	TRUE	
0	2	2	2	2	0	2	FALSE	
1	0	0	0	0	1	2	FALSE	Start polynomials of degree 3
1	0	0	1	1	2	0	FALSE	Example from sheet
1	0	0	2	2	0	1	FALSE	
1	0	1	0	0	2	1	FALSE	
1	0	1	1	1	0	2	FALSE	
1	0	1	2	2	1	0	FALSE	
1	0	2	0	0	0	0	FALSE	
1	0	2	1	1	1	1	TRUE	
1	0	2	2	2	2	2	TRUE	
1	1	0	0	0	2	0	FALSE	
1	1	0	1	1	0	1	FALSE	Example from sheet
1	1	0	2	2	1	2	TRUE	
1	1	1	0	0	0	2	FALSE	
1	1	1	1	1	1	0	FALSE	
1	1	1	2	2	2	1	TRUE	
1	1	2	0	0	1	1	FALSE	
1	1	2	1	1	2	2	TRUE	
1	1	2	2	2	0	0	FALSE	
1	2	0	0	0	0	1	FALSE	
1	2	0	1	1	1	2	TRUE	Example from sheet
1	2	0	2	2	2	0	FALSE	
1	2	1	0	0	1	0	FALSE	
1	2	1	1	1	2	1	TRUE	Example from sheet
1	2	1	2	2	0	2	FALSE	
1	2	2	0	0	2	2	FALSE	
1	2	2	1	1	0	0	FALSE	
1	2	2	2	2	1	1	TRUE	
2	0	0	0	0	2	1	FALSE	
2	0	0	1	1	0	2	FALSE	
2	0	0	2	2	1	0	FALSE	
2	0	1	0	0	0	0	FALSE	
2	0	1	1	1	1	1	TRUE	
2	0	1	2	2	2	2	TRUE	
2	0	2	0	0	1	2	FALSE	
2	0	2	1	1	2	0	FALSE	
2	0	2	2	2	0	1	FALSE	
2	1	0	0	0	0	2	FALSE	
2	1	0	1	1	1	0	FALSE	
2	1	0	2	2	2	1	TRUE	
2	1	1	0	0	1	1	FALSE	
2	1	1	1	1	2	2	TRUE	
2	1	1	2	2	0	0	FALSE	
2	1	2	0	0	2	0	FALSE	
2	1	2	1	1	0	1	FALSE	
2	1	2	2	2	1	2	TRUE	
2	2	0	0	0	1	0	FALSE	
2	2	0	1	1	2	1	TRUE	
2	2	0	2	2	0	2	FALSE	
2	2	1	0	0	2	2	FALSE	
2	2	1	1	1	0	0	FALSE	
2	2	1	2	2	1	1	TRUE	
2	2	2	0	0	0	1	FALSE	
2	2	2	1	1	1	2	TRUE	
2	2	2	2	2	2	0	FALSE	

Exercise 94

Task: Decompose $x^4 + x^3 + 1$ into irreducible factors over $\mathbb{Z}_2$.

Seems to be really irreducible already

Solution: Say $p(x) = x^4 + x^3 + 1$. We see that p doesn't have a linear factor by calculating $p(0) \equiv p(1) \equiv 1 \mod 2$ (no root). It could still have quadratic factors. The only quadratic irreducible polynomial over $\mathbb{Z}_2$ is $x^2 + x + 1$.

a	b	c	f(0)	f(1)	
1	0	0	0	1	FALSE
1	0	1	1	0	FALSE
1	1	0	0	0	FALSE
1	1	1	1	1	TRUE

But $\frac{p(x)}{x^2+x+1} = (x^2 - 1) + x + 2$, that means $p(x)$ is not divisible by $x^2 + x + 1$.

So there is nothing to decompose for $x^4 + x^3 + 1$ is already irreducible.

