Algebra
Prof. Anna Lachowska — EPFL

Notes by Joachim Favre

Computer science bachelor — Semester 5
Autumn 2023

I made this document for my own use, but I thought that typed notes might be of interest to others. There are mistakes, it is impossible not to make any. If you find some, please feel free to share them with me (grammatical and vocabulary errors are of course also welcome). You can contact me at the following e-mail address:

joachim.favre@epfl.ch

If you did not get this document through my GitHub repository, then you may be interested by the fact that I have one on which I put those typed notes and their LaTeX code. Here is the link (make sure to read the README to understand how to download the files you're interested in):

https://github.com/JoachimFavre/EPFLNotesIN

Please note that the content does not belong to me. I have made some structural changes, reworded some parts, and added some personal notes; but the wording and explanations come mainly from the Professor, and from the book on which they based their course.

I think it is worth mentioning that in order to get these notes typed up, I took my notes in LaTeX during the course, and then made some corrections. I do not think typing handwritten notes is doable in terms of the amount of work. To take notes in LaTeX, I took my inspiration from the following link, written by Gilles Castel. If you want more details, feel free to contact me at my e-mail address, mentioned hereinabove.

https://castel.dev/post/lecture-notes-1/

I would also like to specify that the words "trivial" and "simple" do not have, in this course, the definition you find in a dictionary. We are at EPFL, nothing we do is trivial. Something trivial is something that a random person in the street would be able to do. In our context, understand these words more as "simpler than the rest". Also, it is okay if you take a while to understand something that is said to be trivial (especially as I love using this word everywhere hihi).

Since you are reading this, I will give you a little advice. Sleep is a much more powerful tool than you may imagine, so do not neglect a good night of sleep in favour of studying (especially the night before an exam). I wish you to have fun during your exams.

Version 2024–07–31–Official

To Gilles Castel, whose work has
inspired me this note taking method.

Rest in peace, nobody
deserves to go so young.

Contents

List of lectures

Chapter 1

Summary by lecture

Lecture 1 : Pretty colours — Monday 25th September 2023 *p. 15*

- Explanation of the simple induction principle, the well ordering principle and the strong induction principle; and proof that they are equivalent.
- Definition of divisibility, prime and composite numbers.
- Proof of the Euclidean division theorem.
- Definition of greatest common divisor.
- Proof of the Euclidean algorithm, and of Bézout's construction.
- Definition of Euler's totient function.

Lecture 2 : AICC 2 — Monday 2nd October 2023 *p. 21*

- Explanation of the RSA cryptosystem.
- Definition of groups and order.
- Definition of subgroups.
- Definition of left cosets, and of index.
- Proof of Lagrange's theorem, and some corollaries.

Lecture 3 : Homeomorphisms are better though — Monday 9th October 2023 *p. 26*

- Definition of homomorphisms, and proof of some of their properties.
- Definition of automorphism.
- Definition of generators and cyclic groups.
- Definition of relation.
- Definition of the presentation in generators and relations of a group.
- Proof of the characterisation of a homomorphism by the presentation in generators and relations of a group.

Lecture 4 : Defining normality mathematically — Monday 16th October 2023 *p. 30*

- Definition of normal subgroup.
- Definition of the kernel of a homomorphism, and proof that it is a normal subgroup.
- Definition of image of a homomorphism, and proof that it is a subgroup.
- (Very) quick introduction to elliptic curves.
- Definition of the group of rigid symmetries of a flat regular n-gon, and proof of its representation in generators and relations.
- Definition of quotient groups, and proof that they make sense for normal subgroups.

Lecture 5 : Proof by staring — Monday 23rd October 2023 *p. 35*

- Definition of the symmetric group.
- Definition of orbits, and proof that they are either disjoint or equal.
- Explanation that the cycle decomposition of a permutation is unique, except for the order of factors.
- Explanation of how to compute the product of two permutations, and proof of a quick method to compute the special case of a conjugation.
- Proof that the symmetric group is generated by the transpositions.

Lecture 6 : Enlarge your orbit — Monday 30th October 2023 *p. 40*

- Proof of the sign invariance of a permutation.
- Definition of the alternating group.
- Definition of a group acting on itself by permutation.
- Definition of the orbit and the conjugacy class.
- Definition of the stabiliser and the centraliser.
- Proof of the orbit-stabiliser theorem.
- Definition of the center of a group.
- Proof of the class equation of a group.

Lecture 7 : A complete description of abelian group (☺) — Monday 6th November 2023 *p. 46*

- Definition of direct products.
- Proof of the elementary divisors characterisation of abelian groups.
- Explanation of the invariant factors characterisation of abelian groups.
- Explanation of algorithms to find the elementary divisors and invariant factors characterisation of abelian groups.

Lecture 8 : Gollum's favourite subject — Monday 13th November 2023 *p. 53*

- Definition of commutative ring.
- Definition of zero divisor, and proof that multiplicative inverses are not divisors.
- Definition of fields and integral domains, and proof that the first one implies the second one.
- Definition of ideal.
- Proof of a proposition allowing to generate more ideals from known ideals.

Lecture 9 : ✨ Prof. de Lataillade ✨ — Monday 20th November 2023 *p. 59*

- Definition of principal ideal.
- Definition of congruence relation.
- Proof that ideals generate congruence relations and inversely.
- Definition of principal ideal domains.
- Definition of ring homomorphism.
- Definition of the characteristic of a ring.

Lecture 10 : Generalising Euclidean division — Monday 27th November 2023 *p. 66*

- Proof of the Chinese remainder theorem.
- Proof of the CRT for integers, and examples on how to use it.

- Definition of polynomial rings, and proof of some properties.
- Definition of Euclidean domain, and proof of some properties.

- Definition of lcm and gcd.
- Proof of the CRT for an arbitrary number of factors.
- Explanation on how to use the CRT to solve a system of congruences of polynomials.
- Definition of irreducible elements and maximal ideals.

- Proof that an ideal is maximal if and only if its quotient ring is a field.
- Proof of theorems allowing to know when a polynomial is irreducible.
- Proof of theorems doing a classification of the finite fields.

Chapter 2

Integers

2.1 Axioms of natural numbers

Definition: Natural numbers The set of **natural numbers** is the set of non-negative numbers:

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

Remark When we want to exclude the zero, we can write:

$$\mathbb{Z}_+ = \{1, 2, \ldots\}$$

Axiom: Induction principle Let $S \subset \mathbb{N}$ be a set such that $0 \in S$ and $n \in S \implies n+1 \in S$.
Then, $S = \mathbb{N}$.

Axiom: Well ordering principle Let $S \subset \mathbb{N}$ be non-empty.
Then, S has a least element.

Axiom: Strong induction principle Let $S \subset \mathbb{N}$ be a set such that $0 \in S$ and $\{0, \ldots, n\} \subset S \implies n+1 \in S$.
Then, $S = \mathbb{N}$.

Theorem: Equivalence We have the following implications:

$$\text{induction} \implies \text{strong induction} \implies \text{well ordering} \implies \text{induction}$$

In other words, all three axioms are equivalent. We can take any of the propositions as an axiom, and the other two will come from that.

Proof 1 We want to show that the induction principle implies the strong induction principle. In other words, we suppose the induction principle holds and we want to prove the strong induction principle.
Let $S \subset \mathbb{N}$ be an arbitrary set such that $0 \in S$ and $\{0, \ldots, n\} \subset S \implies n+1 \in S$. Also, let $P(n)$ be the proposition $\{0, \ldots, n\} \subseteq S$.
We know that $P(0)$ is true since $0 \in S$.
Now, let's assume that $P(k)$ is true. This means that $\{0, \ldots, k\} \subset S$. By our supposition on S, this implies that $k+1 \in S$. Putting both together, we get that $\{0, \ldots, k+1\} \subset S$ and thus that $P(k+1)$ is true. However, we have proven that $P(k) \implies P(k+1)$. This implies by regular induction that $P(n)$ is true for all $n \in \mathbb{N}$, and thus that strong induction indeed holds.

Proof 2 The proof that the strong induction principle implies the well ordering principle will be done in the first exercise series.

Proof 3 We want to show that the well ordering principle implies the induction principle.

Let $S \subset \mathbb{N}$ be an arbitrary set such that $0 \in S$ and $n \in S \implies n+1 \in S$; and let $S' = \mathbb{N} \setminus S$.

We suppose for contradiction that $S' \neq \emptyset$. By the well ordering principle, this implies that there exists a least element $k \in S'$.

We know that $0 \notin S'$ because $0 \in S$ by hypothesis. This means that $m = k - 1 \in \mathbb{N}$. We know $m \notin S'$ since k was the least element; and thus $m \in S$. Moreover, we know that $m \in S \implies m+1 \in S$ and thus $k \in S$. We have shown that $k \in S$ and $k \in S'$ even though $S \cap S' = \emptyset$. This is our contradiction, showing that $S' = \emptyset$ and thus $S = \mathbb{N}$. We have thus indeed shown the induction principle.

□

Remark This last proof uses a structure named "the minimal criminal". We pick an element which should be minimal with a certain property, but we construct a smaller one with the same property.

Definition: Division Let $a, b \in \mathbb{Z}$, such that $a \neq 0$. We define that a **divides** b, written $a \mid b$ or $b \in a\mathbb{Z}$ (or $b = a\mathbb{Z}$ *(though this notation is awful)*), when $\exists c \in \mathbb{Z}$ such that:

$$b = ac$$

Definition: Prime number Let $n \in \mathbb{Z}_+ = \{1, 2, \ldots\}$.

If $p > 1$ and its only divisors are 1 and p, then it is said to be a **prime**. Otherwise, it is said to be a **composite**.

Theorem Any natural number $n > 1$ has a prime divisor.

Proof Let $S \subset \mathbb{N}_{n \geq 2}$ be the set of numbers strictly greater than 1 which have no prime divisor.

Let's suppose for contradiction that $S \neq \emptyset$. Then, there exists a least element $k \in S$. We notice that k cannot be a prime since, otherwise, $k \mid k$ would be a prime divisor. Since k is composite, we can write $k = ab$ for $1 < a, b < k$. Since $a < k$ and k was the least element, we know that $a \notin S$. Thus, a must have a prime divisor p, meaning that we can write $a = pt$ for some $t \in \mathbb{N}$. This yields that:

$$k = ab = ptb$$

However, this means that k has a prime divisor p, which is our contradiction. This implies that $S = \emptyset$, which concludes our proof.

□

Theorem Any integer $n > 1$ is a product of primes.

Proof The proof is left as an exercise to the reader, since it is very similar to the previous one.

Theorem Let $n \in \mathbb{N}$ be such that $n > 1$.

The prime factorisation of n is unique.

Proof Let n be the smallest number be the smallest integer greater than 1 with two different factorisations:

$$n = p_1 \cdots p_k = q_1 \cdots q_m$$

For all (i, j), we have $p_i \neq q_j$ since, otherwise, we could simplify it on both side and get another smaller integer n with the same property.

Let's suppose without loss of generality that $q_1 > p_1$ and let:

$$t = (q_1 - p_1)q_2 \cdots q_m > 0$$

Then:

$$\begin{aligned} t &= \overbrace{q_1 \cdots q_m}^{=n} - p_1 q_2 \cdots q_m \\ &= n - p_1 q_2 \cdots q_m \\ &= p_1 \cdots p_k - p_1 q_2 \cdots q_m \\ &= p_1(p_2 \cdots p_k - q_2 \cdots q_m) \end{aligned}$$

However, this implies that $p_1 \mid t$. Thus, this implies that $t \geq p_1 > 1$. Now, we saw that $t = (q_1 - p_1)q_2 \cdots q_m$ and $p_1 \neq q_j$ for all j, so $p_1 \mid t$ implies that p_1 must necessarily divide $(q_1 - p_1)$. In other words, there exists a $s \in \mathbb{N}$ such that:

$$q_1 - p_1 = sp_1 \iff q_1 = (s+1)p_1 \iff p_1 \mid q_1$$

This is our contradiction, a prime cannot divide a different prime.

□

2.2 Basic properties of integer arithmetic

Theorem: Euclidean division Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}_+$. There exists two integers $q, r \in \mathbb{Z}$ such that $n = qd + r$ and $0 \leq r < d$. Moreover, these q, r are unique.
The q is named the **quotient**, and the r is named the **remainder**.

Proof of existence Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}_+$.
We consider the following set:

$$S = \{n - kd | k \in \mathbb{Z}\} \cap \mathbb{N} = \{n - kd | k \in \mathbb{Z} \text{ such that } n \geq kd\} \subset \mathbb{N}$$

Intuitively, this represents the set of non-negative numbers with the same rest modulo d as n.
We know that $S \neq \emptyset$. Indeed, if $n \geq 0$, we can pick $k = 0$ to get $n \in S$. Otherwise, if $n < 0$, we can take $k = |n| + 1$, which is such that $kd > |n|$ and thus $n + kd \in S$.
By the well-ordering principle, this means that there exists a smallest element $r \in S$, i.e.:

$$r = n - kd \iff n = kd + r$$

Now, let's suppose for contradiction that $r \geq d$. This means that:

$$n - (k+1)d = n - kd - d = r - d \geq 0$$

However, this is a contradiction since r was the least element in S, and we constructed a new one smaller. We have thus indeed shown the existence of r, k such that $n = kd + r$ and $0 \leq r < d$.

Proof of unicity Let's suppose for contradiction that we can write:

$$n = r_1 + q_1 d = r_2 + q_2 d$$

If $q_1 = q_2$, then necessarily we have $r_1 = r_2$ and they are not unique. Thus, let's suppose without loss of generality that $q_1 > q_2$. This

implies that:

$$r_2 = \underbrace{(q_1 - q_2)}_{>0} d + \underbrace{r_1}_{\geq 0} \geq d$$

However, this is a contradiction to the definition of r_2, which should be such that $0 \leq r_2 < d$.

□

Remark The integers (q, r) can be found by doing an integer long division *(division en colonne* in French).

Definition: GCD Let $a, b \in \mathbb{Z}$.
Their **greatest common divisor**, written $\gcd(a, b)$, is the greatest positive integer c such that $c \mid a$ and $c \mid b$.

Theorem: Euclidean algorithm Let $n, q \in \mathbb{Z}$ and $d \in \mathbb{Z}_+$ such that $n = dq + r$ and $0 \leq r < d$.
Then, $\gcd(n, d) = \gcd(d, r)$.

Proof Let c_1 be an arbitrary divisor of both n and d. Since $n = qd + r$, this means that c_1 also divides $r = n - qd$.
Let c_2 be an arbitrary divisor of both d and r. Since $n = qd + r$, this means that c_2 also divides n.
However, this implies that the set of common divisors of both n and d is the same as the set of common divisors of d and r. This indeed yields that:

$$\gcd(n, d) = \gcd(d, r)$$

□

Euclidean algorithm This lemma is a proof that the Euclidean algorithm works.
Let $d_1 = q_1 d_2 + d_3$. We know that $\gcd(d_1, d_2) = \gcd(d_2, d_3)$. Thus, we can divide d_1 by d_2 to get d_3, then divide d_2 by d_3, and so on until we get $d_k = 0$. We then know that:

$$\gcd(d_1, d_2) = d_{k-1}$$

This always terminate since the sequence of the d_i is strictly decreasing.

Example Let us consider:

$$\gcd(492, 126)$$

We make the following divisions, computed using long division:

$$492 = 126 \cdot 3 + 114, \quad 126 = 114 \cdot 1 + 12, \quad 114 = 12 \cdot 9 + 6, \quad 12 = 6 \cdot 2 + 0$$

Since we got a rest of 0 at the end, it yields that the GCD was the rest of the division right before, 6:

$$\gcd(492, 126) = 6$$

Corollary 1 Let $a, b \in \mathbb{Z}_+$. Then, there exists $x, y \in \mathbb{Z}$ such that:

$$\gcd(a, b) = ax + by$$

Proof This can be proven by using an algorithm. The idea is to first use the Euclidean algorithm, and then rewind back to our numbers.
Let's make a proof by example. In the previous example, we found that:

$$\gcd(492, 126) = 6$$

The intermediate steps of the Euclidean algorithm were:

$$492 = 126 \cdot 3 + 114, \quad 126 = 114 \cdot 1 + 12, \quad 114 = 12 \cdot 9 + 6, \quad 12 = 6 \cdot 2 + 0$$

We start with the second-to-last equality:

$$\gcd(492, 126) = 6 = 114 - 12 \cdot 9$$

We then use the third-to-last equality to see that $12 = 126 - 114 \cdot 1$, so:

$$6 = 114 - (126 - 114 \cdot 1) \cdot 9 = 114 \cdot 10 - 126 \cdot 9$$

Finally, the first equality yields that $114 = 492 - 126 \cdot 3$, and thus:

$$6 = (492 - 3 \cdot 126) \cdot 10 - 126 \cdot 9 = 492 \cdot 10 - 126 \cdot 39$$

To sum up, we found that:

$$6 = \gcd(492, 126) = 492 \cdot 10 - 126 \cdot 39$$

This is the end of our algorithm.

Corollary 2

Let $a, b \in \mathbb{Z}_+$ and $d = \gcd(a, b)$.
The equation $ax + by = c \in \mathbb{Z}$ has a solution $x, y \in \mathbb{Z}$ if and only if $c \in d\mathbb{Z}$ (meaning $d \mid c$).

Proof $\implies$

Let $c \in \mathbb{Z}$ and $x, y \in \mathbb{Z}$ be solutions to $ax + by = c$.
We notice that, by definition of the greatest common divisor, $d \mid a$ and $d \mid a$. In particular, this means that $d \mid ax + by$, and thus this necessarily means that $d \mid c$.

Proof $\impliedby$

Let $c = kd$ for some $k \in \mathbb{Z}$.
By our first corollary, we know we can find $x, y \in \mathbb{Z}$ such that:

$$ax + by = \gcd(a, b) = d$$

Multiplying both sides by k, this implies that:

$$akx + bky = kd \iff a\widetilde{x} + b\widetilde{y} = c$$

for $\widetilde{x} = kx$ and $\widetilde{y} = ky$.
We have indeed found a solution to $ax + by = c$.

□

Definition: Relatively prime

Let $a, b \in \mathbb{Z}_+$.
We say that they are **relatively prime** if:

$$\gcd(a, b) = 1$$

Bézout's theorem

Let $a, b \in \mathbb{Z}_+$.
They are relatively prime if and only if there exists $x, y \in \mathbb{Z}$ such that:

$$ax + by = 1$$

Proof

This is a special case of the second corollary.

Definition: Euler's totient function

Let $n \in \mathbb{Z}_+$.
We define $\varphi(n)$ to be the number of positive integers k, such that $1 \leq k \leq n$ and:

$$\gcd(n, k) = 1$$

Example For instance, since 1 is only coprime with 1:

$$\varphi(1) = 1$$

Also, since 3 is coprime with both 1 and 2:

$$\varphi(3) = 2$$

Property Let p be a prime number. Then:

$$\varphi(p) = p - 1$$

Proof Any of the $p - 1$ numbers strictly smaller than p is coprime with p, so this gives our result.

□

Property Let p and q be different prime numbers. Then:

$$\varphi(pq) = (p - 1)(q - 1)$$

Proof There are pq numbers from 1 to pq. p of them are divisible by q and q of them are divisble by p. We finally need to be careful by not double counting that pq is divisible by both p and q. Thus:

$$\varphi(pq) = pq - p - q + 1 = (p - 1)(q - 1)$$

□

Property Let m, n such that $\gcd(m, n) = 1$.
Then:

$$\varphi(nm) = \varphi(n)\varphi(m)$$

Proof The proof will be done later, using ring theory.

Chapter 3

Groups

RSA

Groups are very useful for the RSA cryptosystem. The algorithm goes as follows:

1. We choose two large distinct primes p, q.
2. Let $m = pq$. We notice that we can easily compute $\varphi(m) = (p-1)(q-1)$.
3. We choose some $e \leq m-1$ such that $\gcd(e, \varphi(m)) = 1$.
4. We use the Euclidean algorithm to find a $d \leq m-1$ such that $ed - k\varphi(m) = 1$ for some $k \in \mathbb{Z}$.
5. We finally publish the encoding key (m, e) and keep secret the decoding key (m, d).

Let's say that Bob wants to send a secret message to Alice. The message is a number x such that $0 \leq x \leq m-1$.

Alice previously published the encoding key (m, e) and kept the decoding key (m, d). Bob uses the public key to compute $y = x^e \bmod m$, and sends y publicly to Alice. It is very hard to inverse this function (this problem is called the Discrete logarithm problem), so this is secure. Alice can finally recover $x = y^d \bmod m$. Other people cannot do that since it is very hard to compute d from m, because it is hard to compute $\varphi(m)$ (this comes from the difficulty to compute the prime factorisation of a number).

To show that this algorithm works, we need to show that:

$$x^{ed} \bmod m = x, \quad \forall x \in \{0, 1, \ldots, m-1\}$$

This is done by group theory.

3.1 Definitions

Definition: Group

A **group** is a non-empty set G together with a binary operation $\cdot : G \times G \mapsto G$, satisfying the following axioms:

- (Associativity) For any $a, b, c \in G$:
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
- (Existence of a neutral element) There exists some $1 \in G$, such that, for any $a \in G$:
$$1 \cdot a = a \cdot 1 = a$$
- (Existence of the inverse) For any $a \in G$, there exists some $a^{-1} \in G$ such that:
$$a^{-1} \cdot a = a \cdot a^{-1} = 1$$

We write groups G, $(G, \cdot)$ or $(G, \cdot, 1)$.

Definition: Order

Let $(G, \cdot)$ be a group.
It is said to be **finite** if $|G| < \infty$. In this case, we name $|G|$ to be the order of the group.

Definition: Abelian group

Let $(G, \cdot)$ be a group.
It is said to be **Abelian** (or commutative) if it also follows the following property, for any $a, b \in G$:

$$a \cdot b = b \cdot a$$

Examples

We have the following examples:

1. $(\mathbb{R}, +, 0)$ is an infinite Abelian group. For any $x \in \mathbb{R}$, the inverse in this group is $-x$.
2. $(\mathbb{Z}, +, 0)$ is another infinite Abelian group.

Definition: Integers modulo n

The set of integers modulo n is written $\mathbb{Z}/n\mathbb{Z}$. Its elements are equivalence classes of the equivalence relation of numbers modulo n:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], \dots, [n-1]\}$$

Definition: Cyclic group of order n

We notice that $(\mathbb{Z}/n\mathbb{Z}, +_m)$ where $+_m$ is the addition modulo m, is an Abelian group of order n. The inverse of an element $[k]$ is $[n-k]$.
This is named the **cyclic group of order n**, written C_n

Example

For instance, in $\mathbb{Z}/12\mathbb{Z} = \{[0], \dots, [11]\}$, we have:

$$[7] + [5] = [12], \quad [10] + [3] = [1]$$

Remark

All sets are not Abelian. Indeed, let us consider the group $GL_n(\mathbb{R})$, which is the set of real $n \times n$ matrices with non-zero determinant with respect to matrix multiplication.
There is indeed a neutral element—the identity matrix—the operation is indeed associative, and they all have inverses. However, this group is non-abelian since matrix multiplication is not commutative in general.

Proposition

Let $n \in \mathbb{Z}^*$ and $a \in \mathbb{Z}$.
a has an inverse with respect to the multiplication modulo n if and only if:

$$\gcd(a, n) = 1$$

Proof

The existence of some $x \in \mathbb{Z}$ such that $ax \bmod n = 1$ is equivalent to the existence of $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. However, by Bézout's theorem, this is equivalent to:

$$\gcd(a, n) = 1$$

□

Observation

Let $G = (\mathbb{Z}/n\mathbb{Z}, \cdot, 1)^*$ be the group of invertible numbers with respect to the multiplication mod n. By our proposition, this is of the form:

$$G = \{1 \leq x \leq n | \gcd(x, n) = 1\}$$

Thus, by definition of $\varphi(n)$, this yields that the order of G is:

$$|G| = \varphi(n)$$

We thus see that this is a finite Abelian group of order $\varphi(n)$, and with identity $[1]$.

3.2 Subgroups and cosets

Definition: Subgroup

Let $(G, \cdot, 1)$ be a group, and $H \subset G$ be a subset of G.
H is a **subgroup** of G if H is such that:

1. $1 \in H$
2. For any $a, b \in H$, then $a \cdot b \in H$.
3. For any $a \in H$, then $a^{-1} \in H$.

Proposition

Let G be a group and $H \subset G$ be a subgroup.
Then, H is a group.