Exercise 95

An integral domain R is a factorial ring if $\forall a \in R \setminus (\{0\} \cup R^*)$ it holds there is a unit $\exists \epsilon \in R^*$ and irreducible elements $\exists q_1, \ldots, q_l$ such that $a = \epsilon q_1 q_2 \ldots q_l$ and this is unique in the following sense: If $a = \epsilon_1 q_1 q_2 \ldots q_l = \epsilon_2 q_1 q_2 \ldots q_k$ then $k = l$ and there is a permutation $\exists \pi \in S_l : q_j \sim p_{\pi(j)}$ with $j = 1, \ldots, l$ (unique up to order and units).

$p(x)$ is irreducible if $p(x) \neq a(x) \cdot b(x)$ with $\deg a(x) < \deg p(x)$ and $\deg b(x) < \deg p(x)$.

As $(\mathbb{K}[x], +, \cdot)$ is an Euclidean ring, it is an integral domain and there is division with remainder. As $(\mathbb{K}[x], +, \cdot)$ is an integral domain, it is a ring and it holds that there are no zero divisors $a \neq 0, b \neq 0 \implies ab \neq 0$. As $(\mathbb{K}[x], +, \cdot)$ is Euclidean, it is also factorial.

As $2 \cdot 4 = 0$ in $\mathbb{Z}_8$, $\mathbb{Z}_8$ is not an integral domain. $x^2 - 1$ has degree 2 and 4 roots $\{1, 3, 5, 7\}$ in $\mathbb{Z}_8$. The "no zero divisors" property does not hold for $\mathbb{Z}_8$.

Task: Let $\mathbb{K}$ be a field and $p(x) \in \mathbb{K}[x]$ a polynomial of degree m. Prove that $p(x)$ cannot have more than m zeros (counted with multiplicities). Hint: Use the fact that $\mathbb{K}[x]$ is a factorial ring.

Explanation of exercise presentations something like: With the factorial ring property, we get that all constant polynomials of a field are units. If you have an element of a factorial field then there is the unique prime decomposition. Since all elements of the field are units, all other factors have to be polynomials of degree at least one. So the prime decomposition has irreducible polynomials, so a can be at most linear. So you would have at most m of the factors so at most m zeros.

Solution:

- Stackexchange
- The Gallian book Contemporary Abstract Algebra can be found online
- Stackexchange about $\deg(fg)$

Proof by induction on n. A polynomial of degree 0 over the field $\mathbb{K}$ has no zeros. Suppose that $p(x)$ is a polynomial of degree m over $\mathbb{K}$ and a is a zero of $p(x)$ of multiplicity k. Note that $(x - a)$ is irreducible and by the factorial ring property there is a unique factorization with irreducible factors. Then $p(x) = (x - a)^k q(x)$ and $q(a) \neq 0$. It holds $\deg(f(x)g(x)) = \deg f(x) \cdot \deg f(x)$ because of the factorial ring property and no zero divisors and

$$\begin{aligned}
&\deg\left(\left(c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0\right)\left(d_m x^m + d_{m-1} x^{m-1} + \cdots + d_1 x + c_0\right)\right) \\
=&\deg\left(c_n d_m x^{n+m} + \ldots\right) \\
=&n + m
\end{aligned}$$

Since

$$m = \deg p(x) = \deg(x - a)^k q(x) = k + \deg q(x)$$

we have $k \leq m$. If $p(x)$ has a as only zero then we are done. If on the other hand b is also a zero of $p(x)$ and $b \neq a$ then $0 = p(b) = (b-a)^k q(b)$. Then $(b-a)^k$ is not 0. Then b is a zero of $q(x)$ with the same multiplicity as it has for $p(x)$.

Note that as $(\mathbb{K}[x], +, \cdot)$ is an Euclidan ring the no zero divisors property does hold. This means we can do cancellation, so for a root a we get $p(x) = (x-a)q(x)$ and we can cancel off $(x-a)$ on both sides and are left with $q(x)$ which is of lower degree.

By strong induction [1], we know that $q(x)$ has at most $\deg q(x) = m-k$ zeros, counting multiplicity. Thus, $p(x)$ has at most $k + m - k = m$ zeros, counting multiplicity.

Example with $m = 3, k = 1, a = 1$:

$$\underbrace{(x-1)^3(x-2)^4(x-3)^5}_{p(x)} = (x-1)^3 \underbrace{(x-2)^4(x-3)^5}_{q(x)}$$

See also

- link
- Stackexchange

[1] If 1. $P(1)$ and 2. $\forall 1 \leq i \leq k : P(i) \implies P(k+1)$ then $\forall n \in \mathbb{N} : P(n)$

Exercise 96

- link
- link

Task: Prove that if G is a finite group and $a \in G$ is an element with $ord_G(a) = r$, then for every $k \in \mathbb{N}$, $ord_G\left(a^k\right) = r/\gcd(r,k)$

Solution: The order of a is the smallest $r > 0$ such that $a^r = 1$. The order of a^k is the smallest $x > 0$ such that $a^{kx} = 1$. Then kx is a multiple of the order r of a. This means kx is the least common multiple of k and r. By definition $lcm(k,r) = \frac{kr}{\gcd(k,r)}$. It follows

$$lcm(k,r) = kx = \frac{kr}{\gcd(k,r)} \implies x = ord_G\left(a^k\right) = \frac{r}{\gcd(k,r)}$$

More detailed approach: By definition $a^r = 1$ (where 1 denotes the identity), it follows that any power of a^r is also the identity. That includes the power $\frac{k}{\gcd(r,k)}$. It follows

$$1 = (a^r)^{\frac{k}{\gcd(r,k)}} = a^{r \cdot \frac{k}{\gcd(r,k)}} = a^{k \cdot \frac{r}{\gcd(r,k)}} = (a^k)^{\frac{r}{\gcd(r,k)}}$$

We now show that $\frac{r}{\gcd(r,k)}$ is the smallest positive power x of a^k such that $\left(a^k\right)^x = 1$. This means

$$\forall m > 0 : (\left(a^k\right)^m = 1 \implies \frac{r}{\gcd(r,k)} \leq m$$

Let $m \in \mathbb{N}$ be such that $\left(a^k\right)^m = a^{km} = 1$. Since the order of a is r, it follows that $r \mid km$. Therefore we have

$$\frac{r}{\gcd(r,k)} \mid \frac{k}{\gcd(r,k)} m$$

It is known that

$$\gcd\left(\frac{r}{\gcd(r,k)}, \frac{k}{\gcd(r,k)}\right) = 1$$

and from this it follows from Euclid's lemma

> If $n \mid ab$ and n is relatively prime to a, then $n \mid b$.

that

$$\frac{r}{\gcd(r,k)} \mid m$$

In particular holds

$$\frac{r}{\gcd(r,k)} \leq m$$

Example: As example, consider the dihedral group D_3. It has the following multiplication table:

D_3	1	A	B	C	D	E
1	1	A	B	C	D	E
A	A	B	1	D	E	C
B	B	1	A	E	C	D
C	C	E	D	1	B	A
D	D	C	E	A	1	B
E	E	D	C	B	A	1

From that we can read off the order $ord_{D_3}(x) = \min\{k \geq 1 : x^k = 1\}$ of some elements:

- $ord_{D_3}(1) = 1$
- $ord_{D_3}(A) = 3$
- $ord_{D_3}(B) = 3$
- $ord_{D_3}(C) = 2$

For C with $r = 2$ we choose $k = 3$ and get

$$ord_{D_3}(C^3) = ord_{D_3}(C) = 2 = \frac{2}{1} = \frac{2}{\gcd(2,3)}$$

For A with $r = 3$ we choose $k = 6$ and get

$$ord_{D_3}(A^6) = ord_{D_3}(1) = 1 = \frac{3}{3} = \frac{3}{\gcd(3,6)}$$

So about the first solution, we see that $A^3 = 1$ and $r = 3$ and that for $k = 2$ and $x = 3$ we get $A^2 = B$ and $(A^2)^3 = B^3 = 1$ where 6 is the lcm of 2 and 3.

Exercise 97

Task: Let R be a ring and $(I_j)_{j\in J}$ be a family of ideals of R. Prove that $\bigcap_{j\in J} I_j$ is also an ideal of R.