Example 1

We noticed that $(GL_n(\mathbb{R}), \cdot)$ is a group.
Now, we can take $H \subset GL_n(\mathbb{R})$ to be the set of invertible diagonal matrices:

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} | a, b \in \mathbb{R}^* \right\}$$

The identity matrix is indeed in D. Moreover, multiplications and inverses are closed under D:

$$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{pmatrix} \in D$$

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \in D$$

Thus, H is a subgroup of $GL_n(\mathbb{R})$.

Example 2

We notice that $(3\mathbb{Z}, +, 0) \subset (\mathbb{Z}, +, 0)$ is a subgroup.

Definition: Subgroup generated by one element

Let G be a group, and $g \in G$.
The **subgroup generated by g** is defined as:

$$\langle g \rangle = \{1, g, g^2, \ldots\} \cup \{g^{-1}, g^{-2}, \ldots\}$$

where $g^{i+k} = g^i \cdot g^k$ is the operation $\cdot$ repeated on $i + k$ g's.

Property $\langle g \rangle \subset G$ is a subgroup by construction.

Remark If g has a finite order k, then we just have:

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{k-1}\}$$

Indeed, we for instance have that $g^{k-1} = g^{-1}$ since:

$$g^{k-1} g = g^k = 1$$

Example

Let us consider the group $G = (\mathbb{Z}, +, 0)$, and $g = 3 \in \mathbb{Z}$. Then, this generates:

$$\langle g \rangle = \{0, \pm 3, \pm 6, \ldots\} = 3\mathbb{Z}$$

Definition: Order of an element

Let $(G, \cdot)$ be a group. If there exists some minimal $n \in \mathbb{N}^*$ such that $g^n = 1$, then n is called the **order** of g.

Remark This must not be mistaken with the order of the group.

Observation In a finite group, each element has a finite order by the pigeon-hole principle. If however the group is infinite, some elements might be such that $g^n \neq 1$ for all n.

Definition: Left coset

Let G be a group, $H \subset G$ be a subgroup and $g \in G$.
The **left coset gH** (the left coset of g with respect to H) is the set of group elements of the form:

$$gH = \{gh | h \in H\}$$

Remark This is not necessarily a subgroup, since there might not be the identity element for instance.

Properties

Let G be a finite group, and $H \subset G$ be a subgroup of G.
We have the following properties:

1. Two left cosets xH and yH are either equal or disjoint:

$$xH = yH \quad \text{or} \quad xH \cap yH = \emptyset$$

2. Any $g \in G$ belongs to a left H-coset.
3. For any $x \in G$, then $|xH| = |H|$.

Proof 1 Let's suppose that we have $xH \cap yH \neq \emptyset$.
Then, there exist $h_1, h_2 \in H$ such that $xh_1 = yh_2$. Since elements of a group are invertible, we get:

$$x = y \underbrace{h_2 h_1^{-1}}_{\in H} = yh_3$$

This means that any element of xH can be written as:

$$xh = y \underbrace{h_3 h}_{\in H} = yh_4 \in yH$$

Since any element $xh \in xH$ is such that $xh \in yH$, this yields that $xH \subset yH$. By starting the proof again but using a symmetrical argument, we can get that $yH \subset xH$. Combining both together, we indeed find $xH = yH$.

Proof 2 Let $g \in G$. We consider the following coset:

$$gH = \{g \cdot 1, g \cdot h_1, g \cdot h_2, \ldots\}$$

However, $g = g \cdot 1$; so $g \in gH$.

Proof 3 To show that two sets have the same cardinality, a good way is to find a bijection $f : H \mapsto xH$. Thus, let:

$$f(h) = xh$$

We first notice that f is surjective since we reach any element of xH by definition of cosets. It is moreover injective since:

$$xh_1 = xh_2 \iff x^{-1}xh_1 = x^{-1}xh_2 \iff h_1 = h_2$$

This yields that f is bijective, and thus that $|H| = |xH|$ for any $x \in G$.

□

Example

Let us consider the group $(\mathbb{Z}, +, 0)$ and the subgroup $3\mathbb{Z} \subset \mathbb{Z}$.
The coset of 0 with respect to $3\mathbb{Z}$ in $\mathbb{Z}$ is:

$$\{0 + 3k\}_{k \in \mathbb{Z}} = 3\mathbb{Z}$$

The coset of 1 with respect to $3\mathbb{Z}$ in $\mathbb{Z}$ is:

$$\{1+3k\}_{k\in\mathbb{Z}} = \{1,-2,4,-5,7,\dots\}$$

which the set of all numbers which rest after a division by 3 is 1.
We notice that the coset of 10 with respect to $3\mathbb{Z}$ in $\mathbb{Z}$ is exactly the same coset:

$$\{10+3k\}_{k\in\mathbb{Z}} = \{1,-2,4,-5,7,\dots\}$$

Definition: Index The number of left H-cosets in G is called the **index** of H in G, written $[G:H]$.

Lagrange's theorem Let G be a finite group, and $H \subset G$ be a subgroup.
Then, $|H|$ divides $|G|$; and:

$$\frac{|G|}{|H|} = [G:H]$$

Proof We know that each $g \in G$ belongs to a left H-coset and that either $xH = yH$ or $xH \cap yH = \emptyset$. We can thus write $G = \bigcup_{i=1}^{r} x_i H$ as a disjoint union of finitely many left H-cosets.
This allows us to compute its cardinality:

$$|G| = \sum_{i=1}^{r} |x_i H|$$

Now, we now that $|x_i H| = |H|$, so:

$$|G| = \sum_{i=1}^{r} |H| = r|H|$$

We indeed get that $|H|$ divides $|G|$. However, r is the number of cosets, so this is the index of H in G, yielding:

$$[G:H] = r = \frac{|G|}{|H|}$$

□

Corollary 1 Let G be a finite group and $g \in G$.
Then, the order of g divides $|G|$.

Proof Let us consider the subgroup generated by g:

$$H = \langle g \rangle = \left\{1, g, \dots, g^{k-1}\right\}$$

where k is the order of g.
We know that $H \subset G$ is a subgroup. Thus, by Lagrange's theorem, $|H|$ divides $|G|$. However, $|\langle g \rangle| = k$, so we indeed got that the order of g divides $|G|$.

□

Corollary 2 Let G be a finite group, and $g \in G$.
Then, $g^{|G|} = 1$.

Proof Let k be the order of g. We know that k divides $|G|$, so there exists some integer t such that:

$$|G| = kt$$

This yields that:

$$g^{|G|} = \left(g^k\right)^t = 1^t = 1$$

□

Euler's theorem

Let $a, n \in \mathbb{Z}_+$ such that $\gcd(a, n) = 1$.
Then:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof

Let $G = (\mathbb{Z}/n\mathbb{Z}, \cdot, 1)^*$. We saw that $|G| = \varphi(n)$.
We know that if $\gcd(a, n) = 1$, then $[a] \in G$. This tells us by our second corollary that:

$$[a]^{\varphi(n)} = [1]$$

In other words:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

□

Fermat's little theorem

Let $a \in \mathbb{Z}_+$ and p be a prime such that p does not divide a.
Then:

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof

We notice that, by hypothesis, $\gcd(a, p) = 1$. So, by Euler's theorem:

$$a^{\varphi(p)} \equiv 1 \pmod{p} \iff a^{p-1} \equiv 1 \pmod{p}$$

□

Monday 9th October 2023 — **Lecture 3 : Homeomorphisms are better though**

Proposition: RSA

Let p, q be distinct primes, and $m = pq$. Also, let $e \in \mathbb{Z}$ be such that $\gcd(e, \varphi(m)) = 1$ and $d, k \in \mathbb{Z}$ be such that $ed - k\varphi(m) = 1$.
Then, for any $x \in \{1, \dots, m\}$:

$$x^{ed} \equiv x \pmod{m}$$

Proof

We first want to show that $x^{ed} \equiv x \pmod{p}$. To do so, we consider two cases. If x is divisible by p, then $x^{ed} \equiv 0 \pmod{p}$ and $x \equiv 0 \pmod{p}$. If x is not divisible by p then, by Fermat's theorem:

$$x^{k\varphi(m)} = x^{k(p-1)(q-1)} = \left(x^{(p-1)}\right)^{k(q-1)} \equiv 1^{k(q-1)} \equiv 1 \pmod{p}$$
$$\implies x^{k\varphi(m)+1} \equiv x \pmod{p}$$

Thus, in both cases:

$$x^{ed} \equiv x \pmod{p}$$

We can use a completely symmetrical argument to get that:

$$x^{ed} \equiv x \pmod{q}$$

This means that $x^{ed} - x$ is divisible by both p and q. However, a number is divisible by two different prime numbers if and only if it is divisible by the product of those prime numbers. This means that $x^{ed} - x$ is divisible by $pq = m$, and thus:

$$x^{ed} \equiv x \pmod{m}$$

□

Example

Let $p = 3$ and $q = 11$. Then, we have $m = pq = 33$ and $\varphi(m) = (p-1)(q-1) = 20$. Finally, we pick $e = 7$, since $\gcd(7, 20) = 1$.

We compute d by using the extended Euclidean algorithm to notice that:

$$1 = \gcd(7, 20) = 7 \cdot 3 - 20$$

This yields that $d = 3$. Thus, our encoding key is $(m, e) = (33, 7)$ and our decoding key is $(m, d) = (33, 3)$.
Now, let's suppose that we want to send $x = 20$. To encode it, we compute:

$$x^e \bmod m = 20^7 \bmod 33 = 26$$

which we can get through fast exponentiation.
Then, to decode we do:

$$y^d \bmod m = 26^3 \bmod 33 = 20 = x$$

as expected.

3.3 Homomorphisms

Definition: Group of roots of unity

The **group of n^{th} complex roots of unity**, written C_n, is:

$$\sqrt[n]{1} = \left\{ e^{\frac{2\pi k i}{n}}, k = 0, 1, \dots, n-1 \right\} = C_n$$

with the regular complex multiplication.

Remark This is named the cyclic group of order n. This is what we named $(\mathbb{Z}/n\mathbb{Z}, +, 0)$ too, but this makes sense since, in C_5, multiplying the third root (q_2) and the fifth one (q_4) yields the second one $(q_2 \cdot q_4 = q_{(2+4) \bmod 5} = q_1)$; meaning that this is like adding numbers modulo n. The two groups are thus, in some sense, structurally the same.
This introduces the following notion.

Definition: Homomorphism

Let G, H be groups.
A map $\varphi : G \mapsto H$ is a **group homomorphism** if, for any $x, y \in G$:

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

where the first group operation $\cdot$ is done in G, and the second one in H.

Trivial homomorphism

Let G, H be groups, of identity 1_G and 1_H, respectively.
We notice that the following is a trivial homomorphism:

$$\varphi(x) = 1_H, \quad \forall x \in G$$

This shows that there always exists a homomorphism from a group to another one.

Proposition

Let G, H be groups of identity 1_G and 1_H, respectively. Moreover, let $\varphi : G \mapsto H$ be a homomorphism.
Then, $\varphi(1_G) = 1_H$ and $\varphi\left(x^{-1}\right) = \varphi(x)^{-1}$ for any $x \in G$.

Proof Let $x, y \in G$. Then, we notice the following important property:

$$\varphi(x) = \varphi\left(xyy^{-1}\right) = \varphi\left(xy^{-1}\right)\varphi(y) \implies \varphi\left(xy^{-1}\right) = \varphi(x)\varphi(y)^{-1}$$

Thus, if $y = x$:

$$\varphi(1_G) = \varphi\left(xx^{-1}\right) = \varphi(x)\varphi(x)^{-1} = 1_H$$

And, if $x = 1_G$:

$$\varphi\left(y^{-1}\right) = \varphi\left(1_G y^{-1}\right) = \varphi(1_G)\varphi(y)^{-1} = 1_H\varphi(y)^{-1} = \varphi(y)^{-1}$$

□

Definition: Isomorphism

Let G, H be groups, and $\varphi : G \mapsto H$ be a homomorphism.
If φ is invertible, then it is named a **isomorphism**. G and H are then said to be **isomorphic** groups, written $G \simeq H$.

Remark This means that we can find a group homomorphism $\psi : H \mapsto G$ such that $\varphi \circ \psi = \mathrm{Id}_H$ and $\psi \circ \varphi = \mathrm{Id}_G$ where Id_X maps an element of X to itself.

Definition: Automorphism

Let G be a group, and $\varphi : G \mapsto G$ be a homomorphism mapping elements from G to G.
Then, φ is named a group **automorphism**.

Example

Following our intuition from the beginning of this section, we want to show that:

$$C_n \simeq (\mathbb{Z}/n\mathbb{Z}, 0, +)$$

where $C_n = \left\{1, q, \dots, q^{n-1}\right\}$ is the group of n^{th} root of unity, as usual.
We will pick the following isomorphism:

$$\varphi : q^k \mapsto [k]$$

This is indeed a bijection, which respects the group operations:

$$\varphi\left(p^i q^j\right) = \varphi\left(q^{i+j}\right) = [i+j]$$

$$\varphi\left(p^i\right)\varphi\left(q^j\right) = [i] + [j] = [i+j]$$

Thus, from the viewpoint of group theory, those two groups are indistinguishable one from another.

Definition: Generator

Let G be a group.
The **generators** of G are the elements of a minimal subset of G such that any element of G can be written as a product of those generators and their inverses.

Definition: Cyclic group

Let G be a group.
If it is generated by a single element, we say that it is **cyclic**.

Example 1

Let us consider the group of n^{th} root of unity:

$$C_n = \left\{1, q, \dots, q^{n-1}\right\}$$

We can pick the generator $\{q\}$, showing it is indeed cyclic. We could also take $\left\{q^{n-1}\right\}$ since $q^{n-1} = q^{-1}$. In fact, we can pick $\left\{q^k\right\}$ for any k such that $\gcd(k, n) = 1$.

Example 2

Let us consider $(\mathbb{Q}_{>0}, \cdot, 1)$.
We see that the set of primes is a generator, since we can use the prime factorisation of the numerator and of the denominator. However, if we throw away one prime, then we will not be able to represent some number; indeed showing they are generators.

Definition: Relation

Any equation satisfied by some group elements is called a **relation**.

Remark Since we only have manipulate group elements thanks to the group operation $\cdot$, a relation can always be written in the form:

$$x_1 \cdot x_2 \cdots x_n = y_1 \cdot y_2 \cdots y_m, \quad x_1, \dots, y_m \in G$$

Multiplying both sides of this equation by $(y_1 \cdots y_m)^{-1}$, it means that we can write any relation as:

$$z_1 \cdot \cdots z_k = 1, \quad z_1, \dots, z_k \in G$$

We can then name the relation $R = z_1 \cdots z_k$.

Example For instance, in C_n, $q^n = 1$ and $q^{n+3} = q^3$ are relations.

Definition: Presentation in generators and relations

Let G be a group.

A **presentation in generators and relations** of G is an expression $\langle S|R\rangle$, where S is a set of generators, and R is a minimal set of relations that only use the generators in S and that are such that any other relation in G follows from these.

Example For instance, $C_n = \langle q|q^n = 1\rangle$ is such a presentation of C_n. We for instance indeed get that $q^{n+3} = q^3$ by multiplying both sides of $q^n = 1$ by q^3.

Proposition

Let $G = \langle S|R_1 = 1, \dots, R_k = 1\rangle$, H be a group and $a_1, \dots, a_{|S|} \in H$.

1. There is at most one homomorphism $\varphi : G \mapsto H$ such that $\varphi(S_i) = a_i$ for all generators $S_i \in S$.
2. There exists such a homomorphism if and only if we have $a_{i_1} \cdots a_{i_n} = 1_H$ for all relations $R_j = S_{i_1} \cdots S_{i_n} = 1_G$ (all relations are satisfied by the images of the generators $a_i = \varphi(S_i)$).

Proof 1 This is a constructive proof. If there exists a homomorphism $\varphi : G \mapsto H$ such that $\varphi(S_i) = a_i$ for all $S_i \in S$, we can force its other values:

1. We need $\varphi\left(S_i^{-1}\right) = \varphi(S_i)^{-1}$ for each generator $S_i \in S$.
2. Any element $x \in G$ can be expressed as a product of generators or their inverses $S_1 \cdots S_n$. So, this requires:

$$\varphi(x) = \varphi(S_1 \cdots S_n) = \varphi(S_1) \cdots \varphi(S_n)$$

There is no choice in this construction, showing the unicity.

Proof 2 $\implies$ We suppose by hypothesis that there exists a homomorphism $\varphi : G \mapsto H$ such that $\varphi(S_i) = a_i$ for all generators S_i.

Let's suppose for contradiction that there exists some relation $R_j = S_1 \cdots S_k = 1$, which is not satisfied by the images of the generators. In other words:

$$\varphi(S_{i_1}) \cdots \varphi(S_{i_\ell}) \neq 1_H$$

However, by definition of a relation and since φ is a homomorphism:

$$\varphi(S_{i_1} \cdots S_{i_\ell}) = \varphi(1_G) = 1_H$$

This is a contradiction to the fact that φ is a homomorphism.

Proof 2 idea $\impliedby$ We want to show that the construction from part 1 does not have a contradiction.

First, we notice the following fact. By definition of the presentation in generators and relations, any relation $S_{i_1} \cdots S_{i_k} = 1$ on G follows from $R_1, \dots, R_k$. However, this means that any relation $\varphi(S_{i_1}) \cdots \varphi(S_{i_k}) = 1$ also follows from the fact that the $\varphi(S_i)$ satisfy the relations $R_1, \dots, R_k$.

The rest of this proof is taken from an explantation from Zichen Gao on EdStem. Now, the only possible contradiction in the construction of φ in the first part of the proof is that we could have two different definitions for some $\varphi(x)$ for a $x \in G$. Indeed, an element x can be written in at least two different ways as a product of generators:

$$x = s_1 \cdots s_n = t_1 \cdots t_m$$

However, this is equivalent to the following relation on G:

$$s_1 \cdots s_n t_1^{-1} \cdots t_m^{-1} = 1$$

Using the fact we noticed at the beginning of this proof, we know that, since this is a relation on G, the images of the generators also respect it:

$$\varphi(s_1) \cdots \varphi(s_n)\varphi(t_1)^{-1} \cdots \varphi(t_n)^{-1} = 1$$

However, this is equivalent to:

$$\varphi(s_1) \cdots \varphi(s_n) = \varphi(t_1) \cdots \varphi(t_n)$$

We thus indeed have no problem in the definition of $\varphi(x)$, it has a unique value.

□

Example We want to make a homomorphism $f : C_8 \mapsto C_4$, where:

$$C_8 = \langle q | q^8 = 1 \rangle, \quad C_4 = \langle t | t^4 = 1 \rangle$$

We only need to consider how the generator q is mapped. We thus consider the mapping $\varphi_k : q \mapsto t^k$ for an arbitrary $k \in \{0, 1, 2, 3\}$. There is a homomorphism if and only if $\varphi_k(q)^8 = 1$, i.e.:

$$1 = \varphi_k(q)^8 = \left(t^k\right)^8 = t^{8k} = \left(t^4\right)^{2k} = 1^{2k} = 1$$

Thus, there is no condition on k for $\varphi_k(q) = t^k$ to be a homomorphism. This yields 4 different homomorphisms.

		1	q	q^2	q^3	q^4	q^5	q^6	q^7
φ_0	$k=0$	1	1	1	1	1	1	1	1
φ_1	$k=1$	1	t	t^2	t^3	1	t	t^2	t^3
φ_2	$k=2$	1	t^2	1	t^2	1	t^2	1	t^2
φ_3	$k=3$	1	t^3	t^2	t	1	t^3	t^2	t

We finally notice that no φ_k is an isomorphism since the C_8 and C_4 have a different size and, thus, no $f : C_8 \mapsto C_4$ can be bijective.

Monday 16th October 2023 — **Lecture 4 : Defining normality mathematically**

Definition: Kernel Let $\varphi : G \mapsto H$ be a homomorphism.
Its **kernel** is the set of elements $g \in G$ such that $\varphi(g) = 1_H$.

Example For instance, considering the previous example:

$$\ker \varphi_1 = \{1, q^4\}$$

Proposition Let $\varphi : G \mapsto H$ be a group homomorphism.
Then, $\ker \varphi \subset G$ is a subgroup.

Proof

- We first notice that the identity belongs to the kernel. Indeed, $\varphi(1) = 1$, and thus $1 \in \ker \varphi$.
- It is closed under the group operation. Indeed, if $a, b \in \ker \varphi$, it means that $\varphi(a) = 1$ and $\varphi(b) = 1$. This implies that $\varphi(ab) = \varphi(a)\varphi(b) = 1$, and thus that $ab \in \ker \varphi$.
- It is also closed under the inverse. Indeed, if $a \in \ker \varphi$, it means that $\varphi(a) = 1$. This implies that $\varphi\left(a^{-1}\right) = \varphi(a)^{-1} = 1$, and thus $a^{-1} \in \ker \varphi$.

□

Definition: Normal subgroup

Let G be a group, and $H \subset G$ be a subgroup.
H is a **normal subgroup**, written $H \lhd G$, if for any $h \in H$ and $g \in G$, we have:

$$ghg^{-1} \in H$$

Remark

We will justify the usefulness of this definition a bit after, showing that normal subgroups allow us to create new groups out of cosets.

Observation

Let G be Abelian group, and $H \subset G$ be a subgroup.
Then, H is a normal subgroup:

$$ghg^{-1} = gg^{-1}h = h \in H, \quad \forall h \in H, g \in G$$

Proposition

Let $\varphi : G \mapsto H$ be a group homomorphism.
Then, $\ker \varphi \lhd G$ is a normal subgroup.

Proof

Let $h \in \ker \varphi$ and $g \in G$ be both arbitrary.
To show that $ghg^{-1} \in \ker \varphi$, we want to show that $\varphi\left(ghg^{-1}\right) = 1$. And, indeed:

$$\varphi\left(ghg^{-1}\right) = \varphi(g)\underbrace{\varphi(h)}_{=1}\varphi\left(g^{-1}\right) = \varphi(g)\varphi(g)^{-1} = 1$$

since $h \in \ker \varphi$ and thus $\varphi(h) = 1$.

□

Definition: Image

Let $\varphi : G \mapsto H$ be a group homomorphism.
Its **image** is $\varphi(G) = \{h \in H | \exists g \in G, \varphi(g) = h\}$, the set of all elements that it reaches.

Example

In our previous example, we had:

$$\varphi_2(C_8) = \left\{1, t^2\right\}$$

Proposition

Let $\varphi : G \mapsto H$ be a homomorphism.
Its image $\varphi(G)$ is a subgroup of H.

Proof

- We notice that the identity is in the image. Indeed, $\varphi(1_G) = 1_H$.
- This is moreover closed under the group operation. Indeed, if $a_1, a_2 \in \varphi(G)$, then there exists $g_1, g_2 \in G$ such that $a_1 = \varphi(g_1)$ and $a_2 = \varphi(g_2)$. Now, $g = g_1 g_2$ is such that:

  $$\varphi(g) = \varphi(g_1)\varphi(g_2) = a_1 a_2$$

  This shows that $a_1 a_2 \in \varphi(G)$.
- This is finally closed under the inverse. Indeed, if $a \in \varphi(G)$, then there exists a $g \in G$ such that $\varphi(g) = a$. However, g^{-1} is such that $\varphi\left(g^{-1}\right) = \varphi(g)^{-1} = a^{-1}$, showing that $a^{-1} \in \varphi(G)$.

Remark In general, the image is not a normal subgroup.

3.4 Elliptic curves

Remark The following introduction will be very brief. However, elliptic curves represent a very broad area of maths, which is very useful.

Definition: Elliptic curve An **elliptic curve** is a curve for which there exists some $a, b \in \mathbb{R}$ such that it satisfies the following equation:

$$y^2 = x^3 + ax + b$$

Property We notice that it is always symmetric along the x axis, since y is squared.

Definition: Elliptic curve group Let us consider some elliptic curve. Both the real points and the rational points on this elliptic curve has a group structure.

Given two elements P, Q on the curve, we introduce an operation $+$, which is such that $P + Q = -R$ if and only if P, Q, R are collinear. This has the following properties:

- The zero is at $x \to \infty$. It is such that $P + 0 = 0 + P = P$.
- $-P$ is the point symmetric with respect to the horizontal axis.

This is (somehow) an associative law.

Lenstra's algorithm Let $n \in \mathbb{N}$, we want to factorise it using elliptic curves.

1. We pick an elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}/n\mathbb{Z}$, and a point $P(x_0, y_0)$ on it.
2. We compute $2P, 3!P, \dots, k!P$ for some integer $k > 0$. This only involves computing operations $2Q$ which are easy to do on a computer. For instance:

$$3!P = 3 \cdot 2P = 2 \cdot 2P + 2P$$

This operation involves computing slopes of lines modulo n. This only makes sense if v is invertible modulo n, meaning $\gcd(n, v) = 1$. Thus, if the operation fails, it means that $\gcd(n, v) > 1$ and thus that we have found a non-trivial factor of n. Otherwise, we change slightly the elliptic curve.