Solution: Let $S = \bigcap_{j\in J} I_j$. We have to show:

1. Subgroup $(S, +) \leq (R, +)$. We know

$$\forall j \in J : (I_j, +) \leq (R, +) \tag{1}$$

   It is widely known that the intersection of two subgroups of a group is itself a subgroup of that group:

$$\forall H_1, H_2 \leq (G, \circ) : H_1 \cap H_2 \leq G$$

2. Stackexchange Stackexchange Show $a \in R \implies a \cdot S \subseteq S$. This is equivalent to $\forall s \in S : a \in R \implies as \in S$ Suppose $s \in S$ and $a \in R$. By definition of S holds $\forall j \in J : s \in I_j$. Then as all I_j are ideals of R holds $\forall j \in J : as \in I_j$. Therefore $as \in \bigcap_{j\in J} I_j = S$.

Exercise 98

Task: Let R be a ring and I an ideal of R. Then $(R/I, +)$ is the factor group of $(R, +)$ over $(I, +)$. Define a multiplication on R/I by

$$(a + I) \cdot (b + I) := (ab) + I.$$

Prove that this operation is well defined, i.e. that

$$a + I = c + I \textbf{ and } b + I = d + I \implies (ab) + I = (cd) + I.$$

Furthermore, show that $(R/I, +, \cdot)$ is a ring

Ring

Exercise presentations: Proving in such a way is OK. You may asssume that addition is well-defined and multiplication as well.

$(R/I, +, \cdot)$ is a ring if and only if

1. $(R/I, +)$ is a commutative group.
2. $(R/I, \cdot)$ is a semi-group (associative law holds).
3. Multiplication is distributive wrt addition: $(a+b)\cdot c = a\cdot c+b\cdot c, c\cdot(a+b) = c\cdot a+c\cdot b$

We define the addition to be

$$(a + I) + (b + I) := (a + b) + I$$

Proof:

Exercise presentations: I seem to have forgotten additive closure

1. - As $a, b, c \in R$ and $(R, +)$ is associative

$$\begin{aligned}&((a + I) + (b + I)) + (c + I)\\ =&((a + b) + I) + (c + I)\\ =&((a + b) + c) + I\\ =&(a + (b + c)) + I\\ =&(a + I) + ((b + c) + I)\\ =&(a + I) + ((b + I) + (c + I))\end{aligned}$$

   $(R/I, +)$ is associative.

   - $a \in R$ and 0 is the neutral element of $(R, +)$

$$(0 + I) + (a + I) = (0 + a) + I = a + I = (a + 0) + I = (a + I) + (0 + I)$$

   so $(0 + I)$ is the zero-element of $(R/I, +)$.

- As $a \in R$ and $-a \in R$ is the inverse element of $(R, +)$

$$(a + I) + (-(a + I)) = (a + I) + ((-a) + I) = (a + (-a)) + I = (0 + I)$$
$$(-(a + I)) + (a + I) = ((-a) + I) + (a + I) = ((-a) + a) + I = (0 + I)$$

  so $-(a + I)$ is the inverse element of $(R/I, +)$. Hence, $(R, +)$ is a group.

- R/I is commutative because addition in R is commutative and

$$(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I)$$

  with $a, b \in R$.

Alternative for the group part: $(R, +)$ is an abelian group because R is a ring. As I is an ideal of R it holds $I \leq R$ by definition from the lecture. Then I inherits the property of being abelian. This means I is a *normal* subgroup of R. R/I is the factor group of R by I. It is known that the factor group of a group by a normal subgroup forms a group itself. Then the factor group R/I is a group under addition.

2. Considering that $(R, \cdot)$ is associative because R is a ring, we get

$$\begin{aligned}((a + I) \cdot (b + I)) \cdot (c + I) &= \\ ((a \cdot b) + I) \cdot (c + I) &= \\ ((a \cdot b) \cdot c) + I &= \\ (a \cdot (b \cdot c)) + I &= \\ (a + I) \cdot ((b \cdot c) + I) &= \\ (a + I) \cdot ((b + I) \cdot (c + I))\end{aligned}$$

   that $(R/I, \cdot)$ is a semi-group.