This method is very efficient, and its asymptotic time is sub-exponential in $\log(n)$.

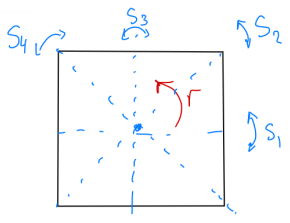
3.5 Dihedral groups

Definition: Group of rigid symmetries The **group of rigid symmetries of a flat regular n-gon** is written D_n. The group law is composition: a rotation of angle π followed by a rotation of angle $\frac{\pi}{2}$ is a rotation of angle $\frac{3\pi}{2}$.

In other words, it is the group of operations (rotations and axial symmetries) we can do, which will yield the same shape.

Example Let us consider D_4. We thus want to find the symmetries of a square.

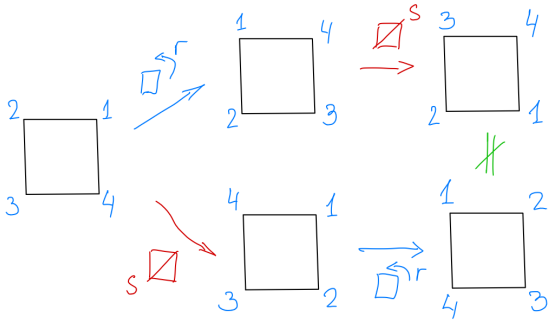
We can rotate the square by angles 0, $\frac{\pi}{2}$, π and $\frac{3\pi}{2}$, which we write $1, r, r^2, r^3$. We can also take axial reflections, along the x-axis, the y-axis and the two diagonals, which we write s_1, s_2, s_3, s_4.



Thus, we have $|D_4| = 8$.

Remark D_n is not an Abelian group.

Let us consider D_4. We label the vertices of our square to be able to know if two transformations are equal. We notice that the following transformations are not commutative, showing $rs \neq sr$:



Proposition The number of elements in D_n is $2n$.

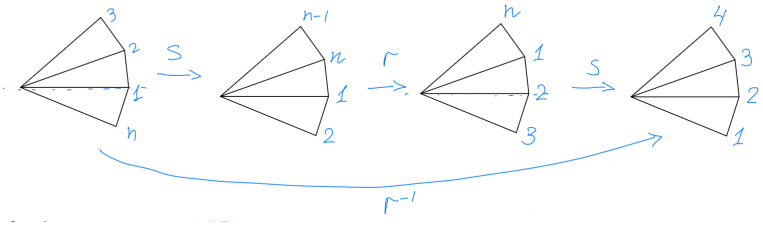
Proof We label all the vertices of our polygon from 1 to n. We can pick a transformation that sends vertex 1 to any of the n other places. Then, the vertex 2 needs to stay next to the first one, giving 2 possibilities. This yields that $|D_n| \leq 2n$.

However, we are able to construct $2n$ different operations with the n rotations (including the one of angle 0), and the n symmetries. This shows that $|D_n| \geq 2n$.

We can therefore indeed conclude that $|D_n| = 2n$.

□

Relation Let s be a reflection through a vertex, and $r_{\frac{2\pi}{n}}$ be a counterclockwise rotation of angle $\frac{2\pi}{n}$. We can see that $srs = r^{-1}$:



We thus deduce the first relation, $srs = r \iff (sr)^2 = 1$.

Proposition: Presentation in generators and relations

D_n admits the following presentation in generators and relations:

$$D_n = \langle r, s | r^n = 1, s^2 = 1, srs = r^{-1} \rangle$$

Moreover, the elements of D_n can be written as:

$$D_n = \{1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$$

Proof idea

We noticed that $sr = r^{-1}s$. Thus, any product $s^{i_1}r^{i_2}s^{i_3}\cdots$ can be written in the form $s^a r^b$. Now, we know that $s^2 = 1$, telling us that:

$$D_n = \{r^i, sr^j | (i,j) \in \{0,1,\dots,n-1\} \times \{0,1,\dots,n-1\}\}$$

It is possible to show that any additional relation will reduce the number of elements. However, we already have $2n$ elements and we showed that $|D_n| = 2n$. Therefore, it is impossible that there is another relation.

Definition: Subgroup of rotations

Let $R = \langle r \rangle = \{1, \dots, r^{n-1}\} \subset D_n$. It is a normal subgroup, the **subgroup of rotations**.

Normal subgroup

We want to show that $gr^k g^{-1} = r^j$ for any $g \in D_n$. If $g = r^i$, this is easy:

$$r^i r^k r^{-i} = r^{i+k+-i} = r^k \in R$$

If $g = s$, we use the fact that $s^2 = 1$ (which notably implies that $s^{-1} = s$) and $srs = r^{-1}$:

$$sr^k s^{-1} = s\underbrace{rr\cdots r}_{k \text{ times}}s = s\underbrace{rs^2rs^2\cdots s^2r}_{k \text{ times}}s = (srs)^k = r^{-k} = r^{n-k} \in R$$

We can make a similar proof if $g = sr^i$.

Cosets

We notice that it has two cosets:

$$1R = \{1, r, \dots, r^{n-1}\}$$

$$sR = \{s, sr, \dots, sr^{n-1}\}$$

They are indeed all since $|1R| = |sR| = n$, so there must only be 2 of them.

Definition: Subgroup of symmetry

Let $K = \langle s \rangle = \{1, s\} \subset D_n$.
This is a subgroup, but not a normal one. Indeed, since $sr^{-1} = rs$, we know that $rsr^{-1} = rrs = r^2 s \notin K$.

3.6 Quotient groups

Quotient group

If $H \lhd G$ is normal, then the set of left H-cosets in G naturally form a group, named the **quotient group** and written G/H. We define $(xH)(yH) = xyH$ where $1H$ is the neutral element and $x^{-1}H$ is the inverse.
However, the choice of the representative z of zH is ambiguous, so we need to show this makes sense.

Proposition

Let $H \lhd G$ be normal.
The product on cosets is well defined and defines a group structure of the set of cosets.

Proof

We need to check that the product does not depend on the choice of the representation.

Let $x' \in xH$ and $y' \in yH$. We know by definition that there exists some $h_1, h_2 \in H$ such that $x' = xh_1$ and $y' = yh_2$. We want to show that $x'y' \in xyH$:

$$x'y' = xh_1yh_2 = xy\underbrace{y^{-1}hy}_{=h_3}h_2 = xyh_3h_2 \in xyH$$

where we used that $h_3 \in H$ since H is normal.
Since $x'y' \in xyH$, this shows that we cannot get a different result for this operation by choosing different representatives of our cosets.

□

Example

Let us consider the cosets of $R = \{1, r, \dots, r^{n-1}\}$ in D_n. We saw that they were:

$$1R = \{1, r, \dots, r^{n-1}\}, \quad sR = \{s, sr, \dots, sr^{n-1}\}$$

We consider the quotient group D_n/R. It has 2 elements, which are $1R$ and sR. As mentioned earlier, the operation is the product of their representations, and the neutral element is $1R$.
For instance:

$$(1R)(sR) = sR, \quad (sR)(sR) = s^2R = 1R$$

We can verify that this works picking any representative of the cosets. For instance, for $(sR)(1R) = (sR)$, let $g_1 \in sR$ and $g_2 \in 1R$. Then:

$$g_1g_2 = \underbrace{sr^i}_{\in sR}\underbrace{r^j}_{\in 1R} = sr^{i+j} \in sR$$

This indeed shows that $(g_1R)(g_2R) = sR$, and is non-ambiguous.

Remark It is possible to show that there exists only one group of 2 elements (this directly comes from the fact that we need an identity and an inverse for all elements). Our quotient group is thus isomorphic to $D_n/R \simeq C_2 = \langle t | t^2 = 1 \rangle = \{1, t\}$. In that case, $\varphi(1) = 1R$ and $\varphi(t) = sR$.

Monday 23rd October 2023 — **Lecture 5 : Proof by staring**

3.7 Symmetric group

Definition: Permutation

A **permutation** of an *ordered* set is a bijective map.

Example For instance, the following function π is a permutation:

$$\pi(\{1, 2, 3, 4, 5\}) = \{5, 2, 4, 3, 1\}$$

Definition: Symmetric group

The **symmetric group** S_n is the group of all permutations of n elements. The group operation is the composition of the permutations (composition of the functions).
The identity is the trivial permutation, where $\mathrm{id}(i) = i$ for all $i \in \{1, \dots, n\}$. The inverse permutation of $\rho \in S_n$ is the inverse function ρ^{-1} such that $\rho^{-1}(k) = i$ when $\rho(i) = k$.

Remark This is not an Abelian group.

Remark By doing combinatorics, we can find that $|S_n| = n!$.

Example

S_3 is for instance:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

The last element for instance means that $\pi(1) = 3$, $\pi(2) = 1$ and $\pi(3) = 2$. We notice that this notation is not nice to use, so we will improve it.
The first element is typically written 1 or e, since this is the identity.

Definition: Orbit

Let $\rho \in S_n$, and $x \in \{1, \dots, n\}$ be a number (notice that it is not an element of S_n). The **orbit** of x under the action of $\langle \rho \rangle$ is defined as:

$$\mathrm{Orb}_\rho(x) = \left\{ \rho^j x | \rho^j \in \langle \rho \rangle \right\} = \left\{ x, \rho x, \rho^2 x, \dots, \rho^{k-1} x \right\}$$

This is all the numbers in $\{1, \dots, n\}$ that can be reached by applying ρ successively.

Example

Let us consider $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$. Then:

$$\mathrm{Orb}_\rho(1) = \mathrm{Orb}_\rho(2) = \{1, 2\}$$

Indeed, 3 can never be reached by applying ρ to 1 or 2. However:

$$\mathrm{Orb}_\rho(3) = \{3\}$$

We thus see that:

$$\{1, 2, 3\} = \mathrm{Orb}_\rho(1) \cup \mathrm{Orb}_\rho(3)$$

Proposition

Let $\rho \in S_n$, and $x_1, x_2 \in \{1, \dots, n\}$.
Either their orbits are equal, or they are disjoint:

$$\mathrm{Orb}_\rho(x_1) = \mathrm{Orb}_\rho(x_2) \quad \text{or} \quad \mathrm{Orb}_\rho(x_1) \cap \mathrm{Orb}_\rho(x_2) = \emptyset$$

Proof

Let's suppose that $\mathrm{Orb}_\rho(x_1) \cap \mathrm{Orb}_\rho(x_2) \neq \emptyset$. Thus, let $y \in \mathrm{Orb}_\rho(x_1) \cap \mathrm{Orb}_\rho(x_2)$.
This means that $y = \rho^i x_1$ and $y = \rho^k x_2$ for some i, j. However, this yields that:

$$x_2 = \rho^{i-k} x_1$$

This shows that $x_2 \in \mathrm{Orb}_\rho(x_1)$. However, by definition of the orbit, it also means that $\rho^k x_2 \in \mathrm{Orb}_\rho(x_1)$ for any k. We have thus just showed that $\mathrm{Orb}_\rho(x_2) \subset \mathrm{Orb}_\rho(x_1)$.
We can do the same reasoning to find that $\mathrm{Orb}_\rho(x_1) \subset \mathrm{Orb}_\rho(x_2)$. Putting this fact with the previous one, we get $\mathrm{Orb}_\rho(x_1) = \mathrm{Orb}_\rho(x_2)$.
This thus indeed shows that, if $\mathrm{Orb}_\rho(x_1) \cap \mathrm{Orb}_\rho(x_2) \neq \emptyset$, then $\mathrm{Orb}_\rho(x_1) = \mathrm{Orb}_\rho(x_2)$; which is equivalent to our proposition.

□

Personal remark: Fun fact

This means that we can construct an equivalence relation using those orbits; where two elements of $\{1, \dots, n\}$ are in relation if and only if they are in the same orbit.

Definition: Trivial orbit

Let $\rho \in S_n$, and $x \in \{1, \dots, n\}$.
If $\mathrm{Orb}_\rho(x) = \{x\}$ has a single element, then it is said to be a **trivial orbit**.

Definition: Cycle

$\pi \in S_n$ is said to be a **cycle** if it has a single non-trivial orbit (and possibly several trivial orbits). Its **length** is the number of elements inside its non-trivial orbit.

Letting x be any element of its non-trivial orbit, we note a cycle of length q as:

$$\pi = \big(x, \pi(x), \pi^2(x), \dots, \pi^{q-1}(x)\big)$$

In other words, any element which is in the cycle in mapped to the one to its right in this notation (if it is the last element, it is mapped to the first element); and any element which is not in this notation is mapped to itself.

Remark This notation is not completely unique, since we can take a cyclic permutation: $(1,2,3) = (2,3,1)$. However, as soon as we fix the first element, this notation is unique.

Example We notice that $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$ is a cycle: it has two orbits, but only one non-trivial orbit. We can thus write:

$$\rho = (1,2)$$

This means that $\rho(1) = 2$, the element to its right; $\rho(2) = 1$ the first element (the element to its right with an overflow); and $\rho(3) = 3$ since it is not in the notation. Note that we could have written equivalently $\rho = (2,1)$.

However, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$ is not a cycle, since it has two non-trivial orbits:

$$\mathrm{Orb}_\sigma(1) = \{1,2\}, \quad \mathrm{Orb}_\sigma(3) = \{3,4\}$$

Personal remark: Cycle inverse The inverse of a cycle $(x_1, x_2, \dots, x_n)$ is just $(x_n, \dots, x_2, x_1)$. Indeed, $(x_1, \dots, x_n)(x_n, \dots, x_1)$ is such that elements which are not in the cycle are not touched, and the other ones are mapped to the element to their right, and then back to where started.

Definition: Disjoint cycles Let π_1, π_2 be cycles.
They are said to be **disjoint** if their non-trivial orbits do not intersect.

Example For instance, $(1,2)$ and $(4,5)$ are disjoint. However, $(1,2)$ and $(1,3,4)$ are not disjoint since they share a 1 in their orbit.

Proposition: Commutativity Disjoint cycles commute in S_n

Proof Let π_1 and π_2 be disjoint cycles. Also, let $O_1, O_2 \subset \{1, \dots, n\}$ be their non-trivial orbits. We notice that, since π_1 and π_2 are disjoint, $O_1 \cap O_2 = \emptyset$ by definition.
If $x \notin O_1 \cup O_2$, it means that it is in a trivial orbit of both cycles. Thus, $\pi_2 x = x$ and $\pi_1 x$. It indeed yields that:

$$\pi_2\pi_1 x = x = \pi_1\pi_2 x$$

Now, let's suppose that $x \in O_1$, and thus $x \notin O_2$. Let $y = \pi_1 x \in O_1$. We also know that $y \notin O_2$ since the orbits don't intersect. Now, we know that both x and y are in a trivial orbit of π_2, meaning that $\pi_2 x = x$ and $\pi_2 y = y$. Therefore, we do have that:

$$\pi_2\pi_1 x = \pi_2 y = y = \pi_1 x = \pi_1\pi_2 x$$

The case where $x \in O_2$ is completely symmetric.

□

Example For instance:

$$(1,2,3)(5,6) = (5,6)(1,2,3)$$

However, it is possible to show that:

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

Theorem: Existence and unicity of the cycle decomposition

Let $\sigma \in S_n$ be a permutation.
Then, σ can be uniquely written (up to the order of factors) as a product of disjoint cycles. When σ is written in this form, it is said to be in **cycle decomposition**.

Proof idea We know that $\{1, \dots, n\}$ can be expressed uniquely as a union of disjoint orbits. However, each orbit can be written uniquely as a cycle, giving our result.

Personal remark: Inverse

If we have the cycle decomposition of a permutation, we can very easily compute its inverse: we only have to compute the inverse of each of its cycles. Since the inverse of a cycle contains the same elements, this will also produce a product of disjoint cycles.

Example For instance, if $\sigma = (1,2,3)(4,5,6)$, then:

$$\sigma^{-1} = (3,2,1)(6,5,4)$$

Since disjoint cycles commute, we do have that:

$$\begin{aligned}\sigma\sigma^{-1} &= (1,2,3)(4,5,6)(3,2,1)(6,5,4)\\ &= (1,2,3)(4,5,6)(6,5,4)(3,2,1)\\ &= (1,2,3)(3,2,1)\\ &= e\end{aligned}$$

Cycle decomposition algorithm

Let's say that we have an element written as a product of non-disjoint cycles. For instance, in S_6:

$$\sigma = (1,3,5,2)(2,5,6)$$

To find its cycle decomposition, we start from the right (in composition order) with some element, say 1, and see to what it is mapped. This way, we would see that 1 is not changed by the first orbit and then mapped to 3 by the second one. We start again with this 3, and see that it is mapped to 5, which is mapped to 6, which is mapped to 1 (since it is mapped to 2 by the rightmost orbit, and then this 2 is mapped to 1 be the second orbit). However, we hit the same element a second time, which means that we finished our first cycle. Then, we need to do this with all our other elements which appear in σ (we wouldn't need to see to what 4 is mapped, since it does not appear in σ). This way, we find that:

$$\sigma = (1,3,5,6)(2) = (1,3,5,6)$$

removing the trivial orbits.

Observation A product of two elements in S_n is thus computed in $O(n)$. However, we will see that it is much easier to compute a conjugation thanks to the following proposition.

Proposition: Conjugation

Let $\pi, \rho \in S_n$.
The cycle decomposition of $\pi\rho\pi^{-1}$ is obtained from that of ρ, by replacing each integer i in the cycle decomposition of ρ with the integer $\pi(i)$.

Example Let's say that $\rho = (6,2,1)$ and $\pi = (3,2)$. Then:

$$\pi\rho\pi^{-1} = (\pi(6), \pi(2), \pi(1)) = (6,3,1)$$

Similarly:

$$(5,3,1)(2,3,5,6)(5,3,1)^{-1} = (2,1,3,6)$$

This can be verified explicitly, by noticing that $(5,3,1)^{-1} = (1,3,5)$ and throwing the one-element orbit (2).

Proof

We see that:

$$\pi\rho\pi^{-1}(\pi(i)) = \pi(\rho(i))$$

We can now do a *"proof by staring"* (Prof. Lachowska): by looking long enough at our proof, we will see that we are done.

The most important thing is to understand what we are trying to prove. We want to show that the cycles of $\pi\rho\pi^{-1}$ are such that, if $\rho(i)$ follows i in some cycle of ρ, then $\pi(\rho(i))$ will follow $\pi(i)$ in a cycle of $\pi\rho\pi^{-1}$. This is exactly what we have shown here: $\pi\rho\pi^{-1} : \pi(i) \mapsto \pi(\rho(i))$, it maps an element $\pi(i)$ to an element $\pi(\rho(i))$.

□

Definition: Transposition

A cycle composed of two elements is named a **transposition**.

Proposition

Let $(i_1, i_2, \dots, i_k)$ be an arbitrary k-cycle of S_n.
Then, it can be written as a product of $k-1$ transpositions:

$$(i_1, i_2, \dots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_2)$$

Personal remark: Intuition

This result makes sense. Indeed, i_1 would be mapped by the first transposition to i_2. Moreover, i_k is mapped to i_1 by the last transposition. Finally, any other element i_j would be mapped to i_1 by some transposition, and then to i_{j+1} by the transposition right after.

Proof

We make our proof by induction on k.

Let us start with $k = 2$. We know that $(i_1, i_2) = (i_1, i_2)$ can be written as a product of a single transposition; so we indeed get our result.

Now, let us consider $(i_1, \dots, i_k, i_{k+1})$, supposing that our hypothesis is true for k. In particular, our inductive hypothesis implies that the following equality holds:

$$(i_1, i_2, \dots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_2)$$

Now, we notice that:

$$(i_1, i_{k+1})(i_1, i_2, \dots, i_k) = (i_1, i_2, \dots, i_k, i_{k+1})$$

since any element i_j is mapped to i_{j+1} for $j < k$; i_k is mapped to i_{k+1} and i_{k+1} is mapped to i_1.

This indeed allows us to find that:

$$(i_1, \dots, i_{k+1}) = (i_1, i_{k+1})(i_1, \dots, i_k) \overset{\text{IH}}{=} (i_1, i_{k+1})(i_1, i_k) \cdots (i_1, i_2)$$

□

Corollary

S_n is generated by all transpositions $\{(i,j) | 1 \leq i \leq j \leq n\}$.

Proof Let $\sigma \in S_n$. We can write it as a product of disjoint cycles. Then, each cycle can be written as a product of transpositions.

□

Remark Decomposition into a product of transpositions is not unique in general. For instance:

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

However, if we also ask for the cycles to be disjoint, this is unique if it exists (because then it would just be the cycle decomposition of our element).

Theorem Let $\sigma \in S_n$.
Then, it is either a product of an even or of an odd number of transpositions. It cannot be both.

Equivalent proposition Equivalently, a product of an even number of transpositions cannot be equal to a product of an odd number of transpositions.

Monday 30th October 2023 — **Lecture 6 : Enlarge your orbit**

Definition: Inversion Let $a_1, \dots, a_n$ be a permutation of $1, \dots, n$
An inversion is a pair of numbers (a_i, a_j) such that $i < j$ and $a_i > a_j$.

Example For instance, there is no inversion in $1,2,3,4,5,6$. However, in $1,2,4,3,5,6$, there is an inversion: $(4,3)$.

Theorem: Sign invariance Let $\sigma \in S_n$. Also, let k be the number of inversions in $\sigma(1, \dots, n)$ and j be the number of transpositions in an expression of σ.
Then:

$$(-1)^k = (-1)^j$$

We call this value the **sign** of σ, written $\operatorname{sgn}(\sigma)$.

Proof idea Let $\sigma \in S_n$. We notice that this permutations maps $(1, \dots, n)$ to:

$$\sigma(1,2,\dots,n) = (a_1, \dots, a_\alpha, i, b_1, \dots, b_\beta, j, c_1, \dots, c_\gamma)$$

Let us consider the action of the transposition (i,j), to see how it changes the number of inversions in the permutation. We notice that the elements a_t and c_s do not contribute to the change of number of inversions: for instance, if (i, a_t) was an inversion, it will stay that way. Also, if $b_k < i$ and $b_k < j$, then b_k also does not contribute; and similarly if $b_k > i$ and $b_k > j$. Thus, the only interesting case appears when $i < b_k < j$ or $j < b_k < i$. In that case, it will contribute $+2$ or -2 to the number of inversions: (i, b_k) and (b_k, j) will either both become an inversion, or stop being inversions.
The only inversion that will change is the one of (i,j) which will either stop being one or become one. Thus, the action by a transposition changes the number of inversions by 1.

Property The function $\operatorname{sgn} : S_n \mapsto \{1, -1\}$ is a group homomorphism.

Proof Let $\sigma, \tau \in S_n$. We need to show:

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$$

Letting $t(\sigma)$ to count the number of tranpositions in an expression of σ, we have:

$$\text{sgn}(\sigma\tau) = (-1)^{t(\sigma\tau)} = (-1)^{t(\sigma)+t(\tau)} = (-1)^{t(\sigma)}(-1)^{t(\tau)} = \text{sgn}(\sigma)\text{sgn}(\tau)$$

□

Definition: Alternating group

The **alternating group** is defined as $A_n = \ker(\text{sgn}) \lhd S_n$:

$$\ker(\text{sgn}) = \{\sigma \in S_n | \sigma \text{ is a product of an even number of transpositions}\}$$

Remark

Since this is the kernel of a group homomorphism of S_n, it is a normal subgroup of S_n.

Observation

A_n has $|A_n| = \frac{|S_n|}{|\{1,-1\}|} = \frac{n!}{2}$ elements.

Example

For instance, let us consider S_3:

$$S_3 = \{1, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$$

Then:

$$A_3 = \{1, (1,2,3), (1,3,2)\}$$

since $(1,2,3) = (1,3)(1,2)$ and $(1,3,2) = (1,2)(1,3)$.

Proposition

Let $h = \rho_{\ell_1} \cdots \rho_{\ell_r} \in S_n$ be a product of disjoint cycles of lengths $\ell_1, \dots, \ell_r$.
Then:

1. For any $g \in S_n$, the conjugation ghg^{-1} is a product of disjoint cycles of the same lengths.
2. For any product of disjoint cycles of the same lengths $x = \gamma_{\ell_1} \cdots \gamma_{\ell_r} \in S_n$, there exists some $g \in S_n$ such that $x = ghg^{-1}$.

Proof 1

Let $\rho_\ell = (i_1, \dots, i_\ell)$ be a cycle. Then, we know that $\gamma_\ell = g\rho_\ell g^{-1} = (g(i_1), \dots, g(i_\ell))$ is a cycle of the same length.
Now, if $h = \rho_{\ell_1} \cdots \rho_{\ell_r}$, then we can express ghg^{-1} as a product of cycles of the same length:

$$ghg^{-1} = g\rho_{\ell_1}\rho_{\ell_2}\cdots\rho_{\ell_r}g^{-1} = g\rho_{\ell_1}\underbrace{g^{-1}g}_{=1}\rho_{\ell_2}g^{-1}\cdots g\rho_{\ell_r}g^{-1} = \gamma_{\ell_1}\cdots\gamma_{\ell_r}$$

Proof 2

Let $\beta_{\ell_1} \cdots \beta_{\ell_r}$ be a product of disjoint cycles of the same length. We want to find a t such that $t\rho_{\ell_1} \cdots \rho_{\ell_r} t^{-1} = \beta_{\ell_1} \cdots \beta_{\ell_r}$. We can just pick t so that it sends each number in each of the disjoint cycles $\rho_{\ell_1}, \dots, \rho_{\ell_r}$ to the corresponding element of the disjoint cycles $\beta_{\ell_1}, \dots, \beta_{\ell_r}$.
For instance, let us consider a t which would map $(1,2)(3,6,7) \mapsto (4,3)(1,5,6)$. The goal is thus to map $1 \to 4$, $2 \to 3$, $3 \to 1$, $6 \to 5$, $7 \to 6$. We can thus take:

$$t = (1,4,2,3)(6,5,7)$$

also mapping $4 \mapsto 2$ and $5 \mapsto 7$.

□

Definition: Conjugacy class

Let G be a finite group and let $h \in G$.
The **conjugacy class** of h in G, written C_h, is the set of all elements conjugated to h:

$$C_h = \left\{ghg^{-1} | g \in S_n\right\}$$

Observation We proved that all elements of the of the same conjugacy class in S_n have cycles of the same length; meaning that two classes cannot intersect.

Remark Let G be an Abelian group. Then:

$$C_h = \left\{ghg^{-1}\right\}_{g\in G} = \left\{ghg^{-1}\right\}_{g\in G} = \{h\}$$

Thus, $|C_h| = 1$ for any $h \in G$.

Definition: Partition of an integer Let $n \in \mathbb{N}^*$.
The partitions of n is the set of $(i_1, \ldots, i_k)$ such that $i_1 + \ldots + i_k = n$, $i_1 \geq i_2 \geq \ldots \geq i_k \geq 1$ and $k \in \mathbb{N}^*$.

Example For instance, the partitions of 4 are:

$$\{(4), (3,1), (2,2), (2,1,1), (1,1,1,1)\}$$

Observation The conjugacy classes of S_n are in bijection with the partitions of n: we can interpret the $(i_1, \ldots, i_k)$ as the lengths of the cycles in the disjoint cycle decomposition.

Example Let $G = S_4$. We want to find its conjugacy classes.
We have one conjugacy class per partition of 4, meaning that they are in bijection with:

$$\{\{4\}, \{3,1\}, \{2,2\}, \{2,1,1\}, \{1,1,1,1\}\}$$

Then, $\{4\}$ represents the set of 4-cycles:

$$(1,2,3,4), \quad (3,1,2,4), \quad , \ldots$$

$\{3,1\}$ represents the set of 3-cycles:

$$(1,2,3), \quad (2,3,4), \quad \ldots$$

$\{2,2\}$ represents the set of products of 2 disjoint 2-cycles:

$$(1,2)(3,4), \quad (1,3)(2,4), \quad \ldots$$

$\{2,1,1\}$ represents the set of 2-cycles:

$$(1,2), \quad (3,1), \ldots$$

$\{1,1,1,1\}$ finally represents the trivial element, 1.
We can do combinatorics to verify that we indeed get the correct number of elements.

3.8 Action of a finite group on a set by permutation

Definition: Action of a group Let G be a finite group and E be a finite set.
We say that G **acts** on E by permutation if, for any $x \in E$ and $g \in G$, we can define an element $g \cdot x$ such that:

1. $gx \in E$ for any $x \in E$ and $g \in G$
2. $1 \cdot x = x$ for any $x \in E$
3. $(g_1 g_2)x = g_1(g_2 x)$ for any $x \in E$, $g_1, g_2 \in G$.

Definition: Orbit Let G be a finite group and E be a finite set.
The **orbit** of $x \in E$ under the action of G is the subset of E given by:

$$\mathrm{Orb}_x = \{gx | g \in G\}$$

Property

Let G be a finite group, E be a finite set and $x, y \in E$.
Then:

$$\text{Orb}_x = \text{Orb}_y \quad \text{or} \quad \text{Orb}_x \cap \text{Orb}_y = \emptyset$$

Implication

Since every element of E belongs to some orbit, it means that we can partition our set E using orbits. In fact it is possible to show that this creates an equivalence relation.
We thus define $\{x_1, \dots, x_r\}$ to be **a complete set of representatives of orbits** if it such that:

1. $\text{Orb}_{x_i} \cap \text{Orb}_{x_j} = \emptyset$ for any $x_i, x_j \in \{x_1, \dots, x_r\}$ such that $x_i \neq x_j$.
2. $E = \bigcup_{i=1}^{r} \text{Orb}_{x_i}$.

Definition: Group acting on itself by conjugation

Let G be a finite group.
We say that it **acts on itself by conjugation** when it acts on the set G using the following action on a $h \in G$:

$$ghg^{-1} \in G$$

Observation

We notice that, in that case, the orbit of some $h \in G$ is the conjugacy class of h in G:

$$\text{Orb}_h = C_h$$

Corollary

Let G be a finite group.
Then, G can be written as a disjoint union of conjugacy classes:

$$G = \bigcup_{i=1}^{r} C_{h_i}$$

where $C_{h_i} \cap C_{h_j} = \emptyset$ for $h_i \neq h_j$.

Proof

Let us consider G acting on itself by conjugation. We know that, in that case, $\text{Orb}_h = C_h$. By our previous property, we know that G can be written as a disjoint union of orbits, giving us our result immediately.

□

Definition: Stabiliser

Let G be a finite group acting on a finite set E, and let $x \in E$.
The **stabiliser** of x is:

$$\text{Stab}_x = \{g \in G | gx = x\}$$

Definition: Centraliser

Let G be a finite group and $h \in G$.
The **centraliser** of h in G, written G_h, is Stab_h with respect to G acting on itself by conjugation:

$$G_{x_i} = \left\{g \in G | gx_i g^{-1} = x_i\right\}$$

Property

Let G be a finite group acting on a finite set E, and let $x \in E$.
Then, $\text{Stab}_x \subset G$ is a subgroup.

Proof

- By definition of a group acting on a set, we know that $1 \cdot x = x$ for all $x \in E$, so $1 \in \text{Stab}_x$.
- Let's suppose that $g_1, g_2 \in \text{Stab}_x$, meaning that $g_1 x = x$ and $g_2 x = x$. Then:

  $$g_1 g_2 x = g_1 x = x$$

  This indeed shows that $g_1 g_2 \in \text{Stab}_x$.

- Let's suppose that $g \in \text{Stab}_x$, meaning that $gx = x$. Then, by the properties of groups acting on sets:

$$x = (g^{-1}g)x = g^{-1} \underbrace{(gx)}_{g \in \text{Stab}_x} = g^{-1}x$$

This indeed shows that $g^{-1} \in \text{Stab}_x$.

□

Orbit-Stabiliser theorem

Let G be a finite group acting on a finite set E, and let $x \in E$.
Then, the number of elements in the orbit of x is equal to the index of Stab_x in G, i.e.:

$$|\text{Orb}_x| = [G : \text{Stab}_x]$$

Proof

Let $H = \text{Stab}_x \subset G$, to simplify the notation.
We know that $[G : \text{Stab}_x] = [G : H]$ is equal to the number of left H-cosets in G. To show that there are as many left H-cosets as there are elements in Orb_x, we can make a bijection between the set of left H-cosets and Orb_x. Thus, let us consider the following function:

$$\begin{aligned} \mu : \{gH\}_{g \in G} &\longmapsto \text{Orb}_x \\ gH &\longmapsto gx \end{aligned}$$

We notice that μ is surjective: any $gx \in \text{Orb}_x$ can be constructed. Indeed, considering an arbitrary $gx \in \text{Orb}_x$, we know that $g \in gH$ and thus $\mu(gH) = gx$.
Moreover, μ is injective. Indeed, let's suppose that $\mu(gH) = \mu(fH)$ (we want to show that $gH = fH$). However, by definition of μ, this means that:

$$gx = fx \implies f^{-1}gx = x \implies f^{-1}g \in \text{Stab}_x = H$$

We can thus consider the left coset of H with respect to $f^{-1}g$ which, by definition, is a subset of H:

$$f^{-1}gH \subset H \implies gH \subset fH$$

using properties of left-cosets.
However, we can do the exact same reasoning but starting with $gx = fx \implies g^{-1}fx = x$, giving us that $fH \subset gH$. This indeed means that $fH = gH$ and thus that μ is injective.
We have shown that μ is bijective, and thus that:

$$|\text{Orb}_x| = \left|\{gH\}_{g \in G}\right| = [G : \text{Stab}_x]$$

□

Example

Let G be the group of rotational symmetries of a cube. We want to find $|G|$.
We notice that G acts on the set of faces by permutation, so E is the set of faces. Let $x \in E$ be an arbitrary face. Then, $\text{Stab}_x = \{1, r, r^2, r^3\}$ where r is the rotation of x by 90°: rotating along the axis which is normal to the face x does not move this face, and rotating any other axis would move it. Since we can move x to any other face, $\text{Orb}_x = E$, and thus:

$$|\text{Orb}_x| = 6$$

By the orbit-stabiliser theorem, we finally get that:

$$|\mathrm{Orb}_x| = \frac{|G|}{|\mathrm{Stab}_x|} \implies |G| = |\mathrm{Orb}_x||\mathrm{Stab}_x| = 6 \cdot 4 = 24$$

Definition: Center

Let G be a group.
The **center** of G is the set of all elements that commute with any $g \in G$:

$$Z(G) = \{x \in G | xg = gx, \forall g \in G\} = \left\{x \in G | gxg^{-1} = x, \forall g \in G\right\}$$

Remark We notice that $Z(G)$ is also the set of 1-element conjugacy classes in G.

Theorem: Class equation of a group

Let G be a finite group.
Then:

$$|G| = |Z(G)| + \sum_{i=1}^{r} |C_{x_i}|$$

where the C_{x_i} are the non-trivial conjugacy classes, i.e. the conjugacy classes with more than one element.
Equivalently:

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : G_{x_i}]$$

where the G_{x_i} are the non-trivial centralisers.

Proof We know we can write G as a disjoint union of its conjugacy classes:

$$G = \bigcup_{i=1}^{m} C_{x_i}$$

Then, we can write:

$$|G| = \sum_{i=1}^{m} |C_{x_i}| = \sum_{i=1}^{t} \underbrace{|C_{x_i}|}_{\text{one element}} + \sum_{i=1}^{r} \underbrace{|C_{x_i}|}_{\text{more than one element}}$$

We recognise the center, telling us that:

$$|G| = |Z(G)| + \sum_{i=1}^{r} |C_{x_i}|$$

The orbit-stabiliser theorem finally tells us that $|C_{x_i}| = [G : G_{x_i}]$, giving us:

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : G_{x_i}]$$

□

Example

Let G be a group of order $|G| = p^n$ for $p \in \mathbb{P}$ prime.
Then, G has a nontivial center.
Indeed, we have that:

$$p^n = |G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$$

We know that $|G_{x_i}| < |G|$ for any i, since $1 \in C_1$ with $|C_1| = 1$, telling us $1 \notin G_{x_i}$.
This shows that:

$$\frac{p^n}{|G_{x_i}|} = \frac{|G|}{|G_{x_i}|} > 1$$

However, since this term is greater than one and only has factors p in its prime decomposition, this means that it is divisible by p. Since all the other terms of the expression are divisible by p, $|Z(G)|$ is also divisible by p.

However, since $1 \in Z(G)$, we know that $|Z(G)| > 0$. This tells us that $|Z(G)|$ is a non-trivial multiple of p, and thus indeed that $|Z(G)| \geq 2$.

Terminology

Let G be a finite group acting on a finite set E, and let $h \in G$ and $x \in E$. Let's sum up our terminology.

In the general case, we have $\mathrm{Orb}_x \subset E$ and $\mathrm{Stab}_x \subset G$.

However, when G acts on itself by conjugation, we have that the orbit is the conjugacy class and the stabiliser is the centraliser:

$$C_h = \mathrm{Orb}_h \subset G, \quad G_h = \mathrm{Stab}_h \subset G$$

Monday 6th November 2023 — **Lecture 7 : A complete description of abelian group (☺)**

3.9 Classification of finite abelian group

Observation

We have only seen the cyclic group as an abelian group. We wonder if there are other abelian groups.

Cauchy's theorem

Let G be a finite group, and p be a prime number such that $p \mid |G|$.

Then, G has an element of order p.

Proof idea 1

Let's first consider abelian groups G.

We suppose towards contradiction that the proposition is not true, and we thus let G be the smallest counter-example. Let $g \in G$ be an arbitrary non-trivial element. Then, the order of g is not divisible by p since, otherwise, $g^{kp} = 1$ and thus g^k would have an order p.

We know that $|\langle g \rangle| = \mathrm{order}(g)$. Moreover, since G is abelian and $\langle g \rangle \subset G$ is a subgroup, we know that $\langle g \rangle \lhd G$ is a normal subgroup. We can thus consider $G/\langle G \rangle$. We know that p divides $|G/\langle g \rangle| = \frac{|G|}{|\langle g \rangle|} < |G|$.

Now, since G was the smallest counter-example to our proposition, this implies that there exists some $h\langle g \rangle \in G/\langle g \rangle$ such that the order of $h\langle g \rangle$ in $G/\langle g \rangle$ is p. By definition of the quotient group and of the order, this means that $h^p\langle g \rangle = \langle g \rangle$, and thus $h^p \in \langle g \rangle$.

This implies that there exists a s such that $h^p = g^s$. However, for $k = \mathrm{order}(g)$, this yields:

$$h^p = g^s \implies (h^p)^k = (g^s)^k \iff \left(h^k\right)^p = \left(g^k\right)^p \iff \left(h^k\right)^p = 1$$

This tells us that the order of h^k is p.

Proof idea 2

The case for non-abelian groups G will be done in the seventh exercise series.

Definition: Proper subgroups

Let G be a group, and $H \subset G$ be a subgroup.

H is said to be **proper** if $H \neq G$.

Definition: Trivial subgroups

Let G be a group.

The subgroup $H = \{1\} \subset G$ is named the **trivial** subgroup of G.

Definition: Simple group

Let G be a group.

G is said to be **simple**, if none of its proper non-trivial subgroups are normal.

Corollary If G is a simple finite abelian group, then $G \simeq C_p$ for some prime p, where C_p is the cyclic group of order p.

Intuition Since all subgroups of an abelian group are normal, an abelian group is simple if it has no non-trivial subgroup. All subgroups of C_p are non-proper or trivial.

Proof We can write $|G|$ as its prime factorisation, $|G| = p_1^{n_1} \cdots p_k^{n_k}$. By Cauchy's theorem, there exists an element of order p_1 in G, $g \in G$. However, since G is abelian, $\langle g \rangle \subset G$ is normal. Since moreover $|\langle g \rangle| = p_1$, it is nontrivial. It is finally proper if and only if $|G| > |\langle g \rangle| = p_1$.
For G to be simple, $\langle g \rangle$ must not be proper; and G thus has to be of order p_1, telling us $G = \langle g \rangle$, which is indeed homeomorphic to C_{p_1}.

□

Definition: Direct product of groups Let G, H be groups.
The **direct product** $G \times H$ is the set $G \times H = \{(g,h) | g \in G, h \in H\}$, where multiplication is:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

Observation We notice that this is indeed a group, of neutral element $(1_G, 1_H)$ and inverse $(g,h)^{-1} = \left(g^{-1}, h^{-1}\right)$.
Moreover, by properties of the Cartesian product:

$$|G \times H| = |G| \cdot |H|$$

Example Let us consider $C_2 = \left\langle a \middle| a^2 = 1 \right\rangle, C_3 = \left\langle b \middle| b^3 = 1 \right\rangle$. Then:

$$C_2 \times C_3 = \{(g,h) | g \in C_2, h \in C_3\}$$

We can write all elements:

$$C_2 \times C_3 = \left\{(1,1), (1,b), \left(1, b^2\right), (a,1), (a,b), \left(a, b^2\right)\right\}$$

Now, let $t = (a,b)$. We notice that:

$$t^2 = \left(a^2, b^2\right) = \left(1, b^2\right), \quad t^3 = \left(a, b^3\right) = (a,1), \quad t^4 = (1,b), \quad t^5 = \left(a, b^2\right), \quad t^6 = (1,1)$$

This yields that t has order 6. Since this is a generator, $C_2 \times C_3 \simeq C_6$ is isomorphic to the cyclic group of order 6.

Generalisation We will generalise this right after. However this is not always true. We can for instance consider:

$$C_2 \times C_2 = \{(1,1), (1,b), (a,1), (a,b)\}$$

However, all three non-trivial elements have order 2, showing this group has no generator and thus that there is no element of order 4. This shows that it cannot be isomorphic to C_4 (which has an element of order 4).

Properties Let G, H be groups. Then:

1. $G \times H \simeq H \times G$.
2. $H \subset G \times H$ and $G \subset G \times H$ are subgroups.
3. $G \times H$ is abelian if and only if both G and H are abelian.

Proof 2 We notice that $H \simeq \{(1,h) | h \in H\}$, which is a subgroup of $G \times H$.

Lemma Let $n, m \in \mathbb{N}^*$, $a \in C_n$ and $b \in C_m$ be generators of their respective group.
Then:

$$\text{order}(a, b) = \text{lcm}(n, m)$$

where we note $\text{order}((a, b)) = \text{order}(a, b)$ for the simplicity of the notation as usual with functions of vectors.

Proof Since a and b are generators, we have:

$$\text{order}(a) = n, \quad \text{order}(b) = m$$

Then:

$$(a, b)^s = (a^s, b^s) := (1, 1) \implies n \mid s \text{ and } m \mid s$$

Thus, the order of (a, b), the smallest number that is divisible by both n and m, is $\text{lcm}(n, m)$.

□

Proposition Let $n, m \in \mathbb{N}^*$.
Then:

$$C_n \times C_m = C_{nm} \iff \gcd(n, m) = 1$$

Proof $\implies$ We do this proof by the contrapositive, we thus suppose by hypothesis that $\gcd(n, m) = d > 1$. Let $a \in C_n$ and $b \in C_m$ be generators. We have that, by our lemma:

$$\text{order}(a, b) = \text{lcm}(n, m) = \frac{nm}{\gcd(n, m)} = \frac{nm}{d} < nm$$

Moreover, if we consider arbitrary other elements a^t and b^q:

$$\left(a^t, b^q\right)^{\frac{nm}{d}} = \left(\left(a^{\frac{nm}{d}}\right)^t, \left(b^{\frac{nm}{d}}\right)^q\right) = (1, 1)$$

This tells us that there is no element of order nm in $C_n \times C_m$, showing that $C_n \times C_m$ cannot be cyclic, and thus that $C_n \times C_m \neq C_{nm}$.

Proof $\impliedby$ We suppose by hypothesis that $\gcd(n, m) = 1$. We notice that it implies by our lemma that:

$$\text{order}(a, b) = \text{lcm}(n, m) = \frac{nm}{\gcd(n, m)} = nm$$

However, $|C_n \times C_m| = |C_n||C_m| = nm$, telling us that (a, b) is a generator. Thus, $C_n \times C_m \simeq C_{nm}$ is cyclic.

□

Corollary Let C_n be a cyclic group, and $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorisation of n.
Then:

$$C_n \simeq C_{p_1^k} \times \ldots \times C_{p_r^{k_r}}$$

Proof Let $m = p_2^{k_2} \cdots p_r^{k_r}$. We notice that $\gcd\left(p_1^{k_1}, m\right) = 1$, so, by our proposition:

$$C_n \simeq C_{p_1^{k_1}} \times C_m$$

We can repeat this recursively to get our result.

□

Lemma Let G be a group, and $H \subset G$ and $K \subset G$ be subgroups such that:

1. $H \cap K = \{1\}$
2. For any $h \in H$ and $k \in K$, we have $hk = kh$.
3. $HK = \{hk | h \in H, k \in K\} = G$

Then:

$$G \simeq H \times K$$

Proof We consider the following function $\varphi : H \times K \mapsto G$:

$$\varphi(h, k) = hk$$

We want to show that this is an isomorphism. We first see that this is an homomorphism, using the second hypothesis:

$$\varphi(h_1, k_1)\varphi(h_2, k_2) = h_1k_1 \cdot h_2k_2 = h_1h_2k_1k_2 = \varphi(h_1h_2, k_1k_2)$$

which we recognise to be $\varphi((h_1, k_1) \cdot (h_2, k_2))$.
We now want to show that φ is bijective. It is indeed surjective thanks to the third property. For injectivity, we have that:

$$\varphi(h_1, k_1) = \varphi(h_2, k_2) \implies h_1k_1 = h_2k_2 \implies \underbrace{h_2^{-1}h_1}_{h} = \underbrace{k_2k_1^{-1}}_{k}$$

for some $h \in H$ and $k \in K$.
However, since $H \cap K = \{1\}$, this necessarily means that $h = k = 1$ and thus $h_1 = h_2$ and $k_1 = k_2$, which ends this proof.

□

Theorem of classification of finite abelian groups Let G be a finite abelian group.
Then, G is isomorphic to a direct product of prime power orders, i.e:

$$G \simeq C_{p_1^{n_1}} \times \cdots \times C_{p_m^{n_m}}$$

where $\{p_1, \ldots, p_m\}$ are primes, which are not necessarily distinct but are such that $p_1^{n_1} \cdots p_m^{n_m} = |G|$. Those numbers $(p_1^{n_1}, \ldots, p_m^{n_m})$ are named the **elementary divisors** of G.
This presentation is moreover unique, up to the order of factors.

Example For instance, $C_2 \times C_2 \simeq G$ is not cyclic, but it is a finite abelian group of order 4.

Proof idea Let $G = \langle g_1, \ldots, g_k | R_1, \ldots, R_\ell \rangle$. The j^{th} relation can be expressed as $g_1^{n_{1,i}} \cdots g_k^{n_{k,i}}$. Thus, the numbers $n_{i,j}$ completely represent our relations. This means that we can encode our set of relations as a matrix:

$$\begin{pmatrix} n_{1,1} & \cdots & n_{k,1} \\ \vdots & \ddots & \vdots \\ n^{1,\ell} & \cdots & n_{k,\ell} \end{pmatrix}$$

It is possible to show that we don't change the set of relations when adding an integer multiple of one row to another row, when adding an integer multiple of one column to another column, when swapping columns and when swapping rows. This means that we can use Gaussian elimination to turn our matrix to an equivalent

diagonal matrix

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r \end{pmatrix}$$

where $r = \min(k, \ell)$ and some columns or rows full of zeros were removed.
This allows us to find that $G = \left\langle g_1, \ldots, g_r \middle| g_1^{d_1} = 1, \ldots, g_r^{d_r} = 1 \right\rangle$; and thus that $G_i = \langle g_i \rangle \simeq C_{d_i}$ are cyclic subgroups of G. Now, it is possible to show that all those G_i meet the hypotheses of our lemma:

1. $G_i \cap G_j = \{1\}$ for any $i \neq j$.
2. For any $g_i \in G_i$ and $g_j \in G_j$, we have $g_i g_j = g_j g_i$ (since G is abelian).
3. $G_1 \cdots G_r = G$ by construction.

Therefore, we have that:

$$G \simeq G_1 \times \ldots \times G_r \simeq C_{d_1} \times \ldots \times C_{d_r}$$

Now, taking the prime factor decomposition of $d_i = p_1^{k_1} \cdots p_s^{k_s}$, we know that $C_{d_i} \simeq C_{p_1^{k_1}} \times \ldots \times C_{p_s^{k_s}}$. This finally gives us our result.

Corollary Let G be a finite abelian group, such that $|G| = p^n$ for some prime p.
Then, G is a direct product of cyclic groups:

$$G \simeq C_{p^{i_1}} \times \ldots \times C_{p^{i_k}}$$

where $i_1 + \ldots + i_k = n$.

Remark This means that all possible groups of order p^n are in bijection with the partitions of n.