3. Considering that multipication in R is distributive wrt addition because R is a ring, we get

$$\begin{aligned}((a + I) + (b + I)) \cdot (c + I) &= \\ ((a + b) + I) \cdot (c + I) &= \\ ((a + b) \cdot c) + I &= \\ (ac + bc) + I &= \\ ((ac) + I) + ((bc) + I) &= \\ (a + I) \cdot (c + I) + (b + I) \cdot (c + I)\end{aligned}$$

and

$$\begin{aligned}(c+I)\cdot((a+I)+(b+I)) &= \\ (c+I)\cdot((a+b)+I) &= \\ (c\cdot(a+b))+I &= \\ (ca+cb)+I &= \\ ((ca)+I)+((cb)+I) &= \\ (c+I)\cdot(a+I)+(c+I)\cdot(b+I)\end{aligned}$$

that $(R/I,\cdot)$ is distributive over $(R/I,+)$

Well-defined

There was a 3 line proof in the presentation and it was too short. It had the multiplication (a+I)(b+I) which is not defined. Tutor mentioned something like: a+I=b+I if and only if a-b in I, so the definition of equivalence classes. Then you show ac-bd is in I. This is sort of clear because you insert terms that are 0 so ac+ad-ad-bd and then you factor out. Tutor said really much about equivalence classes. You have to be really exact and careful here to only do defined things.*

Suppose $a+I=c+I$ and $b+I=d+I$.

Recall again the definition $(R/I,+)=\{a+I \mid a\in R\}$. As I is an ideal of R it holds $I\leq R$. If $I\leq R$ then $a+I$ means $\{a+i \mid i\in I\}$ and is called left coset of I in R. This means $(R/I,+)$ is a set of cosets. Example: We know from the lecture that

$$\begin{aligned}\mathbb{Z}/4\mathbb{Z} &= \{a+4\mathbb{Z} \mid a\in\mathbb{Z}\} = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\} \\ &= \{\{0+i \mid i\in 4\mathbb{Z}\}, \{1+i \mid i\in 4\mathbb{Z}\}, \{2+i \mid i\in 4\mathbb{Z}\}, \{3+i \mid i\in 4\mathbb{Z}\}\}\end{aligned}$$

is a factor ring. Note that a can be in the full range of $\mathbb{Z}$, but for example

$$\begin{aligned}\{0+4\mathbb{Z}\} &= \{-8,-4,0,4,8,12,16,\dots\} \quad \{1+4\mathbb{Z}\} = \{-7,-3,1,5,9,13,17\dots\} \\ \{4+4\mathbb{Z}\} &= \{-8,-4,0,4,8,12,16,\dots\} \quad \{5+4\mathbb{Z}\} = \{-7,-3,1,5,9,13,17\dots\}\end{aligned}$$

see comment With this knowledge, it follows from $a+I=c+I$ that $a=c+x$ and from $b+I=d+I$ $b=d+y$ with $x,y\in I$. For example with $10,2\in\mathbb{Z}$ it follows from $10+4\mathbb{Z}=2+4\mathbb{Z}$ that $10=2+x$ with $x=8\in 4\mathbb{Z}$.

We use the normal subgroup property

Using this and $c,x,d,y\in\mathbb{Z}$ and multiplication in $\mathbb{Z}$ we get

$$ab=(c+x)(d+y)=cd+xd+cy+xy$$

and so

$$ab+I=cd+xd+cy+xy+I=cd+I$$

because I absorbs $xd + cy + xy$ because $x, y \in I$. Using again our example: $x, y \in 4\mathbb{Z} \implies xd, cy, xy \in 4\mathbb{Z}$, and also $6 + 4\mathbb{Z} = 2 + 4 + 4\mathbb{Z} = 2 + 4\mathbb{Z}$. Consequently, multiplication is well-defined.

Exercise 99

For $m \in R$ is $(m) := mR = \{ma \mid a \in R\}$ the multiples of m a principal ideal. (m) is an ideal.

Task: Let $U = \{\bar{0}, \bar{2}, \bar{4}\} \subseteq Z_6$. Show that U is an ideal of $(\mathbb{Z}_6, +, \cdot)$. Is it a subring as well? Does it have a 1-element?

Solution: Let $m = 4$.