Example Let us consider all possible abelian groups G of order $|G| = 8 = 2^3$.
We need to find the partitions of 3. They are:

$$(3), \quad (2,1), \quad (1,1,1)$$

Thus, we have three different abelian groups of order 8:

$$C_{2^3} = C_8, \quad C_{2^2} \times C_{2^1} = C_4 \times C_2, \quad C_2 \times C_2 \times C_2$$

There cannot be any other group, and they are pairwise not isomorphic (since, as we have seen, $C_n \times C_m \simeq C_{nm}$ if and only if $\gcd(n, m)$, which is not the case here).

Theorem Let G be a finite abelian group.
Then, G is isomorphic to a direct product of cylic groups:

$$G \simeq C_{d_1} \times \ldots \times C_{d_n}$$

where $d_n \mid d_{n-1} \mid \ldots \mid d_1$ (d_i divides d_{i-1} for all i), and $|G| = d_1 \cdots d_n$. Those numbers $(d_1, \ldots, d_n)$ are moreover called the **invariant factors** of G.
This presentation is unique.

Remark This is another, equivalent, presentation of any abelian group.

Observation An abelian group is uniquely determined by its elementary divisors, or by its invariant factors.

Algorithm 1: Elementary divisors We want to make an algorithm to find all abelian groups of a given order n, through elementary divisors.

The algorithm goes as follows:

1. Decompose $|G| = n$ as its prime factorisation, $n = p_1^{k_1} \cdots p_n^{k_n}$.
2. Find the possible partitions for each power $k_1, \dots, k_n$.
3. For each partition of k_i, there is a unique group of order $p_i^{k_i}$. In other words, if $k_i = a_1 + \ldots + a_j$, then:

$$C_{p_i^{k_i}} \simeq C_{p_i^{a_1}} \times \ldots \times C_{p_i^{a_j}}$$

The possible groups G are the direct products of all possible groups of orders $p_i^{k_i}$.

Algorithm 2: Invariant factors Let us now make an algorithm to find the invariant factors of all abelian groups of order n.

The algorithm goes as follows:

1. Decompose the Abelian groups using elementary divisors.
2. We consider each group separately, say $G = C_{p_1^{a_1}} \times \ldots \times C_{p_k}^{a_k}$.
3. We write the $C_{p_i^{a_i}}$ in a table as follows: $C_{p_i^{a_i}}$ and $C_{p_j^{a_j}}$ are on the same line if and only if $p_i = p_j$, and, groups are written in decreasing order of a_i on any given line. This table representation is unique up to the order of lines.
4. Since the direct product is commutative, we can consider a direct product of the columns independently. Since they have coprime order, it can be simplified to a single cyclic group C_{d_i}. G is finally the direct product of each column.

By construction, we do have $d_n \mid d_{n-1} \mid \ldots \mid d_1$.

Example We want to find all abelian groups of order $|G| = 72 = 2^3 \cdot 3^2$.

We have the following partitions of 3:

$$(3), \quad (2,1), \quad (1,1)$$

We moreover have the following partitions of 2:

$$(2), \quad (1,1)$$

This yields that we can consider the 6 possibilities:

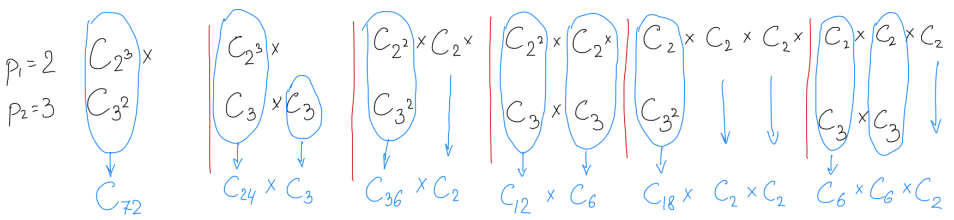
$$C_{2^3} \times C_{3^2}, \quad C_{2^3} \times C_3 \times C_3, \quad C_{2^2} \times C_2 \times C_{3^2}$$

$$C_{2^2} \times C_2 \times C_3 \times C_3, \quad C_2 \times C_2 \times C_2 \times C_{3^2}, \quad C_2 \times C_2 \times C_2 \times C_3 \times C_3$$

In other words, there is a total of 6 non-isomorphic abelian groups of order 72. Their elementary divisors are:

$$\left\{(2^3, 3^2), (2^3, 3, 3), (2^2, 2, 3^2), (2^2, 2, 3, 3), (2, 2, 2, 3^2), (2, 2, 2, 3, 3)\right\}$$

Let's now compute the invariant factors. We represent our 6 possibilities in the table form:



For instance, $C_4 \times C_2 \times C_9 \simeq C_{36} \times C_2$. Indeed, the order does not matter in the direct product, and $C_4 \times C_9 \simeq C_{36}$ since $\gcd(4,9) = 1$. This yields that our 6 possibilities are respectively isomorphic to:

$$C_{72}, \quad C_{24} \times C_3, \quad C_{36} \times C_2$$

$$C_{12} \times C_6, \quad C_{18} \times C_2 \times C_2, \quad C_6 \times C_6 \times C_2$$

Their invariant factors are therefore:

$$\{(72), (24,3), (36,2), (12,6), (18,2,2), (6,6,2)\}$$

Remark This type of questions, finding all elementary divisors and invariant factors of abelian groups of order n, is typically at the exam.

Remark We have classified of all abelian finite groups. Classification of non-abelian finite groups is a lot harder.

They can be split into four categories, including one containing 26 groups, the sporadic groups. They are basically the exception to the three other categories. The biggest in this category, named the monster group, has order:

$$808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000 \approx 8 \cdot 10^{53}$$

Chapter 4

Rings and fields

4.1 Definitions

Definition: Ring A ring is a set A with 2 operations $+$ and $\cdot$, satisfying:

1. $(A, +)$ is an abelian group of neutral element $0 \in A$.
2. $\cdot$ is associative:
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad \forall a, b, c \in A$$
3. $\cdot$ has a neutral element $1 \in A$, such that:
$$1 \cdot a = a \cdot 1 = a, \quad \forall a \in A$$
4. $\cdot$ distributes on $+$ on the left:
$$a \cdot (b + c) = ab + ac, \quad \forall a, b, c \in A$$
And it distributes on the right:
$$(a + b) \cdot c = ac + bc, \quad \forall a, b, c \in A$$

Remark We don't require $\cdot$ to have inverses, nor to be commutative.

Definition: Commutative ring Let $(A, +, \cdot)$ be a ring.
We say that this is a **commutative ring** if the multiplication is commutative, $ab = ba$ for any $a, b \in A$.

Remark We will only consider commutative rings in this course.

Example 1 $(\mathbb{Z}, +, \cdot)$ is a commutative ring.
We notice that some elements don't have a multiplicative inverse. For instance, $2 \in \mathbb{Z}$ but $\frac{1}{2} \notin \mathbb{Z}$.

Notation Let $k \in \mathbb{R}$ and S be some set. We define the following notation:
$$S[k] = \{a + bk \mid a, b \in S\}$$

Observation We notice that, for any $k \in \mathbb{R}$ and set S, then:
$$0, 1 \in S[k]$$
Indeed, we can just set $b = 0$, and $a \in \{0, 1\}$.

Example 2 Let us consider:
$$A = \mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Z}\right\}$$

This is a ring. Indeed, $0, 1 \in A$. Moreover, addition is closed in A:

$$\left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right) = (a + c) + (b + d)\sqrt{2} \in A$$

Any element $a + b\sqrt{2} \in A$ has an additive inverse, $-a - b\sqrt{2} \in A$.
Multiplication is also closed in A:

$$\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = (ac + 2bd) + \sqrt{2}(bc + ad) \in A$$

The other properties come from the fact that we are using the regular additions and multiplications.
However, we notice that there are no multiplicative inverses in A in general:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \underbrace{\frac{a}{a^2 - 2b^2}}_{\notin \mathbb{Z} \text{ in general}} - \underbrace{\frac{b}{a^2 - 2b^2}}_{\notin \mathbb{Z} \text{ in general}} \sqrt{2} \notin A \text{ in general}$$

in general.

Example 3

Let us consider:

$$B = \mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q}\right\}$$

It is possible to show that B is a ring such that every non-zero element has a multiplicative inverse (i.e, a field as we will define later).

Remark

Let $(A, +, \cdot)$ be a commutative ring, and let $a \in A$ (which is not necessarily an integer). We notice that given $n \in \mathbb{Z}$, it makes sense to consider $n \cdot a$.
If $n > 0$, we can write:

$$na = a + a + \ldots + a \in A$$

If $n < 0$, then:

$$na = -(-n)a \in A$$

And, if $n = 0$, then $na = 0$.

Implication

Many formulas thus hold in commutative rings. For instance, we can show that, for any $a, b \in A$:

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Definition: Zero divisor

Let $(A, +, \cdot)$ be a commutative ring, and $a \in A$.
a is a **zero divisor** if there exists a $x \in A \setminus \{0\}$ such that:

$$ax = 0$$

Trivial zero divisor

For instance, $0 \in A$ is always a zero divisor:

$$0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \implies 0 \cdot x = 0$$

This is called the **trivial** zero divisor.

Example 1

The following sets with addition and multiplication are rings without non-trivial zero divisors:

$$\mathbb{Z}, \quad \mathbb{R}, \quad \mathbb{C}$$

Example 2

We want to find a ring with non-trivial zero divisors.
We can consider the set of equivalence classes modulo n:

$$A = \mathbb{Z}/n\mathbb{Z} = \{[0], \ldots, [n-1]\}$$

This is indeed a ring with addition and multiplication modulo n: we do have that $(\mathbb{Z}/n\mathbb{Z}, +) \simeq (C_n, +)$ is an abelian group, $\cdot$ is associative, we have the neutral multiplicative element $[1]$ and multiplication distributes over addition.
Let $a \in A \setminus \{[0]\}$. a is a nontrivial zero divisor if and only if $\gcd(a, n) > 1$.

Proof $\implies$ We do this proof by the contrapositive. We thus suppose by hypothesis that $d = \gcd(a, n) = 1$. We want to show that a is not a zero divisor. By Bézout's theorem, there exists $x, y \in \mathbb{Z}$ such that:

$$ax+ny = 1 \iff ax \equiv 1 \pmod{n} \iff [a][x] = [1] \iff [x] = [a]^{-1}$$

Now, this yields that:

$$[b][a] = [0] \implies [b]\underbrace{[a][x]}_{=[1]} = [0][x] \implies [b] = [0]$$

Proof $\impliedby$ We suppose by hypothesis that $d = \gcd(a, n) > 1$. We indeed have that $[a]$ is a nontrivial zero divisor:

$$[a] \cdot \left[\frac{n}{d}\right] = \left[\frac{an}{d}\right] = \left[\frac{a}{d}\right]\underbrace{[n]}_{=[0]} = [0]$$

Indeed, because $d > 1$, we do have that $\left[\frac{n}{d}\right] \neq [0]$.

Observation An element $[a] \in \mathbb{Z}/n\mathbb{Z}$ is thus either a zero divisor, or invertible.
This tells us that we have $n - \varphi(n)$ zero divisors in $\mathbb{Z}/n\mathbb{Z}$.

Definition: Integral domain Let $(A, +, \cdot)$ be a commutative ring.
If the only zero divisor of A is the trivial zero divisor, then A is called an **integral domain**.

Definition: Field Let $(A, +, \cdot)$ be a commutative ring.
It is called a **field** if all non-zero elements have multiplicative inverses. In other words, for any $a \in A \setminus \{0\}$, there exists a $b \in A$ such that $ab = 1$.

Proposition Let $n \in \mathbb{N}_{\geq 2}$. We have that:

1. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ has non-trivial zero divisors if and only if $n \notin \mathbb{P}$ is not a prime.
2. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a field if and only if $n \in \mathbb{P}$ is a prime.

Proof 1 We see that the following propositions are equivalent:

- There exists a nontrivial zero divisor, $a \in \mathbb{Z}/n\mathbb{Z} \setminus \{[0]\}$.
- There exists some a such that $1 \leq a \leq n-1$ and $\gcd(a, n) > 1$, by our previous example.
- There exists some a such that $1 \leq a \leq n-1$, and n is divisible by a.
- n is not a prime.

Proof 2 We see that the following propositions are equivalent:

- n is a prime.
- For any $[b] \in \mathbb{Z}$, we have $\gcd(b, n) = 1$.
- Any $[b] \in \mathbb{Z}$ has a multiplicative inverse.
- $\mathbb{Z}/n\mathbb{Z}$ is a field, by definition.

□

Example 1 Let us consider:

$$\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$$

Since 5 is prime, this is a field. Thus, all elements different from [0] have a multiplicative inverse:

$$[1]^{-1} = [1], \quad [2]^{-1} = [3], \quad [3]^{-1} = [2], \quad [4]^{-1} = [4]$$

Example 2 Let us consider $\mathbb{Z}/6\mathbb{Z}$. We notice that $[2][3] = [0]$, and thus it is not an integral domain.

Lemma Let $(A, +, \cdot)$ be a commutative ring, and $a \in A$.
If a has a multiplicative inverse, then a is not a zero divisor.

Proof We know by hypothesis that there exists some $a^{-1} \in A$ such that $aa^{-1} = 1$.
Now, let's suppose that $ab = 0$. This yields that:

$$0 = a^{-1}0 = a^{-1}ab = b$$

Thus, a is not a zero-divisor by definition.

□

Converse The converse is wrong. For instance, in $\mathbb{Z}$, 2 is neither a zero-divisor nor inversible.

Proposition Let $(A, +, \cdot)$ be a commutative ring.
If it is a field, then it is an integral domain.

Proof We know that all non-zero element of a field are invertible, so they aren't zero divisors. This shows that A is an integral domain.

Converse The converse is false: $\mathbb{Z}$ is an integral domain, but not a field.
However, as we showed earlier, $A = \mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if it is a field.

Observation We have thus found the following inclusions:

$$\text{Fields} \subset \text{Integral domains} \subset \text{Commutative rings}$$

4.2 Ideals

Definition: Ideal Let A be a commutative ring, and $I \subset A$.
I is called an **ideal** if it has the following properties:

1. $(I, +)$ is a subgroup of $(A, +)$.
2. For any $x \in A$ and $a \in I$, then $xa \in I$.

Proposition: Trivial ideal Let $(A, +, \cdot)$ be a commutative ring.
Then, $\{0\}$ is an ideal, named the **trivial ideal**.

Proposition: Non-proper ideal Let $(A, +, \cdot)$ be a commutative ring.
Then, A is an ideal, named the **non-proper ideal**.

Example Let us consider the ring $A = \mathbb{Z}$, and let $d \in \mathbb{Z}$.
Then, the following is an ideal:

$$d\mathbb{Z} = \{dk \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$$

$(d\mathbb{Z}, +)$ is indeed a subgroup since this is closed under addition, it contains 0, and it contains additive inverses. It moreover also follows the multiplicative property:

$$da \cdot x \in d\mathbb{Z}, \quad \forall x \in \mathbb{Z}$$

Properties Let A be a commutative ring, and let $I, J \subset A$ be ideals.
Then:

1. If $1 \in I$, then $I = A$.
2. $I \cap J$ is an ideal.
3. $I + J \overset{\text{def}}{=} \{x + y \mid x \in I, Y \in J\}$ is an ideal.
4. $I \cdot J \overset{\text{def}}{=} \left\{ \sum_{i=1}^{k} x_i y_i \;\middle|\; x_i \in I, y_i \in J, k \in \mathbb{N} \right\} \subset A$ is an ideal.

Proof 1 Let $a \in A$ be arbitrary. Since $1 \in I$ by hypothesis, we know by the multiplicative property that:

$$1 \cdot a \in I \implies a \in I$$

Thus, $A \subset I$. Since we always have $I \subset A$, this yields that $A = I$.

Proof 2 Let I, J be ideals in A, and let $x, y \in I \cap J$.
We first notice that $(I \cap J, +)$ is indeed an additive subgroup:

1. Since $(I, +)$ and $(J, +)$ are additive subgroups, we know that $x + y \in I$ and $x + y \in J$. This implies by set theory that $x + y \in I \cap J$.
2. By a similar reasoning, we know that $-x \in I$ and $-x \in J$. This indeed means that $-x \in I \cap J$.
3. By the exact same reasoning, we get $0 \in I \cap J$.

We still need to show the multiplicative property. Let $a \in A$. We know that $ax \in I$ and $ax \in J$ since they are ideals. This indeed means that $ax \in I \cap J$.

Proof 3 Let I, J be ideals in A, let $x_1 + x_2, y_1 + y_2 \in I + J$.
This closed under addition:

$$x_1 + x_2 + y_1 + y_2 = \underbrace{x_1 + y_1}_{\in I} + \underbrace{x_2 + y_2}_{\in J}$$

We can check the other properties to show that $I + J$ is an additive subgroup.
Now, let's consider the multiplicative property. Let $a \in A$. Then:

$$a(x + y) = \underbrace{ax}_{\in I} + \underbrace{ay}_{\in J} \in I + J$$

Proof 4 Let I, J be ideals in A.
We directly see that $I \cdot J$ is closed with respect to addition. We can check all other properties to see that this is an additive subgroup.
Now, let's check the multiplicative property. Let $a \in A$. We have:

$$a \sum_{i=1}^{k} x_i y_i = \sum_{i=1}^{k} \underbrace{(a x_i)}_{\in I} y_i = \sum_{i=1}^{k} z_i y_i \in IJ$$

□

Property Let A be a commutative ring, and let $I, J \subset A$ be ideals.
Then, $I \cup J$ is not necessarily an ideal.

Proof We want to show that $I \cup J$ is not an additive subgroup in general. We do this using a counter-example.

Let $I = 3\mathbb{Z} \subset \mathbb{Z}$ and $J = 5\mathbb{Z} \subset \mathbb{Z}$. Then, $I \cup J$ is the multiples of 3 and the ones of 5:

$$I \cup J = \{0, \pm 3, \pm 5, \pm 6, \pm 9, \pm 10, \ldots\}$$

However, $3 + 5 = 8 \notin I \cup J$. It is thus not an additive subgroup, and not an ideal.

Example Let $A = \mathbb{Z}$, $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$. Then, the following are ideals:

1. $I \cap J = \{z \in \mathbb{Z} \mid z = 6n \text{ and } z = 10m; n, m \in \mathbb{Z}\} = \operatorname{lcm}(6, 10)\mathbb{Z} = 30\mathbb{Z}$.
2. $I + J = \{6n + 10m \mid n, m \in \mathbb{Z}\} = \gcd(6, 10)\mathbb{Z} = 2\mathbb{Z}$, by Bézout's theorem.
3. $IJ = \left\{ \sum_{i=1}^{k} 6x_i \cdot 10y_i \;\middle|\; x_i, y_i \in \mathbb{Z} \right\} = \left\{ 60 \sum_{i=1}^{k} x_i y_i \;\middle|\; x_i, y_i \in \mathbb{Z} \right\} = 60\mathbb{Z}$

Generalisation We can generalise our result. Let $n, m \in \mathbb{Z}^*$. The ideals $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$ generate:

1. $I \cap J = \operatorname{lcm}(n, m)\mathbb{Z}$
2. $I + J = \gcd(n, m)\mathbb{Z}$
3. $IJ = nm\mathbb{Z}$

Remark Let $I, J \subset A$ be two ideals. Then:

$$IJ \subset I \cap J \subset I \subset I + J$$

By symmetry, we naturally also have

$$IJ \subset I \cap J \subset J \subset I + J$$

Example Let us consider the set of polynomials in one variable with real coefficients:

$$A = \mathbb{R}[x] = \{a_0 + a_1 x + \ldots + a_n x^n \mid a_0, \ldots, a_n \in \mathbb{R}, n \in \mathbb{N}\}$$

This is indeed a commutative ring: it closed under addition and multiplication, which are commutative and associative, and we have additive inverses.
We can consider the set of polynomials divisible by $(x + 5)$:

$$I = \{(x + 5)f(x) \mid f(x) \in \mathbb{R}[x]\}$$

And, similarly, the set of polynomials divisible by $\big(x^2 + 2\big)$:

$$J = \big\{\big(x^2 + 2\big)f(x) \;\big|\; f(x) \in \mathbb{R}[x]\big\}$$

It is possible to verify that I and J are indeed ideals. Then, the following are ideals:

1. $I \cap J = \big\{(x + 5)\big(x^2 + 2\big)f(x) \;\big|\; f(x) \in \mathbb{R}[x]\big\}$
2. IJ is expressed as:

$$\begin{aligned} IJ &= \left\{ \sum_{i=1}^{k} (x + 5) f_i(x) \big(x^2 + 2\big) g_i(x) \;\middle|\; f_i(x), g_i(x) \in \mathbb{R}[x] \right\} \\ &= \big\{(x + 5)\big(x^2 + 2\big)f(x) \;\big|\; f(x) \in \mathbb{R}[x]\big\} \end{aligned}$$

3. $I + J = \big\{(x + 5)f(x) + \big(x^2 + 2\big)g(x) \;\big|\; f(x), g(x) \in \mathbb{R}[x]\big\}$. It seems like this ideal contains many element, so we want to see if it contains 1, to see if it is not proper. To compensate with the x^2, we can let $f(x)$ be degree one and $g(x)$ be degree zero. We can thus solve the following equation:

$$(x + 5)(ax + b) + \big(x^2 + 2\big)c = 1$$

Doing so, we get that:

$$(x + 5)(x - 5)\frac{-1}{27} - \big(x^2 + 2\big)\left(\frac{-1}{27}\right) = 1 \in \mathbb{R}[x]$$

Thus, $I + J = \mathbb{R}[x]$.

In some form, it would make sense to say that $\gcd(x+5, x^2+2) = 1$. We will dig into this later.

Monday 20th November 2023 — **Lecture 9 : ✨ Prof. de Lataillade ✨**

Definition: Ideal generated by a set

Let $(A, +, \cdot)$ be a commutative ring, and $S \subset A$ be a subset.
The minimal ideal I containing S, written $I = (S)$, is the **ideal generated by the set S**. It can be written as:

$$(S) = \left\{ \sum_i a_i s_i \;\middle|\; a_i \in A, s_i \in S \right\}$$

Remark We can also sometimes write:

$$(S) = \langle S \rangle$$

Definition: Principal ideal

Let $(A, +, \cdot)$ be a commutative ring, and $I \subset A$ be an ideal.
If $I = (x)$ is generated by a single element, it is called **principal**. It can be written as:

$$I = \{xa \mid a \in A\}$$

Example 1

Let $(A, +, \cdot)$ be a commutative ring. We consider the ideals $\{0\} \subset A$ and $A \subset A$. They are both principal:

$$\{0\} = (0), \quad A = (1)$$

Example 2

Let $n \in \mathbb{N}^*$. We consider the ideal $n\mathbb{Z} \subset \mathbb{Z}$. It is principal:

$$n\mathbb{Z} = (n)$$

Theorem

Let $(A, +, \cdot)$ be a commutative ring.
$(A, +, \cdot)$ is a field if and only if 0 and A are the only ideals in A.

Proof $\Longrightarrow$ We suppose by hypothesis that $(A, +, \cdot)$ is a field. We consider an arbitrary non-trivial ideal $I \neq \{0\}$. Our goal is to show that it is non-proper.

We pick some arbitrary element $a \in I \setminus \{0\}$. Since $a \neq 0$ and A is a field, it means that there exists a multiplicative inverse $a^{-1} \in A$. We thus get that $a^{-1}a = 1 \in I$, by the multiplicative property of ideals. However, this implies that $I = A$.

This indeed shows that any non-trivial ideal is non-proper.

Proof $\Longleftarrow$ We suppose by hypothesis that $\{0\}$ and A are the only ideals in A. Let $a \in A \setminus \{0\}$ be arbitrary. We want to show that a has a multiplicative inverse.

We consider the following ideal:

$$I = (a) = \{xa \mid x \in A\}$$

Since $a \neq 0$, we know $I \neq \{0\}$. This means that, by our hypothesis, $I = A$. But then, since $1 \in A$, this means that there exists some $y \in A$ such that $xy = 1$ by definition of I. y is an inverse of x, ending our proof.

□

4.3 Quotient rings over an ideal

Goal We are interested by ideals because they play the role of normal subgroups for fields: we can use them to get a quotient ring.

Definition: Equivalence relation Let E be a *set*, and let $\sim$ be a relation on E.
It is named an **equivalence relation** if it follows the following properties for any $a, b, c \in E$:

1. (Reflexivity) $a \sim a$.
2. (Symmetry) If $a \sim b$, then $b \sim a$.
3. (Transitivity) If $a \sim b$ and $b \sim c$, then $a \sim c$.

Intuition Equivalence relations basically generalise the notion of equality.

Definition: Congruence relation Let $(A, +, \cdot)$ be a *commutative ring*, and let $\sim$ be an equivalence relation on A.
It is named a **congruence** if, for any $a, b, c, d \in A$ such that $a \sim b$ and $c \sim d$, then:

$$a + c \sim b + d \quad \text{and} \quad ac \sim bd$$

Theorem Let $(A, +, \cdot)$ be a commutative ring.
We can construct congruences from ideals, and ideals from congruences:

1. Let $I \subset A$ be an arbitrary ideal. Then, the relation $a \sim b \iff b - a \in I$ is a congruence relation.
2. Let $\sim$ be an arbitrary congruence relation in A. Then, $I = \{a \in A \mid a \sim 0\}$ is an ideal in A.

Proof 1 It is possible to show that $a \sim b$ is indeed an equivalence relation.
Moreover, we can check that this is a congruence. Indeed, if $b - a \in I$ and $d - c \in I$, then, since I is an additive subgroup:

$$I \ni b - a + d - c = (b + d) - (a + c) \implies b + d \sim a + c$$

We can use a similar argument to show that $(b - a)(d - c) \in I$.

Proof 2 Let $a, b \in A$.
Our relation indeed makes an additive subgroup since, supposing that $a \sim 0$ and $b \sim 0$, then $a + b \sim 0$. We also have the additive identity $0 \sim 0$, and the additive inverse $-a \sim 0$.
Moreover, this follows the multiplicative property. Indeed, if $a \sim 0$ and $x \in A$, then:

$$x \sim x \implies ax \sim 0x \implies ax \sim 0$$

□

Example Let us consider the congruences modulo n in $\mathbb{Z}$:

$$a \sim b \iff \exists k \in \mathbb{Z},\ b - a = kn$$

The generated ideal is:

$$I = \{a \in \mathbb{Z} \mid a \sim 0\} = n\mathbb{Z} = (n)$$

Theorem Let A be a commutative ring, and $\sim$ be a congruence relation in A such that $1 \not\sim 0$.
Then, the set of congruence classes is a commutative ring:

$$A/\!\sim \overset{\text{def}}{=} A/\{x \in A \mid x \sim 0\}$$

The elements are congruence classes $\overline{a} = \{x \in A \mid x \sim a\}$, and we define:

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Proof We consider an arbitrary congruence class:

$$\overline{a} = \{x \in A \mid x \sim a\}$$

The operations are well defined since, for $a_1 \sim a_2$ and $b_1 \sim b_2$, we have $a_1 + b_1 \sim a_2 + b_2$ and $a_1 b_1 \sim a_2 b_2$.
We notice that, importantly, $1 \not\sim 0$. This means that $\overline{1} \neq \overline{0}$, which is important since we require for rings that the additive and multiplicative identities are different.

□

Implication An ideal allows to create a congruence relation, which in turns allows to create commutative rings. We can thus write A/I to mean $A/\sim$ where $\sim$ is the congruence relation generated by I.
Ideals allow to create commutative rings, just like normal subgroups allow to create groups.

Example 1 Let us consider $\mathbb{Z}/\sim$ for the following relation:

$$a \sim b \iff \exists k \in \mathbb{Z},\ b - a = kn$$

Then, we have that:

$$\mathbb{Z}/\sim = \mathbb{Z}/n\mathbb{Z} = \{[0], \dots, [n-1]\}$$

Example 2 We consider the ring of polynomials with real coefficients, $A = \mathbb{R}[x]$, and the ideal generated by $x^2 - 4$:

$$I = \langle (x^2 - 4) \rangle$$

We can consider the commutative ring $B = \mathbb{R}[x]/I$. In it:

$$\overline{(x+2)} \cdot \overline{(x+1)} = \overline{x^2 + 3x + 2} = \overline{x^2 + 3x + 2 - (x^2 - 4)} = \overline{3x + 6}$$

$$\overline{x} \cdot \overline{x} = \overline{x^2} = \overline{x^2 - (x^2 - 4)} = \overline{4}$$

We also notice that $x + 2$ and $x - 2$ are non-trivial zero-divisors in B:

$$\overline{(x+2)} \cdot \overline{(x-2)} = \overline{x^2 - 4} = \overline{0}$$

B is thus not an integral domain.
We notice that, in B, we have both any $x \in \mathbb{R}$ and any polynomial of first degree that all yield different congruence classes. Now, any polynomial with higher degree can be turned into a polynomial of first degree or lower by using polynomial division by $x^2 - 4$. Therefore:

$$B = \left\{ \overline{ax + b} \;\middle|\; a, b \in \mathbb{R} \right\}$$

Definition: Principal ideal domain Let $(A, +, \cdot)$ be an integral domain.
If all its ideals are principal, it is called **a principal ideal domain** (PID).

Remark This must not be mistaken with simple groups, which are a similar but different notion for groups.

Summary To sum up, a PID is a commutative ring, without nontrivial zero divisors, and such that every ideal is generated by a single element.

Proposition Let $(A, +, \cdot)$ be a commutative ring.
If it is a field, then it is a PID.

Proof We know a field has only two ideals, which are both principal: $A = (1)$ and $\{0\} = (0)$.

□

Proposition $\mathbb{Z}$ is a PID.

Remark We know that $\mathbb{Z}$ is not a field, showing that PIDs are not necessarily fields. The converse of the previous proposition is thus wrong.

Proof Let I be an arbitrary ideal. We split our proof in two cases.
If $I = \{0\}$, then $I = (0)$. This is indeed principal.
Let's now suppose that $I \neq \{0\}$. Thus, we know that there exists a $a \in I \setminus \{0\}$. We know that this implies that $-a \in I$, and thus that $|a| \in I$. It thus makes sense to consider the smallest positive element of I, which we write $d \in I$.
Let $n \in I$ be arbitrary. By Euclidean division, we know we can write $n = kd + r$, where $0 \leq r \leq d - 1$. By ideal properties, we know that $r = n - kd \in I$ since $n \in I$ and $kd = d + \ldots + d \in I$. However, since d is the smallest positive element of the ideal and $0 \leq r \leq d - 1$, we get that $r = 0$. This tells us that any element n can be written as $n = kd$ for some $k \in \mathbb{Z}$. In other words:

$$I = (d)$$

□

Example Let $a_1, \ldots, a_n \in \mathbb{Z}$. We consider the ideal generated by those elements, $J = (a_1, \ldots, a_n) \subset \mathbb{Z}$. By our proposition, we know that J is principal. In other words, it is generated by a single element.
It is possible to show that $J = (k)$ where $k = \gcd(a_1, \ldots, a_n)$, by using induction on n and Bézout's theorem.

4.4 Ring homomorphisms

Definition: Ring homomorphism Let $(A, +_A, \cdot_A)$ and $(B, +_B, \cdot_B)$ be commutative rings, and $f : A \mapsto B$ be a map. f is said to be a **ring homomorphism** if:

1. $f(a +_A b) = f(a) +_B f(b)$
2. $f(a \cdot_A b) = f(a) \cdot_B f(b)$
3. $f(1_A) = 1_B$

Property We notice that we always have that:

$$f(0) = f(0 + 0) = f(0) + f(0) \implies f(0_A) = 0_B$$

Moreover:

$$f(a) - f(a) = 0 = f(0) = f(a - a) = f(a) + f(-a)$$
$$\implies f(-a) = -f(a)$$

Definition: Ring isomorphism Let A and B be commutative rings, and let $f : A \mapsto B$ be a ring homomorphism. If f is bijective, we call it a **ring isomorphism**. We then say that A and B are **isomorphic**.

Property Let $k \in \mathbb{Z}$, and $f : A \mapsto B$ be a ring homomorphism.
Then:

$$f(k \cdot 1_A) = k \cdot 1_B$$

Proof Let's first suppose that $k = 0$. Then:

$$f(0) = 0$$

Now, let's suppose that $k > 0$:

$$f(k \cdot 1_A) = f(1_A + \ldots + 1_A) = f(1_A) + \ldots + f(1_A) = 1_B + \ldots + 1_B = k1_B$$

Finally, if $k < 0$:

$$f(k \cdot 1_A) = -f(|k| \cdot 1_A) = -|k|1_B = k1_B$$

Definition: Subring Let $(B, +, \cdot)$ be a commutative ring, and $C \subset B$ be a subset.
We say that C is a subring if it is a ring with the same additive identity, multiplicative identity, addition and multiplication (meaning that those operations are closed inside C).

Remark As we will see, this is a very strong definition; there will typically not be many subrings.

Proposition Let $f : A \mapsto B$ be a ring homomorphism.
Then, $\ker(f) \subset A$ is an ideal and $\mathrm{Im}(f) \subset B$ is a subring.

Example Let $C \subset \mathbb{Z}$ be an arbitrary subring.
Then, we need to have:

$$0 \in C, \quad 1 \in C$$

This moreover yields that:

$$-1 \in C$$

Moreover, we need to have:

$$n = 1 + 1 + \ldots + 1 \in C$$

This means that any element $x \in \mathbb{Z}$ is such that $x \in C$, i.e. $\mathbb{Z} \subset C$. Since we always have $C \subset \mathbb{Z}$, we get that the only subring of $\mathbb{Z}$ is $C = \mathbb{Z}$.

Proposition Let $n, m \in \mathbb{N}_{\geq 2}$, and let $f : \mathbb{Z}/n\mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z}$ be a ring homomorphism. Then:

1. $\mathrm{Im}(f) = \mathbb{Z}/m\mathbb{Z}$, which is the unique subring of $\mathbb{Z}/m\mathbb{Z}$.
2. m divides n.
3. This f is unique.

Proof 1 We know that $\mathrm{Im}(f)$ is a subring in $\mathbb{Z}/m\mathbb{Z}$. Moreover, we know that $[1]_m \in \mathrm{Im}(f)$. But then, this means that:

$$[k]_m = [1]_m + \ldots + [1]_m \in \mathrm{Im}(f)$$

Thus, this means that $\mathrm{Im}(f) = \mathbb{Z}/m\mathbb{Z}$, which is the only subring by a similar argument as the previous example.

Proof 2 The existence of this ring homomorphism necessarily implies that:

$$[0]_m = f([0]_n) = f([n]_n) = f(n[1]_n) = n[1]_m = [n]_m$$

This means that m must divide n.

Proof 3 Finally, we know that $f([1]_n) = [1]_m$. Therefore:

$$f([k]_n) = f(k[1]_n) = k[1]_m = [k]_m$$

which is forced. This f is thus indeed unique.

□

Example 1 Let us consider a group homomorphism $f : \mathbb{Z}/10\mathbb{Z} \mapsto \mathbb{Z}/5\mathbb{Z}$.

We necessarily have that:

$$f([0]) = [0], \quad f([1]) = [1], \quad \ldots, \quad f([4]) = [4], \quad f([5]) = [0], \quad \ldots, \quad f([9]) = [4]$$

Then, we have that:

$$\ker(f) = \{[0], [5]\} = ([5]), \quad \mathrm{Im}(f) = \mathbb{Z}/5\mathbb{Z}$$

Example 2 There is no ring homomorphism $f : \mathbb{Z}/6\mathbb{Z} \mapsto \mathbb{Z}/12\mathbb{Z}$.

Example 3 We can construct a unique ring homomorphism $f : \mathbb{Z} \mapsto \mathbb{Z}/6\mathbb{Z}$ such that:

$$\ker(f) = \{0, \pm 6, \pm 12, \ldots\} = (6), \quad \mathrm{Im}(f) = \mathbb{Z}/6\mathbb{Z}$$

4.5 Characteristic of a ring

Proposition Let $(A, +, \cdot)$ be a commutative ring.
There exists a unique ring homomorphism $\tau : \mathbb{Z} \mapsto A$.

Proof We know that we need:

$$\tau(0) = 0, \quad \tau(1) = 1_A$$

Now, we know that, for any $n \in \mathbb{Z}$:

$$\tau(n) = \tau(n \cdot 1) = n1_A \in A$$

Therefore, $\tau(n) = n1_A \in A$ is uniquely determined. We moreover see that this is indeed a ring homomorphism since:

$$\tau(nk) = nk1_A = n1_A \cdot k1_A = \tau(n)\tau(k)$$

□

Remark By construction of τ, the kernel is generated by a single element. However, $\ker(\tau) \neq (1)$, because we know that $\tau(1) = 1 \neq 0$.
This tells us that $\ker(\tau) = (0)$, or $\ker(\tau) = (d)$ for some $d \geq 2$.

Definition: Characteristic of a ring Let A be a commutative ring, and $\tau : \mathbb{Z} \mapsto A$ be the unique homomorphism. Let $d \in \mathbb{N}_0 \setminus \{1\}$ be the number such that $\ker(\tau) = (d)$.
The **characteristic** of A is defined as:

$$c(A) = c_A = d$$

Remark By our remark in the previous paragraph, we always have $d \neq 1$.

Example 1 We want to find the characteristic of $\mathbb{R}$.
The unique homomorphism from $\mathbb{Z}$ is the following:

$$\begin{aligned} \tau : \mathbb{Z} &\longmapsto \mathbb{R} \\ n &\longmapsto n \end{aligned}$$

$\ker(\tau) = \{0\} = (0)$, telling us that $c(\mathbb{R}) = 0$.

Example 2 We want to find the characteristic of $\mathbb{Z}/n\mathbb{Z}$, for $n \geq 2$.
The unique homomorphism from $\mathbb{Z}$ is:

$$\begin{aligned} \tau : \mathbb{Z} &\longmapsto \mathbb{Z}/n\mathbb{Z} \\ k &\longmapsto [k]_n \end{aligned}$$

We notice that $\ker(\tau) = (n)$, and thus $c(\mathbb{Z}/n\mathbb{Z}) = n$.

Definition: Direct product

Let A, B be commutative rings.
The **direct product** of A and B, is a ring over the Cartesian product of A and B:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

The addition and multiplication are done componentwise:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

Finally, the additive identity is $(0_A, 0_B)$ and the multiplicative identity is $(1_A, 1_B)$.

Example

We want to find the characteristic of $A = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
The unique homomorphism from $\mathbb{Z}$ is:

$$\begin{aligned} \tau : \mathbb{Z} &\longmapsto \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ k &\longmapsto ([k]_n, [k]_m) \end{aligned}$$

Thus, the kernel is generated by the smallest k such that:

$$\tau(k) = ([0]_n, [0]_m) \iff k \equiv 0 \pmod{n} \text{ and } k \equiv 0 \pmod{m}$$

Since k is the smallest number that has this property, $k = \operatorname{lcm}(m, n)$. This tells us that $c_A = \operatorname{lcm}(m, n)$.

Generalisation

Let A, B be rings such that $c_A \neq 0$ and $c_B \neq 0$.
Then $c_{A \times B} = \operatorname{lcm}(c_A, c_B)$.

Remark This generalises the previous example.

Example 1

Let $B = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We want to find its characteristic. The unique ring homomorphism from $\mathbb{Z}$ is given by:

$$\tau(k) = (k, [k]_n)$$

The unique case where $\tau(k) = (0, [0]_n)$ is $k = 0$. Therefore, $\ker(\tau) = \{0\} = (0)$, and thus $c_B = 0$.

Example 2

Let $D = \mathbb{Z}/n\mathbb{Z}[x]$ be the ring of polynomials in x with coefficients in $\mathbb{Z}/n\mathbb{Z}$. We want to find its characteristic.
The unique kernel homomorphism is:

$$\tau(k) = [k]_n$$

Therefore, $\ker(\tau) = (n)$, telling us that $c_D = n$.

Proposition

Let A be an integral domain.
Then, $c_A \in \mathbb{P} \cup \{0\}$ is either a prime or zero.

Remark Since fields are integral domains, this property also holds for them.

Proof We do this proof by the contrapositive. We thus suppose that $c_A = mk$ for $m > 1, k > 1$. We notice that $\tau(m) \neq 0$ and $\tau(k) \neq 0$ since, by definition, c_A is the *smallest* positive integer that maps to 0. Then:

$$\underbrace{\tau(m)}_{\neq 0}\underbrace{\tau(k)}_{\neq 0} = \tau(mk) = 0$$

This tells us that $\tau(k), \tau(m) \in A$ are non-trivial zero divisors.

□

Converse

The converse is wrong. Indeed, let $p \in \mathbb{P}$ be a prime number. We know that the characteristic of $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is $c_A = \text{lcm}(p,p) = p$.
However, A has nontrivial zero divisors, such as $(1,0)$ and $(0,1)$:

$$(0,1) \cdot (1,0) = (0,0)$$

Monday 27th November 2023 — **Lecture 10 : Generalising Euclidean division**

4.6 Chinese remainder theorem

Chinese remainder theorem (CRT)

Let A be a commutative ring, and $I, J \subset A$ be ideals such that $I + J = A$.
Then, there exists a ring isomorphism defined by:

$$\begin{aligned} f : A/(I \cap J) &\longmapsto A/I \times A/J \\ f([x]_{I\cap J}) &\longmapsto ([x]_I, [x]_J) \end{aligned}$$

This proposition is known as the **Chinese remainder theorem** (CRT).

Proof

First, we notice that the map $g : [x]_{I\cap J} \mapsto [x]_I$ is a ring homomorphism: it preserves all ring operations. This therefore implies that $f : x \mapsto ([x]_I, [x]_J)$ is also a ring homomorphism.
We now want to show that it is bijective. We begin by showing that f is surjective. Let $a_1, a_2 \in A$. We want to show that there exists some $a \in A$ such that $a \equiv a_1 \pmod I$ and $a \equiv a_2 \pmod J$. Since $I + J = A$, we have that $a_1 - a_2 \in A$ can be written as:

$$a_1 - a_2 = -i + j \iff a_1 + i = a_2 + j \overset{\text{def}}{=} a$$

for some $i \in I$ and $j \in J$. We have indeed got that $a \equiv a_1 \pmod I$ and $a \equiv a_2 \pmod J$, meaning that f is surjective.
We now want to show that f is injective. We keep our $a = a_1 + i = a_2 + j \in A$, and we let $b \in A$ such that $b \equiv a_1 \pmod I$ and $b \equiv a_2 \pmod J$. Then, by definition of quotient rings, there exists $i' \in I$ and $j' \in J$ such that:

$$b = a_1 + i' = a_2 + j' \implies a - b = \underbrace{i - i'}_{\in I} = \underbrace{j - j'}_{\in J} \in I \cap J$$

Therefore, $[a]_{I\cap J} = [b]_{I\cap J}$, meaning that f is indeed injective.
Since f is both surjective and injective, it is bijective. Since it is also a ring homomorphism, it is a ring isomorphism.

□

Corollary: CRT for integers

Let $n, m \in \mathbb{Z}$ be coprime, i.e $\gcd(n,m) = 1$.
Then, for any $a_1, a_2 \in \mathbb{Z}$, there exists some $a \in A$ such that:

$$\begin{cases} a \equiv a_1 \pmod n \\ a \equiv a_2 \pmod m \end{cases}$$

The full set of solutions of this pair of congruences is $\{a + nm\mathbb{Z}\}$.

Proof

We know by hypothesis that $\gcd(n,m) = 1$. This implies by Bézout's theorem that there exists $x, y \in \mathbb{Z}$ such that:

$$xn + ym = 1 \implies n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$$

since an ideal which contains 1 is non-proper.
By the CRT, we know that $\mathbb{Z}/((n)\cap(m)) \simeq \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$. Thus, for any pair $((a_1 \bmod n),(a_2 \bmod m)) \in \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$, there exists a unique $a \in \mathbb{Z}/(n\mathbb{Z}\cap m\mathbb{Z})$ such that:

$$a \equiv a_1 \pmod n, \quad a \equiv a_2 \pmod m$$

Now, an element of $\mathbb{Z}$ is equal to this a if and only if it is of the form:

$$\{a + (n)\cap(m)\} = \{a + nm\mathbb{Z}\}$$

where we used that $\operatorname{lcm}(n,m) = \frac{nm}{\gcd(n,m)} = nm$.

□

Definition: Pairwise coprime

Let $d_1,\dots,d_r \in \mathbb{Z}$.
We say that they are **pairwise coprime**, if $\gcd(d_i,d_j) = 1$ for any $i \neq j$.

Theorem: Generalisation

Let $d_1,\dots,d_r \in \mathbb{Z}$ be pairwise coprime.
Then, for any $a_1,\dots,a_r \in \mathbb{Z}$, there exists a $a \in \mathbb{Z}$ such that:

$$\begin{cases} a \equiv a_1 \pmod{d_1} \\ \vdots \\ a \equiv a_r \pmod{d_r} \end{cases}$$

The full set of solutions is:

$$\{a + (d_1\cdots d_r)\mathbb{Z}\}$$

Proof

This proof can be done by induction. The base case was done by the previous corollary, and, for the inductive step, we suppose that we have a solution a_k to the first k equations, and we construct a a_{k+1} which is a solution to the first $k+1$ equations.

Example

We want to find all solutions $a \in \mathbb{Z}$ of:

$$\begin{cases} a \equiv 2 \pmod 5 \\ a \equiv -1 \pmod{11} \\ a \equiv 3 \pmod 7 \\ a \equiv 0 \pmod 2 \end{cases}$$

Since $\{5,11,7,2\}$ are pairwise coprime, we know that a solution exists by the CRT. We need to find a particular solution. A good way is just guesswork. We notice that $a = 10$ satisfies the last three equations:

$$10 \equiv 3 \pmod 7, \quad 10 \equiv 0 \pmod 2, \quad 10 \equiv -1 \pmod{11}$$

By the CRT, We can therefore turn our system to the following equivalent one:

$$\begin{cases} a \equiv 2 \pmod 5 \\ a \equiv 10 \pmod{154} \end{cases}$$

where $154 = \operatorname{lcm}(7,2,11) = 7\cdot 2\cdot 11$.
Now, to solve this, we can use a direct method. A solution is of the form:

$$a = 154t + 10 = 5s + 2 \iff 154t - 5s = -8$$

for some $t,s \in \mathbb{Z}$.
We can use the extended Euclidean algorithm, or we can notice that 154 is one below a multiple of 5, i.e:

$$154\cdot 1 - 5\cdot 31 = -1 \implies 154\cdot 8 - 5\cdot(31\cdot 8) = -8 \implies 154\cdot 8 - 5\cdot 248 = -8$$

We have thus got $t = 8$ and $s = 248$, telling us:

$$a = 154t + 10 = 154 \cdot 8 + 10 = 1232 + 10 = 1242$$

By the CRT, it tells us that the full set of solutions is:

$$\{1242 + 770\mathbb{Z}\}$$

where $770 = 5 \cdot 11 \cdot 7 \cdot 2$.
In particular, this tells us that the smallest positive solution is $1242 - 770 = 472$.

Algorithmic method

Note that we can solve this kind of problem using a more algorithmic method. We find a solution a_1 such that:

$$\begin{cases} a_1 \equiv 1 \pmod 5 \\ a_1 \equiv 0 \pmod{11} \\ a_1 \equiv 0 \pmod 7 \\ a_1 \equiv 0 \pmod 2 \end{cases} \implies \begin{cases} a_1 \equiv 1 \pmod 5 \\ a_1 \equiv 0 \pmod{11 \cdot 7 \cdot 2} \end{cases}$$

This can be easily done using the extended Euclidean algorithm. Indeed, a_1 must be of the form:

$$a_1 = 5s + 1 = (11 \cdot 7 \cdot 2)t \iff 5s - 154t = 1$$

which can be indeed solved using this algorithm.
Then, we find a solution a_2 such that:

$$\begin{cases} a_2 \equiv 0 \pmod 5 \\ a_2 \equiv 1 \pmod{11} \\ a_2 \equiv 0 \pmod 7 \\ a_2 \equiv 0 \pmod 2 \end{cases}$$

Continuing this way, we then just have:

$$a = 2a_1 - a_2 + 3a_3 + 0a_4$$

Remark

Explaining why a solution exists, describing the set of all solutions and finding the smallest positive solution is a typical exam question.

Definition: Group of units

Let A be a ring.
Its **group of unit**, written A^*, is the subset of invertible elements with respect to multiplication.

Property 1

The group of unit is a multiplicative group.

Property 2

Let A, B be rings. Then:

$$(A \times B)^* \simeq A^* \times B^*$$

Proposition

Let A, B be commutative rings.
If $A \simeq B$ are isomorphic, then $A^* \simeq B^*$ are also isomorphic.

Corollary

Let $n, m \in \mathbb{Z}$ such that $\gcd(n, m) = 1$.
Then, $\varphi(nm) = \varphi(n)\varphi(m)$.

Proof

By the CRT, we know that $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, which means that:

$$(\mathbb{Z}/nm\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

However:

$$\varphi(nm) = \left|(\mathbb{Z}/nm\mathbb{Z})^*\right| = \left|(\mathbb{Z}/n\mathbb{Z})^*\right|\left|(\mathbb{Z}/m\mathbb{Z})^*\right| = \varphi(n)\varphi(m)$$

since isomorphic groups have the same number of elements.