$a \in R$	0	1	2	3	4	5
ma	0	4	8	12	16	20
$ma \mod 6$	0	4	2	0	4	2

So $(m) = U$ is an ideal of $\mathbb{Z}_6$.

$(U, +, \cdot)$ is a subring of $(\mathbb{Z}_6, +, \cdot)$ if it is non-empty and closed under substraction (or alternatively addition and additive inverse) and multiplication.

Consider that $\bar{a} - \bar{b} = \overline{(a - b)}$. Example: $\bar{2} - \bar{4} = \overline{2 - 4} = \overline{-2} = \bar{4}$.

$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6

+	0	2	4
0	0	2	4
2	4	4	0
4	2	0	2

inv	0	2	4
0	0	4	2

-	0	2	4
0	0	2	4
2	4	0	2
4	2	4	0

*	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

We see in the the tables that $(U, +, \cdot)$ is non-empty, closed under substraction & closed under multiplication and therefore a subring of $(\mathbb{Z}_6, +, \cdot)$

4 is the 1-element.

Exercise 100

We know

1. For $m \in R$ is $(m) := mR = \{ma \mid a \in R\}$ the multiples of m. Then (m) is principal ideal. (m) is also an ideal.
2. For $M \subseteq R$ we define the ideal that is generated by M to be $(M) := \bigcap (\text{ideals of } R \text{ that contain } M)$.
3. If R is an Euclidean ring then all ideals are principle.
4. If R is an Euclidean ring and $M = \{m_1, m_2, \ldots, m_n\}$ consists of a finite number of elements, then the ideal that is generated by M is the principal ideal $(M) = (\gcd(m_1, m_2, \ldots, m_n)) = \gcd(m_1, m_2, \ldots, m_n) \cdot R$.

Task: Show that $(\mathbb{Z}[x], +, \cdot)$ is a ring and that $1 \notin (\{x, x+2\})$.
Remark: It can be shown that a principal ideal which is generated by $a_1, a_2, \ldots, a_k$ can be alternatively generated by $\gcd(a_1, a_2, \ldots, a_k)$. Therefore this example shows that $\mathbb{Z}[x]$ is a ring where not every ideal is a principal ideal. As a consequence, $\mathbb{Z}[x]$ cannot be a Euclidean ring.

Solution: From Joseph A. Gallian's Contemporary Abstract Algebra: Let R be a commutative ring. The set of formal symbols

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R, n \text{ is a nonnegative integer}\} \quad (2)$$

is called the ring of polynomials over R in the indeterminate x.

Let R be a commutative ring and let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

belong to $R[x]$. Then

$$f(x) + g(x) = (a_s + b_s) x^s + (a_{s-1} + b_{s-1}) x^{s-1} + \cdots + (a_1 + b_1) x + a_0 + b_0,$$

where s is the maximum of m and n, $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$. Also,

$$f(x)g(x) = c_{m+n} x^{m+n} + c_{m+n-1} x^{m+n-1} + \cdots + c_1 x + c_0$$

where

$$c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$$

for $k = 0, \ldots, m+n$.

Note that this is just the usual multiplication. For example:

$$\begin{aligned}(a_1x + a_0)(b_1x + b_0) &= a_1b_1x^2 + a_1b_0x + a_0b_1x + a_0b_0 \\ &= \underbrace{a_1b_1}_{c_2}x^2 + \underbrace{(a_0b_1 + a_0b_1)}_{c_1}x + a_0b_0\end{aligned}$$

with $k = 0, \ldots, 2$

$$\begin{aligned}c_0 &= a_0b_0 \\ c_1 &= a_1b_0 + a_0b_1 \\ c_2 &= \underbrace{a_2}_{=0}b_0 + a_1b_1 + a_0\underbrace{b_2}_{=0}\end{aligned}$$

Addition and multiplication are formulated so that they are commutative and associative. Furthermore, multiplication is distributive over addition. $(R[x], +)$ has 0 as identity element and as $a_i \in \mathbb{Z}$ we can always find the inverse $-a_i$ such that $a_ix^n + (-a_ix^n) = 0$. This makes $R[x]$ a ring.