□

Remark Together with the fact that $\varphi(p^a) = p^a - p^{a-1}$ for $p \in \mathbb{P}$ and $a \in \mathbb{N}^*$, it allows us to $\varphi(n)$ for any n for which we can find the prime factorisation.

Proposition: Converse of the CRT for integers Let $n, m \in \mathbb{Z}$.
If $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, then $\gcd(n, m) = 1$.

Remark This means that the converse of the CRT is true for integers. Note that this is not true for any field.

Proof We know by hypothesis that $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Therefore, their chacteristic must be equal:

$$\begin{aligned} nm &= \tau(\mathbb{Z}/nm\mathbb{Z}) \\ &= \tau(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \\ &= \operatorname{lcm}(\tau(\mathbb{Z}/n\mathbb{Z}), \tau(\mathbb{Z}/m\mathbb{Z})) \\ &= \operatorname{lcm}(n, m) \\ &= \frac{nm}{\gcd(n, m)} \end{aligned}$$

However, this implies that $\gcd(n, m) = 1$, finishing our proof.

□

Example We know that, since $\gcd(16, 5) = 1$ and $16 \cdot 5 = 80$, we have by the CRT that:

$$\mathbb{Z}/80\mathbb{Z} \simeq \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

However, even though $8 \cdot 10 = 80$, we have by the converse of the CRT for integers that:

$$\mathbb{Z}/80\mathbb{Z} \not\simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$$

since $\gcd(8, 10) = 2 \neq 1$.

4.7 Polynomial ring

Definition: Polynomial ring Let A be a commutative ring.
The **ring of polynomials** over A is:

$$A[x] = \{a_0 + a_1 x + \ldots + a_n x^n | n \in \mathbb{N}, a_1, \ldots, a_n \in A\}$$

with the usual addition and multiplication of polynomials.

Definition: Degree Let $f(x) \in A[x]$ be a polynomial.
If it is non-zero, the **degree** of $f(x) = a_0 + \ldots + a_k x^k$ is defined as the largest $n \in \mathbb{N}$ such that $a_n \neq 0$. We note $\deg(f) = n$.
We also define the degree of the zero-polynomial to be $\deg(0) = -\infty$.

Example We for instance have:

$$\deg(3) = 0, \quad \deg\left(3x^2 - 5\right) = 2$$

Properties

Let $f, g \in A[x]$ be polynomials. Then:

1. $\deg(f+g) \leq \max(\deg f, \deg g)$
2. If A is an integral domain, $\deg(fg) = \deg f + \deg g$

Proof 1

We know that $\deg(f+g) = \max(\deg f, \deg g)$, unless $\deg f = \deg g$ and $a_n = -b_n$.
For instance, summing two polynomials of degree 2, we can get a polynomial of degree 1:

$$\left(3x^2 + 2x\right) + \left(-3x^2 + 5\right) = 2x + 5$$

Proof 2

We notice that:

$$\begin{aligned} f(x)g(x) &= (a_0 + a_1x + \ldots + a_nx^n)(b_0 + b_1x + \ldots + b_mx^m) \\ &= a_nb_mx^{n+m} + \text{lower degree terms} \end{aligned}$$

Let's suppose that neither f nor g is 0. Since the degree of f is n and the degree of g is m, we know that that $a_n \neq 0$ and $a_m \neq 0$ by definition. Since A is an integral domain, $a_nb_m \neq 0$, and thus $f(x)g(x)$ has degree $n+m$.
Now, if f or g is the zero polynomial, then $fg = 0$. However, then, our property reads:

$$-\infty = -\infty + c$$

for some $c \in \mathbb{N}_0 \cup \{-\infty\}$, which we take as a definition (which makes sense). This justifies the definition $\deg(0) = -\infty$.

□

Proposition

Let A be an integral domain.
Then:

1. $A[x]$ is an integral domain.
2. The units of $A[x]$ are the units of A.

Proof 1

Let's suppose that $f(x)g(x) = 0$. This means that:

$$\deg(fg) = -\infty$$

However, we also know that $\deg(f) + \deg(g) = \deg(fg)$ since A is an integral domain. If both $\deg(f)$ and $\deg(g)$ are finite, then their sum is also finite. This requires that either is $-\infty$, telling us that $f(x) = 0$ or $g(x) = 0$. This implies by definition that $A[x]$ is an integral domain.

Proof 2

Let's suppose that $f(x)g(x) = 1$. This means that:

$$\deg(fg) = 0$$

However, we also know that $\deg(f) + \deg(g) = \deg(fg)$ since A is an integral domain. If any of the terms is $-\infty$, then the sum will also be $-\infty$. If either one is strictly positive, then their sum will also be strictly positive. This therefore means that they are both constant. In other words, $f(x) = a_0$ and $g(x) = b_0$, which are such that $a_0 \cdot b_0 = 1$ in A.

□

Example

For instance, the following rings are integral domains:

$$\mathbb{R}[x], \quad \mathbb{Q}[x], \quad \mathbb{Z}[x]$$

However, $\mathbb{Z}/6\mathbb{Z}[x]$ is not an integral domain. We for instance have that $(2x)(3x) = 0$ where $2x \neq 0$ and $3x \neq 0$.

Theorem: Euclidean division in polynomial fields

Let F be a field, and let $f(x), d(x) \in F[x]$ such that $\deg(d) \geq 1$.
Then, there exists polynomials $q(x), r(x) \in F[x]$ be such that:

$$f(x) = q(x)d(x) + r(x)$$

where $r(x) = 0$ or $\deg(r) < \deg(d)$.

Proof

Let's first suppose that $\deg(f) < \deg(g)$. Then, we can take:

$$f(x) = 0 \cdot d(x) + f(x)$$

Let's now suppose that $\deg(f) \geq \deg(g)$. The idea is that we can use the regular polynomial division algorithm. Let's describe it formally. We can write:

$$f(x) = a_0 + \ldots + a_m x^m$$

$$d(x) = b_0 + \ldots + b_n x^n$$

We now construct the following polynomial:

$$p_1(x) = f(x) - d(x) \cdot \frac{a_m}{b_n} x^{m-n}$$

where $\frac{a_m}{b_n} = a_m b_n^{-1} \in F$ since it is a field.
If $\deg(p_1) < \deg(f)$, we are done. Otherwise, we can can repeat:

$$\begin{aligned} p_2(x) &= p_1(x) - d(x)\frac{a_{m-1}}{b_n} x^{m-n-1} \\ &= f(x) - d(x)\frac{a_m}{b_n} x^{m-n} - d(x)\frac{a_{m-1}}{b_n} x^{m-n-1} \end{aligned}$$

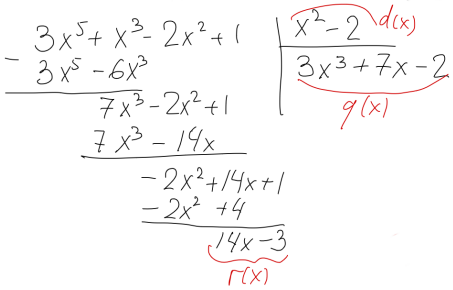
The sequence of degrees is strictly decreasing, so, at some point, the process terminates with a $p(x) = f(x) - d(x)q(x)$ such that:

$$f(x) - d(x)q(x) = r(x)$$

□

Remark

As mentioned above, this is just the regular polynomial division algorithm. For instance, if we have $f(x) = 3x^5 + x^3 - 2x^2 + 1$ and $d(x) = x^2 - 2$, we have:



where, for example, the first term of $q(x)$ was chosen to be $3x^3$ since $3x^3(x^2 - 2) = 3x^5 + \ldots$, which allows to decrease the degree of $f(x)$.

This allows us to write:

$$\begin{aligned} & f(x) = d(x)q(x) + r(x) \\ \iff & 3x^5 + x^3 - 2x^2 + 1 = \big(x^2 - 2\big)\big(3x^3 + 7x - 2\big) + (14x - 3) \end{aligned}$$

4.8 Euclidean domains

Definition: Euclidean domain

Let A be a commutative ring.
It is said to be a **Euclidean domain** if:

1. A is an integral domain.
2. There exists a function $\nu : A \setminus \{0\} \mapsto \mathbb{N}$ such that for any $a, b \in A$ where $b \neq 0$, there exists $q, r \in A$ such that:

$$a = qb + r$$

and either $r = 0$ or $\nu(r) < \nu(b)$.

Intuition This generalises abstractly any space which admits a Euclidean division.

Example We can for instance consider the following Euclidean domain, which is the main one we have been worked with since the beginning of the course:

$$\mathbb{Z}, \quad \nu(n) = |n|$$

It is also possible (though harder than exam material) to show that the following integral domain is a Euclidean domain:

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}, \quad \nu(a + ib) = |a + ib|^2 = a^2 + b^2$$

Proposition

Let A be a field.
Then, A is a Euclidean domain.

Proof For any $a, b \in A$, we can find a $q \in A$ such that:

$$a = qb + 0 = qb$$

We can therefore take ν to be any function.

□

Corollary

Let $\mathbb{F}$ be a field.
Then, $\mathbb{F}[x]$ is a Euclidean domain.

Proof We can just take $\nu = \deg$.
Then, given $f(x), d(x) \in \mathbb{F}[x]$, we know that we can find $q(x), r(x)$ such that

$$f(x) = q(x)d(x) + r(x)$$

where $r(x) = 0$ or $\deg(r) < \deg(d)$.

□

Proposition

Let A be a Euclidean domain.
Then, A is a PID (principal ideal domain).

Proof Let E be a Euclidean domain of function ν, and $I \subset E$ be an ideal.
If $I = \{0\}$, then we directly have $I = (0)$.
Let's now suppose that $I \neq \{0\}$. We can pick a $d \in I \setminus \{0\}$ such that $\nu(d)$ is the minimum on I. Now, let $a \in I$ be arbitrary. This

yields that there exists q, r such that $\nu(r) < \nu(d)$ or $r = 0$, and:

$$a = qd + r \implies r = \underbrace{a}_{\in I} - \underbrace{qd}_{\in I} \in I$$

However, since $r \in I$ and we picked d such that $\nu(d)$ was the minimum on I, we cannot have $\nu(r) < \nu(d)$. This means that $r = 0$, and thus that:

$$a = qd \implies I = (d)$$

Any ideal is principal, showing this is indeed a PID.

□

Remark This for instance implies that, for a field F, $F[x]$ is a PID, i.e. all its ideals are generated by a single element.

Remark We have proven the following inclusions:

$$\text{Fields} \subset \text{Euclidean domains} \subset \text{PID} \subset \text{Integral domain} \subset \text{Commutative rings}$$

We have the following examples:

1. Fields:
$$\mathbb{R}, \quad \mathbb{C}, \quad \mathbb{Z}/p\mathbb{Z}$$
for $p \in \mathbb{P}$ prime.
2. Euclidean domains that are not fields:
$$\mathbb{Z}, \quad \mathbb{R}[x]$$
3. PID that are not Euclidean domain: *"They exist, but don't worry about it."*
4. Integral domains that are not PIDs:
$$\mathbb{R}[x, y]$$
5. Commutative rings that are not integral domains:
$$\mathbb{Z}/n\mathbb{Z}$$
for $n \in \mathbb{N}_{\geq 2} \setminus \mathbb{P}$ composite.

Monday 4th December 2023 — **Lecture 11 : Polynomials don't appear so strong yet**

Definition: Divisibility Let A be a commutative ring, and $a, b \in A$.
We say that a **divides** b, written $a \mid b$, if there exists a $c \in A$ such that:

$$b = ac$$

Definition: GCD Let A be an integral domain, and $a, b \in A$.
We say that d is a **greatest common divisor** of a and b, written $d = \gcd(a, b)$ if $d \mid a$, $d \mid b$ and, for any $c \in A$ such that $c \mid a$ and $c \mid b$, then $c \mid d$.

Remark This is not unique in general.

Definition: LCM Let A be an integral domain, and $a, b \in A$.
We say that ℓ is a **least common multiple** of a and b, written $\ell = \text{lcm}(a, b)$, if $a \mid \ell$, $b \mid \ell$ and for any $m \in A$ such that $a \mid m$ and $b \mid m$, then $\ell \mid m$.

Remark This is not unique in general.

Definition: Associate elements

Let A be an integral domain, and $a, b \in A$.
a and b are said to be **associates** if there exists a unit $u \in A^*$ such that:

$$b = au$$

Or, equivalently, if there exists a unit $v \in A^*$ such that:

$$a = bv$$

Proposition

Let A be an integral domain, and $a, b \in A \setminus \{0\}$ be nonzero elements.

- If d_1, d_2 are $\gcd(a, b)$, then d_1 and d_2 are associates.
- If ℓ_1, ℓ_2 are $\text{lcm}(a, b)$, then ℓ_1 and ℓ_2 are associates.

Proof 1

Since $d_1 \mid a, b$ and d_2 is a gcd, we know by definition that $d_1 \mid d_2$ and thus that $d_1 = xd_2$ for some $x \in A$. Doing the same reasoning, we get that $d_2 = zd_1$ for some $z \in A$. This yields:

$$d_1 = xd_2 = xzd_1 \implies d_1(1 - xz) = 0$$

However, since this is an integral domain, one of the two terms is 0. Since $d_1 \neq 0$ by definition of the gcd, we get:

$$1 - xz = 0 \implies xz = 1$$

showing that both x and z are units. This indeed means that d_1 and d_2 are associates, by definition.

Proof 2

The case for lcms is similar.

□

Proposition

Let A be a PID and $f, g \in A$.
f and g are associates if and only if:

$$(f) = (g)$$

Proof $\implies$

We know by hypothesis that f and g are associates, i.e. that there exists a unit u such that:

$$g = uf$$

This however means that $g \in (f)$ and thus $(g) \subset (f)$.
We can do the exact same reasoning from the fact that $f = u^{-1}g$ to get that $(f) \subset (g)$. This indeed yields that:

$$(f) = (g)$$

Proof $\impliedby$

This case is left as an exercise to the reader.

□

Example 1

Let us consider $A = \mathbb{Z}$. The only units are $\{-1, 1\}$.
We therefore get that $n, m \in \mathbb{Z}$ are associates if and only if $|n| = |m|$. And, we do have that:

$$(m) = (-m)$$

Example 2

Let F be a field, and $A = F[x]$.
The units of A are the non-zero constants since all non-zero elements of a field are invertible, i.e. $A^* = F^* = F \setminus \{0\}$. This means that $f(x)$ and $g(x)$ are associates if and only if there exists a $\alpha \in F^*$ such that $f(x) = \alpha g(x)$. We do also have that:

$$(f(x)) = (\alpha f(x)) \subset F[x]$$

Properties

Let E be a Euclidean domain, and $a, b, c \in E \setminus \{0\}$.
Then:

1. $\gcd(a, b)$ can be found by the Euclidean division algoriithm.
2. $(a) + (b) = (\gcd(a, b))$
3. $(a) \cap (b) = (\mathrm{lcm}(a, b))$
4. If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.
5. If $\gcd(a, b) = 1$, then $\mathrm{lcm}(a, b) = ab$.

Chinese remainder theorem

Let E be a Euclidean domain, and $m_1, \dots, m_r \in E$ such that $\gcd(m_i, m_j) = 1$ for any i, j such that $i \neq j$.
Then, the following function is a ring isomorphism:

$$f : E/(m_1 \cdots m_r) \longmapsto E/(m_1) \times \ldots \times E/(m_r)$$
$$[x]_{(m_1 \cdots m_r)} \longmapsto \Big([x]_{(m_1)}, \dots, [x]_{(m_r)}\Big)$$

Proof idea

We first notice that this is a ring homomorphism by construction, using a similar argument as in the proof of the CRT for two factors.
We now need to prove bijectivity. Let's begin with surjectivity. By the CRT for 2 factors, we know that there exists $a_{12} \in E$ such that:

$$a_{12} \equiv a_1 \pmod{m_1}, \quad a_{12} \equiv a_2 \pmod{m_2}$$

Since $\gcd(m_1, m_2) = 1$ by hypothesis, this means that $(m_1)+(m_2) = E$. We moreover know that $\gcd(m_3, m_1) = \gcd(m_3, m_2) = 1$ by hypothesis. By one of our properties, we know that:

$$\gcd(m_3, m_1 m_2) = 1$$

But then, this means that $(m_3) + (m_1 m_2) = E$. We can thus again use the CRT for 2 factors, to get that there exists $a_{123} \in E$ such that:

$$a_{123} \equiv a_{12} \pmod{m_1 m_2}, \quad a_{123} \equiv a_3 \pmod{m_3}$$

We can continue until we get all congruences, showing surjectivity.
Let's now show injectivity. We thus suppose that, for all i:

$$a \equiv a_i \pmod{m_i}, \quad b \equiv a_i \pmod{m_i}$$

However, this means that $a - b \equiv 0 \pmod{m_i}$ for any i. This implies by definition of quotient rings that $a - b \in \bigcap_{i=1}^{r}(m_i) = (\mathrm{lcm}(m_1, \dots, m_r))$. However, since $\gcd(m_i, m_j) = 1$, we get that:

$$a - b \in (m_1 \cdots m_r)$$

Now, by definition of quotient rings, we indeed get that:

$$a \equiv b \pmod{m_1 \cdots m_r}$$

showing injectivity in $E/(m_1 \cdots m_r)$.
Since this map is both injective and surjective, it is bijective. Since it is moreover a ring homomorphism, it is a ring isomorphism.

Corollary

Let F be a field, and $\{f_1(x), \dots, f_r(x)\} \subset F[x]$ be polynomials satisfying $\gcd(f_i(x), f_j(x)) = 1$ for any $i \neq j$.
Then:

$$F[x]/(f_1(x) \cdots f_r(x)) \simeq F[x]/(f_1(x)) \times \ldots \times F[x]/(f_r(x))$$

Observation We know that $\gcd(f(x), g(x))$ is not unique. However, since any gcd are associates, they are determined up to a nonzero constant in F. There therefore exists a unique gcd with leading coefficient equal to 1. This yields the following definition.

Definition: Monic Let F be a field, and $f(x) \in F[x]$.
f is said to be **monic** if its leading coefficient is 1.

Remark By our observation, for any nonzero $f(x), g(x)$, there exists a unique monic $\gcd(f(x), g(x))$.

Example We want to find the monic $\gcd(f(x), g(x))$ where:

$$f(x) = x^4 - x^3 + 3x^2 + 2x - 5, \quad g(x) = x^2 - 2x + 1$$

As usual, we use the Euclidean algorithm. Doing regular polynomial division, we get that:

$$x^4 - x^3 + 3x^2 + 2x - 5 = \big(x^2 - 2x + 1\big)\big(x^2 + x + 4\big) + \underbrace{9x - 9}_{=r_1}$$

Then:

$$x^2 - 2x + 1 = (9x - 9)\left(\frac{1}{9}x - \frac{1}{9}\right) + \underbrace{0}_{=r_2}$$

Since we have found a rest of 0, we finished the algorithm. This means that:

$$r_1 = 9x - 9 = \gcd(f(x), g(x))$$

We however want a monic gcd, so we divide by the leading coefficient, giving that the monic gcd of $f(x)$ and $g(x)$ is:

$$\frac{1}{9}(9x + 9) = x + 1$$

Remark This is a typical exam question.

4.9 Solving systems of congruences of polynomials

Goal We want to find a way to use the CRT to solve systems of congruences of polynomials.

Example Let $\mathbb{F}_3 = \{0, 1, 2\} = \mathbb{Z}/3\mathbb{Z}$ be a field. We consider $\mathbb{F}_3[x]$. We want to find all solutions of the following system of congruences:

$$\begin{cases} f(x) \equiv x + 1 \pmod{x^2 + 1} \\ f(x) \equiv 1 \pmod{x} \\ f(x) \equiv -x \pmod{x^2 - 1} \end{cases}$$

We first notice that $\big(x^2 + 1\big), x$ and $\big(x^2 - 1\big)$ are pariwise coprime. Indeed, we know that $\gcd(g_1(x), g_2(x)) = 1$ if and only if there exists $a(x), b(x) \in \mathbb{F}_3[x]$ such that $a(x)g_1(x) + b(x)g_2(x) = 1$. With a bit of trial and error, we indeed find that:

$$\big(x^2 + 1\big) \cdot 1 + (x) \cdot 2x = 1$$

$$\big(x^2 + 1\big) \cdot 2 + \big(x^2 - 1\big) \cdot 1 = 1$$

$$\big(x^2 - 1\big) \cdot 2 + (x) \cdot x = 1$$

Since they are pairwise coprime, the CRT tells us that there exists solutions of the form:

$$a(x) + k\big(x^2 + 1\big)\big(x^2 - 1\big)x, \quad k \in \mathbb{F}_3$$

We now need to find such a $a(x)$. We start with 2 congruences:

$$\begin{cases} f(x) \equiv x+1 \pmod{x^2+1} \\ f(x) \equiv 1 \pmod{x} \end{cases}$$

We therefore try to find $h(x), g(x)$ such that:

$$f(x) = \big(x^2+1\big)h(x) + (x+1) = xg(x) + 1 \iff \big(x^2+1\big)h(x) - xg(x) = -x$$

However, we have already found that:

$$\big(x^2+1\big) \cdot 1 + (x) \cdot 2x = 1$$

Therefore, multiplying both sides by $-x$:

$$\big(x^2+1\big) \underbrace{(-x)}_{h(x)} + x \underbrace{\big(-2x^2\big)}_{-g(x)} = -x$$

From this, we can deduce that, modulo $x\big(x^2+1\big)$:

$$f(x) = \big(x^2+1\big)h(x) + (x+1) = \big(x^2+1\big)(-x) + x + 1 = -x^3 + 1$$

We can simplify it to get that:

$$f(x) \equiv x+1 \pmod{x^3+x}$$

Now, taking back the third equation, we have the following system of equations:

$$\begin{cases} f(x) \equiv x+1 \pmod{x^3+x} \\ f(x) \equiv -x \pmod{x^2-1} \end{cases}$$

We can repeat the exact same method to solve this, which gives:

$$f(x) \equiv x^4 + 2x^3 + x^2 + 1 \pmod{x^5 - x}$$

General method for two equations

Let's generalise the previous example. We suppose that we have the following system of equations:

$$\begin{cases} f(x) \equiv h_1(x) \pmod{g_1(x)} \\ f(x) \equiv h_2(x) \pmod{g_2(x)} \end{cases}$$

where $\gcd(g_1, g_2) = 1$.
Then, we know that there exists $t_1(x), t_2(x) \in F[x]$ such that:

$$t_1(x)g_1(x) + t_2(x)g_2(x) = 1$$

which we can find using the Euclidean algorithm backwards, just like integers; or by guessing, which is typically faster.
But then, the following is a solution:

$$f(x) = h_1(x)t_2(x)g_2(x) + h_2(x)t_1(x)g_1(x)$$

Indeed, using the fact that $t_1(x)g_1(x) + t_2(x)g_2(x) = 1$:

$$f(x) = h_1(x)(1 - t_1(x)g_1(x)) + h_2(x)t_2(x)g_2(x) \implies f(x) \equiv h_1(x) \pmod{g_1(x)}$$

$$f(x) = h_1(x)t_2(x)g_2(x) + h_2(x)(1 - t_2(x)g_2(x)) \implies f(x) \equiv h_2(x) \pmod{g_2(x)}$$

General method

Let's now suppose that we have a general system of equations $f(x) \equiv h_i(x) \pmod{g_i(x)}$ for pairwise coprime $g_i(x)$.

We define $G(x) = g_1(x) \cdots g_r(x)$ and $G_i(x) = \frac{G(x)}{g_i(x)}$. By hypothesis, we have that $\gcd(G_i, g_i) = 1$ for any i. This means that, for all i, there exists some $t_i(x), s_i(x)$ such that:

$$t_i(x)G_i(x) + s_i(x)g_i(x) = 1$$

which we can again find using the Euclidean algorithm, or by guesssing.
Our answer can then be expressed as:

$$f(x) = \sum_{i=1}^{r} h_i(x)G_i(x)t_i(x)$$

Example

Let us consider $r = 3$. Then:

$$\begin{aligned} f(x) &= (h_1G_1t_1 + h_2G_2t_2 + h_3G_3t_3)(x) \\ &= (h_1(1 - g_1s_1) + h_2G_2t_2 + h_3G_3t_3)(x) \end{aligned}$$

which indeed implies that:

$$f(x) \equiv h_1(x) \pmod{g_1(x)}$$

This is similar for $h_2(x)$ and $h_3(x)$.