As the multiplication of integers is a commutative operation, $\mathbb{Z}$ is a commutative ring. Then by our previous definition $\mathbb{Z}[x]$ is a ring.

Let for brevity $P(i)$ be the property that $a_i \in \mathbb{Z}, n$ is a nonnegative integer.

- $1 \in \mathbb{Z}$. Therefore by equation 2 holds $1x = x \in \mathbb{Z}[x]$. Therefore

  $$\begin{aligned}(x) = x\mathbb{Z}[x] &= \{xa \mid a \in \mathbb{Z}[x]\} \\ &= \{a_nx^{n+1} + a_{n-1}x^n + \cdots + a_1x^2 + a_0x \mid P(i)\}\end{aligned}$$

  is a (principal) ideal of $\mathbb{Z}[x]$.

- $1 \in \mathbb{Z}$ and $2 \in \mathbb{Z}$. Therefore by equation 2 holds $x + 2 \in \mathbb{Z}[x]$. Therefore

  $$\begin{aligned}(x+2) = (x+2)\mathbb{Z}[x] &= \{(x+2)a \mid a \in \mathbb{Z}[x]\} \\ &= \{a_nx^n(x+2) + a_{n-1}x^{n-1}(x+2) + \cdots + a_1x(x+2) + a_0(x+2) \mid P(i)\} \\ &= \{a_nx^{n+1} + 2a_nx^n + a_{n-1}x^n + 2a_{n-1}x^{n-1} + \cdots + a_1x^2 + 2a_1x + a_0x + 2a_0 \mid P(i)\}\end{aligned}$$

  is a (principal) ideal of $\mathbb{Z}[x]$.

An alternative definition for the ideal generated by a set is: If R is a commutative ring with unity and $a_1, a_2, \ldots, a_n$ belong to R then $I = \langle a_1, a_2, \ldots, a_n\rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R\}$ is an ideal of R called the ideal generated by $a_1, a_2, \ldots, a_n$

x and $x + 2$ belong to $\mathbb{Z}[x]$. We get $\langle x, x, +2\rangle = (\{x, x + 2\}) = \{r_1x + r_2(x + 2) \mid r_1, r_2 \in \mathbb{Z}[x]\}$.

Note that there is a mistake here. r_1 and r_2 are not necessarily equal, so all the variable names should be different.

We already calculated the single summands before, so now we have to add them:

$$\begin{aligned}\cdots &= \{2a_n x^{n+1} + 2a_n x^n + 2a_{n-1}x^n + 2a_{n-1}x^{n-1} + \cdots + 2a_1 x^2 + 2a_1 x + 2a_0 x + 2a_0 \mid P(i)\} \\ &= \{x\left(2a_n x^n + 2a_n x^{n-1} + 2a_{n-1}x^{n-1} + 2a_{n-1}x^{n-2} + \cdots + 2a_1 x + 2a_1 + 2a_0\right) + 2a_0 \mid P(i)\} \\ &= \{2x\left(a_n x^n + a_n x^{n-1} + a_{n-1}x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1 x + a_1 + a_0\right) + 2a_0 \mid P(i)\}\end{aligned}$$

There is no way to set the a_i such that this polynomial equals 1. Hence $1 \notin (\{x, x+2\})$

About the remark: From 4. and by the definition of an implication it holds $\mathbb{Z}[x]$ is not Euclidean or the ideal that is generated by $\{x, x+2\}$ is not the principal ideal $(M) = \gcd(x, x+2) \cdot \mathbb{Z}[x]$.

$gcd(x, x+2)$ is 1 if x is odd and 2 otherwise . $1 \cdot \mathbb{Z}[x] = \mathbb{Z}[x]$ and $2 \cdot \mathbb{Z}[x]$ is $\mathbb{Z}[x]$ with all coefficients even.

$1 \in \mathbb{Z}[x]$ but $1 \notin (\{x, x+2\})$. So those sets are not equal. $2 \in 2\mathbb{Z}[x]$ but $2 \notin (\{x, x+2\})$. So those sets are not equal either. It follows that $\mathbb{Z}[x]$ is not Euclidean.