Example

We consider again the following system of equations in $\mathbb{F}_3[x]$:

$$\begin{cases} f(x) \equiv x + 1 \pmod{x^2 + 1} \\ f(x) \equiv 1 \pmod{x} \\ f(x) \equiv -x \pmod{x^2 - 1} \end{cases}$$

By construction we have:

$$G_1(x) = x\big(x^2 - 1\big) = x^3 - x$$

$$G_2(x) = \big(x^2 + 1\big)\big(x^2 - 1\big) = x^4 - 1$$

$$G_3(x) = \big(x^2 + 1\big)x = x^3 + x$$

By guessing, we find that:

$$\begin{aligned} \big(x^2 + 1\big)\big(x^2 + 1\big) \; -x\big(x^3 - x\big) &= 1 \\ x^3 \cdot x \; -1\big(x^4 - 1\big) &= 1 \\ \big(x^2 - 1\big)\big(x^2 - 1\big) \; \underbrace{-x\big(x^3 + x\big)}_{t_i(x)G_i(x)} &= 1 \end{aligned}$$

Now, we know that the solution is:

$$\begin{aligned} f(x) &= \sum_{i=1}^{3} h_i(x)t_i(x)G_i(x) \\ &= (x + 1)(-x)\big(x^3 - x\big) + 1(-1)\big(x^4 - 1\big) + (-x)(-x)\big(x^3 + x\big) \\ &= x^4 + 2x^3 + x^2 + 1 \end{aligned}$$

This is a solution modulo $x\big(x^2 - 1\big)\big(x^2 + 1\big) = x^5 - x$, meaning that the set of all solutions is:

$$\Big\{x^4 + 2x^3 + x^2 + 1 + \big(x^5 - x\big)k \;\Big|\; k \in \mathbb{F}_3[x]\Big\}$$

We can verify this using polynomial division.

4.10 Irreducible elements and maximal ideals

Definition: Irreducible element

Let A be a commutative ring, and $c \in A$.
c is **irreducible** if it has all the following properties:

1. $c \neq 0$.
2. c is not a unit.
3. For any a, b such that $ab = c$, then either a or b is a unit.

Personal remark

This can be understood as some kind of generalisation of prime numbers. This is not completely true since "prime elements" are defined differently and are a different concept. However, irreducible elements share some properties with prime numbers that allow us to make a link between them for intuition.

Example

Let us consider $A = \mathbb{Z}/9\mathbb{Z}$. We know that the units are:

$$A^* = \{[1], [2], [4], [5], [7], [8]\}$$

The candidates for being irreducible elements are [3] and [6]. We consider the products of non-units non-zero elements:

$$[3][3] = [0], \quad [3][6] = [0], \quad [6][6] = [0]$$

This means that, if $ab = [3]$, then either a or b is a unit; it is impossible that they are both non-unit; and similarly for [6]. This means that both [3] and [6] are irreducible.

Definition: Maximal ideal

Let A be a commutative ring, and $I \subset A$ be an ideal.
I is said to be **maximal** if $I \neq A$ and there is no ideal $J \subset A$ such that:

$$I \subsetneq J \subsetneq A$$

Theorem

Let A be a PID, and $p \in A$.
p is irreducible if and only if $p \neq 0$ and (p) is maximal.

Proof $\implies$

Let p be an irreducible element. We suppose towards contradiction that there exists an ideal $J \subset A$ such that:

$$(p) \subsetneq J \subsetneq A$$

Since A is a PID, we know there exists a d such that $J = (d)$. Since $(p) \subset J$, we know $p \in (d)$ and thus $p = dt$ for some $t \in A$. However, since p is irreducible, we have two cases. If d is a unit, this yields that d and 1 are associates and thus $(d) = (1) = A$. If however t is a unit, we get that d and p are associates and thus that $(d) = (p)$. In both case, it contradicts they hypothesis that $(p) \subsetneq J \subsetneq A$.

Proof $\impliedby$

We do this proof by the contrapositive. We therefore suppose that p is not irreducible, i.e. that there exists y, z both non units such that $p = yz$. We want to show that (p) is not maximal.
By construction, we have that:

$$(p) \subset (y) \subset A$$

Since y is not a unit, $(y) \neq A$. We still need to show that $(p) \neq (y)$. This is true since, otherwise, $y = pt$, which would yield that:

$$p = yz = ptz \implies p(1 - tz) = 0 \overset{p \neq 0}{\implies} tz = 1 \implies z \text{ is a unit}$$

This means that:

$$(p) \subsetneq (y) \subsetneq A$$

which indeed shows that (p) is not maximal.

□

Monday 11th December 2023 — **Lecture 12 : And now they do**

Proposition Let A be a commutative ring, and $I \subset A$ be an ideal.
I is maximal if and only if A/I is a field.

Proof $\implies$ We do this proof by the contrapositive. We therefore want to show that A/I is not a field implies that $I \subset A$ is not maximal.

Since it is not a field, there exists some non-zero non-unit $[b] \in A/I$. Our goal is to show that $J = I + (b)$ is such that $I \subsetneq J \subsetneq A$.

By definition of quotient rings, we know that $[b] \neq [0] \iff b \notin I$. We moreover trivially now that $I \subset J = I + (b)$. This directly gives us that $I \subsetneq J$.

Since J is an ideal, we also know that $J \subset A$. Let us therefore suppose towards contradiction that $J = A$. This yields that $1 \in J = I + (b)$ and thus, by definition of the addition of ideals and of (b), that there exists some $a \in I$ and $y \in A$ such that:

$$a + by = 1$$

This however implies that $[by]_I = [1]_I$, showing that $[b]$ is a unit in A/I, which is a contradiction.

We have therefore indeed constructed a J such that $I \subsetneq J \subsetneq A$.

Proof $\impliedby$ We will only do this proof for PIDs, but this is valid for any commutative ring.

We consider two cases. We first suppose that $I = (0)$. This means that $A/I = A$; which is a field by hypothesis. This means that any $b \in A \setminus \{0\}$ is a unit in A, and thus that $(b) = A$. Since adding any non-zero element of A to the ideal makes it non-proper, this indeed means that (0) is maximal.

We now consider $I = (a)$ for some $a \neq 0$. We do this proof by the contrapositive, i.e. we suppose that (a) is not maximal and we want to show that A/I is not a field. Since (a) is not maximal, there must exist some $b \in A$ such that $(a) \subsetneq (b) \subsetneq A$. This however means that $a \in (b)$ and thus that $a = bt$ for some $t \in A$. We want to show that $[b], [t] \neq [0]$ since they would then represent zero-divisors in $A/(a)$.

We directly notice that $[b] \neq [0]$ by definition of quotient rings, since $b \notin (a)$. Now, let us suppose towards contradiction that $t \in (a)$. This means that there exists some $s \in A$ such that:

$$t = sa \implies a = bt = bsa \iff a(1 - bs) = 0$$

Since we are considering a PID, this is an integral domain. We have moreover seen that $a \neq 0$, telling us that:

$$1 - bs = 0 \iff bs = 1$$

However, this means that $1 \in (b)$, which implies that $(b) = A$. This is our contradiction.

This allows us to know that $[b]$ and $[t]$ are non-trivial zero-divisors in $A/(a)$:

$$[b]_{(a)}[t]_{(a)} = [bt]_{(a)} = [0]_{(a)}$$

This shows that $A/(a)$ cannot be a field.

□

Personal remark 1 This is analogous to the following proposition we already saw: $p \in \mathbb{P}$ is prime (which, in this context, is equivalent to it being irreducible and thus that (p) is maximal) if and only if $\mathbb{Z}/p\mathbb{Z}$ is a field.
This is one of the observations that justify my remark on the definition of irreducible: even if irreducible elements are not exactly prime elements, we can make a link between them to get a stronger intuition.

Personal remark 2 I thank Zichen Gao for their help on these proofs:

`https://edstem.org/eu/courses/719/discussion/83995`

Corollary Let F be a field, and $f(x) \in F[x]$ be a polynomial.
$F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Goal We therefore now want to understand when a polynomial is irreducible.

4.11 Irreducible polynomials

Theorem: Polynomial irreducibility 1 Let F be a field, and $f(x) \in F[x]$ be a polynomial of degree 1.
Then, it is irreducible in $F[x]$.

Proof Let $f(x)$ be a polynomial of degree 1. Let's suppose that there exists $g(x), h(x)$ such that:

$$f(x) = g(x)h(x)$$

This yields that:

$$1 = \deg f = \deg g + \deg h$$

This means that one of $g(x)$ and $h(x)$ has degree 1, and the other has degree 0. However, degree 0 means that it is a constant, and therefore a unit since we are working over a field F. This means that $f(x)$ is irreducible by definition.

□

Theorem: Polynomial irreducibility 2 Let F be a field, and $f(x) \in F[x]$ be a polynomial of degree 2 or 3.
$f(x)$ is irreducible in $F[x]$ if and only if it has no root in F.

Proof $\implies$ Let $f(x)$ be a polynomial of degree 2 or 3, which is reducible. This yields that there exists $g(x), h(x)$ both non-units such that:

$$f(x) = g(x)h(x)$$

Since they are not units, they cannot have degree 0. This means that one of them has degree 1 and the other has degree 1 or 2. We suppose without loss of generality that $g(x)$ has degree 1, i.e. $g(x) = ax + b$ for some $a, b \in F$ and $a \neq 0$. However, we then notice that $x = -\frac{b}{a}$ is a root:

$$f\left(-\frac{b}{a}\right) = g\left(-\frac{b}{a}\right)h\left(-\frac{b}{a}\right) = 0 \cdot h\left(-\frac{b}{a}\right) = 0$$

Remark This is not true for polynomials of degree strictly greater than three. Indeed, for instance, $\big(x^2+1\big)\big(x^2+2\big)$ has no roots in $\mathbb{Q}$, but it is not irreducible.

Proposition We consider the commutative ring $\mathbb{Q}[x]$. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial with integer coefficient:

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

If $\alpha \in \mathbb{Q}$ is a root of $f(x)$ with reduced fraction form $\alpha = \frac{r}{s}$, then $s \mid a_n$ and $r \mid a_0$.

Proof We notice that:

$$0 = f\Big(\frac{r}{s}\Big)s^n = a_n r^n + \ldots + a_1 r s^{n-1} + a_0 s^n$$

Since r divides the left hand side and all terms of the right hand side except possibly $a_0 s^n$, we must have $r \mid a_0 s^n$. However, since $\frac{r}{s}$ is a reduced fraction we get that $\gcd(r,s) = 1$ and thus that r cannot divide s^n. This indeed yields that $r \mid a_0$.

For a similar reasoning, s divides everything of the right hand side except possibly $a_n r^n$, meaning that $s \mid a_n$.

□

Implication This allows us to find rational roots of polynomials with integer coefficients: we only have few terms to verify.

Personal remark: Mnemonic To recall if $s \mid a_n$ or $s \mid a_0$, one can think of a simple example such as $x^2 - 4$. The roots are $\pm\frac{2}{1}$, telling us indeed that $\pm 2 = r \mid a_0 = 4$ and $1 = s \mid a_n = 1$.

Theorem: Eisenstein criterion Let $f(x) = a_0 + \ldots + a_n x^n \in \mathbb{Z}[x]$ be a polynomial such that:

$$\gcd(a_0, \ldots, a_n) = 1$$

Also, let $p \in \mathbb{P}$ be a prime such that $p \mid a_i$ for all $0 \leq i \leq n-1$, but $p \nmid a_n$ and $p^2 \nmid a_0$.
Then, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof This proof is available in the course notes on Moodle.

Example 1 We consider the following polynomial over $\mathbb{Q}[x]$:

$$g(x) = 2x^3 + 4x^2 + 11x + 1$$

We know that, if $\frac{r}{s} \in \mathbb{Q}$ is a root, then $r \mid 1$ and $s \mid 2$. We therefore have:

$$r \in \{\pm 1\}, \quad s \in \{\pm 1, \pm 2\}$$

This yields:

$$\alpha = \frac{r}{s} \in \left\{\pm\frac{1}{2}, \pm 1\right\}$$

However, checking all the four values, none of them is a root. Since $\deg g = 3$ and it has no roots, it is irreducible.

Example 2 Let us consider the following polynomial over $\mathbb{Q}[x]$:

$$f(x) = 7x^6 + 21x^4 + 12x^2 + 9x + 3$$

Since this is of degree greater than 3, we cannot use the same strategy. Even if we find that it has no root, it would tell us no information on whether $f(x)$ is reducible.

We therefore want to use Eisenstein's criterion. We find that $p = 3 \in \mathbb{P}$ works:

$$3 \nmid 7, \quad 3 \mid 21, \quad 3 \mid 12, \quad 3 \mid 9, \quad 3 \mid 3, \quad 9 \nmid 3$$

By Eisenstein's criterion, this means that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example 3 Let $p \in \mathbb{P}$. We consider the following polynomial over $\mathbb{Q}[x]$:

$$g(x) = x^k - p$$

This is irreducible by Eisenstein's criterion. Indeed:

$$p \nmid 1, \quad p \mid p, \quad p^2 \nmid p$$

Remark However, the following polynomial is not irreducible:

$$h(x) = x^{2k} - p^2 = \big(x^k - p\big)\big(x^k + p\big)$$

All hypotheses of Eisenstein's criterion apply, except that $p^2 \nmid a_0^2$. This show that this hypothesis is very important.

Proposition Let F be a field with q elements, $f(x) \in F[x]$ be of degree n, and $K = F[x]/(f(x))$. If $f(x)$ is irreducible, then any element of K has degree $n-1$ or less, i.e. any element has the form:

$$a_0 + a_1\overline{x} + \ldots + a_{n-1}\overline{x}^{n-1}$$

where $a_i \in F$ and $\overline{x}^i = \big\{x^i + f(x)g(x) \;\big|\; g(x) \in F[x]\big\}$.
Moreover, the field K has q^n elements.

Proof idea We can use Euclidean division to find:

$$a(x) = f(x)q(x) + r(x)$$

where $f(x)q(x) \in (f(x))$ and $\deg r \leq n-1$.
Then, we have q choices for a_0, q for a_1, and so on until a_{n-1}; showing that K has q^n elements.

Example 1 We consider the following polynomial over $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$:

$$f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$$

We notice that f has no roots in $\mathbb{F}_2$, trying all elements of the set: $f(0) = f(1) = 1$. Moreover, since $\deg f = 3$, it is irreducible.
Now, let us consider $K = \mathbb{F}_2[x]/(f(x))$, which we know is a field since $f(x)$ is irreducible. We also know that:

$$|K| = |\mathbb{F}_2|^3 = 2^3 = 8$$

Furthermore, any element of K has the form:

$$a\overline{x}^2 + b\overline{x} + c, \quad a, b, c \in \mathbb{F}_2$$

This means that:

$$K = \big\{0, 1, \overline{x}, \overline{x}^2, \overline{x}+1, \overline{x}^2+1, \overline{x}^2+\overline{x}, \overline{x}^2+\overline{x}+1\big\}$$

It is quite surprising that K is a field; it might not appear at first that all its non-zero elements must have an inverse. Note that we know that $\mathbb{F}_2[x]$ is definitely not a field on the other hand since, for instance, x has no multiplicative inverse. Let's find the inverse of $\overline{x}$.
We know that $\gcd\big(x, x^3 + x^2 + 1\big) = 1$ by construction of K (otherwise, $\overline{x}$ would not have an inverse). This means that there exists $h(x), g(x)$ such that:

$$xg(x) + \big(x^3 + x^2 + 1\big)h(x) = 1$$

Doing guesswork, we can find that:

$$x\left(x^2+x\right)+\left(x^3+x^2+1\right)=2x^3+2x^2+1=1$$

over $\mathbb{F}_2$.
This means that, indeed, $\overline{x}$ has an inverse, which is:

$$(\overline{x})^{-1}=\overline{x}^2+\overline{x}\in K$$

Remark This is a typical exam question.

Example 2 Let's consider the following polynomial, over the field $F=\mathbb{R}$:

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

This yields that $K=\mathbb{R}[x]/\left(x^2+1\right)$ is a field. This is in fact also a vector space of dimension 2 over $\mathbb{R}$, with all elements of the form:

$$\{a+b\overline{x}\mid a,b\in\mathbb{R}\}$$

We moreover notice that:

$$\overline{x}^2=\overline{x}^2-\left(\overline{x}^2+1\right)=-1$$

We notice that this has the structure of $\mathbb{C}$. We managed to construct this set algebraically.

Remark We have seen the great power of polynomials: given some field F, they allow us to create a bigger field $F[x]/(f(x))$. *I definitely did not see that coming!*

4.12 Finite fields and their classification

Fundamental theorem of Algebra Let F be a field, and $f(x)\in F[x]$ be a polynomial of degree $n=\deg f$.
If f is non-zero, then it has as most n roots.

Proof idea Let $a_1\in F$ be a root of $f(x)$, i.e. $f(a_1)=0$. Then, doing Euclidean division, we can find that $g_2(x)=\frac{f(x)}{x-a_1}$ has a rest of 0. Now, we again take $a_2\in F$ to be a root of $g_2(x)$, and compute $g_3(x)=\frac{f(x)}{(x-a_1)(x-a_2)}$. We stop when g_k has no root.
Every iteration, we decrease the degree of g_k by 1. We cannot decrease the degree of a constant polynomial, there can therefore be at most $\deg f=n$ roots.

Remark Over rings that are not fields, polynomials of degree m may have more than m roots. Indeed, let's consider the following polynomial of degree 2 over $\mathbb{Z}/8\mathbb{Z}$:

$$f(x)=x^2-1$$

It has 4 roots:

$$\{[1],[3],[5],[7]\}$$

Proposition Let K be a finite field.
Then, its group of units, $K^*=K\setminus\{0\}$ (a field only has 0 as non-unit) with multiplication, is cyclic.

Proof Let $n=|K^*|$.

We moreover know that $(K^*, \cdot)$ is a finite Abelian group, it has all properties thanks to the definition finite fields. We can therefore express it using invariant factors:

$$K^* \simeq C_{d_1} \times \ldots \times C_{d_s}$$

where $d_1 \mid \ldots \mid d_s$ and $d_1 \cdots d_s = n$.
Let $m = d_s$. We notice that this is the maximal order of an element of K^*, since $m = \operatorname{lcm}(d_1, \ldots, d_s)$. However, since the order of an element is less than or equal to the order of the group, we have that $m \leq n$.
Moreover, $t^m = 1$ for any $t \in K^*$, since $d_1, \ldots, d_{s-1} \mid d_s$. This yields that the elements of K^* are solutions of $t^m - 1 = 0$. However, a polynomial of degree m has at most m roots in a field by the fundamental theorem of Algebra. This yields that $n \leq m$.
Putting those two facts together, we get that $n = m$. Since also $d_1 \cdots d_s = n$, this forces $s = 1$. This indeed means that $K^* \simeq C_m$ is a cyclic group.

□

Remark This is again not true over rings that are not fields. For instance, the group of units of $\mathbb{Z}/8\mathbb{Z}$ is not cyclic:

$$(\mathbb{Z}/8\mathbb{Z})^* = \{[1], [3], [5], [7]\} \simeq C_2 \times C_2 \not\simeq C_4$$

which we can show using the following isomorphism:

$$(1,1) \mapsto [1], \quad (1,t) \mapsto [3], \quad (q,1) \mapsto [5], \quad (q,t) \mapsto [7]$$

Example Let us consider the following polynomial over $\mathbb{F}_2[x]$:

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

We have already shown that $K = \mathbb{F}_2[x]/(f(x))$ is a field in a previous example. Therefore, K^* is cyclic. Since $|K| = 8$, we have that $|K^*| = 7$, and thus:

$$K^* \simeq C_7$$

We found that:

$$K = \left\{0, 1, \overline{x}, \overline{x}^2, \overline{x}+1, \overline{x}^2+1, \overline{x}^2+\overline{x}, \overline{x}^2+\overline{x}+1\right\}$$

Let us check that $\overline{x} \in K^*$ is indeed a generator of K^*:

$$\overline{x}^2, \quad \overline{x}^3 = \overline{x}^2 + 1, \quad \overline{x}^4 = \overline{x}^2 + \overline{x} + 1, \quad \overline{x}^5 = \overline{x} + 1, \quad \overline{x}^6 = \overline{x}^2 + \overline{x}, \quad \overline{x}^7 = 1$$

where we used that:

$$\overline{x}^3 = -\overline{x}^2 - 1 = \overline{x}^2 + 1$$

Remark This is a typical exam question.

Proposition 1 Let K be a finite field.
Then, the characteristic of K is a prime number:

$$c(K) = p \in \mathbb{P}$$

Proof We do this proof by the contrapositive.

Thanks to the characteristic, we know that there exists a ring homorphism $\tau : \mathbb{Z} \mapsto K$ such that $\tau(1) = 1$. Moreover:

$$\tau(m) = m \cdot 1$$

We know that the characteristic of an integral domain is either a prime or 0. Now, if the characteristic is 0, then $\tau(m) \neq 0$ for any $m \in \mathbb{N}$. This yields that K is infinite.

Proposition 2 Let K be a finite field of characteristic $c(K) = p$.

Then, K contains a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z} \stackrel{\text{def}}{=} \mathbb{F}_p$.

Proof idea Let $\tau : \mathbb{Z} \mapsto K$ be the usual characteristic homomorphism. We know that $x = p$ is the smallest positive integers such that $\tau(x) = 0$, since $c(K) = p$.

This means that $\hat{\tau} : \mathbb{Z}/p\mathbb{Z} \mapsto \tau(\mathbb{Z}/p\mathbb{Z})$, the restriction of τ to $\mathbb{Z}/p\mathbb{Z}$, is injective. We can verify that this is also a homomorphism, which is surjective by definition of its image. This yields that $\tau(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$.

Proposition 3 Let K be a finite field of size $|K| = p$.

Then:

$$K \simeq \mathbb{F}_p$$

Remark This means that the finite fields of a prime size are always unique.

Proposition 4 Let K be a finite field of characteristic $c(K) = p$.

Then, $|K| = p^n$ for some $n \in \mathbb{N}^*$. Moreover, K is a vector space over $\mathbb{F}_p$.

Proposition 5 Let $p \in \mathbb{P}$ be a prime, and $n \in \mathbb{N}^*$.

There exists a finite field K with $|K| = p^n$ and an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ such that $\mathbb{F}_p[x]/(f(x)) \simeq K$.

If $g(x)$ is another irreducible polynomial of degree n over $\mathbb{F}_p$, then:

$$K \simeq \mathbb{F}_p[x]/(f(x)) \simeq \mathbb{F}_p[x]/(g(x))$$

Summary To sum up, we have seen the following (very powerful) classification of finite fields:

1. For any prime p and any $n \geq 1$, there exists a unique field $\mathbb{F}_{p^n}$ of p^n elements. It has a characteristic $c(\mathbb{F}_{p^n}) = p$.
2. For $n = 1$, this unique field is isomorphic to $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$.
3. For $n > 1$, this unique field can be constructed as a quotient $F_{p^n} \simeq \mathbb{F}_p[x]/(f(x))$, where $f(x)$ is any irreducible polynomial of degree n over $\mathbb{F}_p$.

Example Let us consider the following polynomials over $\mathbb{F}_2$:

$$f(x) = x^3 + x^2 + 1, \quad g(x) = x^3 + x + 1$$

Then:

$$\mathbb{F}_2[x]/(f(x)) \simeq \mathbb{F}_2[x]/(g(x))$$

which have size $2^3 = 8$.

We will find an explicit isomorphism in the problem set 13.

Corollary Over $\mathbb{F}_p$, there exists an irreducible polynomial of any degree $n \in \mathbb{N}_{\geq 1}$.

Remark This may however fail for fields of characteristic 0. For instance, over $\mathbb{R}$, the only irreducible polynomials are of degree 1 or 2. Similarly, over $\mathbb{C}$, polynomials are irreducible if and only if they are of degree 1.

On the other hand, for $\mathbb{Q}$, we can always take $x^n - p$, which is irreducible in $\mathbb{Q}$ by Eisenstein s criterion.

Definition: Algebraically closed field

Let F be a field.

If its only irreducible polynomials are of degree 1, it is called **algebraically closed**.

Example $\mathbb{C}$ is algebraically closed, but $\mathbb{R}, \mathbb{Q}$ and $\mathbb{F}_p$ are not.

Remark

We know that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We may therefore wonder whether $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{F}_{p^n}$ are isomorphic.

However, we directly notice that $\mathbb{Z}/p^n\mathbb{Z}$ is not a field.

For instance, $\mathbb{Z}/4\mathbb{Z}$ has zero-divisors: $[2] \cdot [2] = [0]$ for example. Another way to see this is not a field is to see that it has a characteristic 4, which is not a prime.

This means that:

$$\mathbb{F}_{p^n} \not\simeq \mathbb{Z}/p^n\mathbb{Z}$$