Algebra - MATH310

Jacopo “quartztz” Moretti

January 2024

Preface

Helo! I'm Jack :3.

I'm a student that needs to type out courses in order to make sure they properly understand them. So I put them out into the world! They might help you more than they help me :D. They are given as they are, with no guarantee of quality but guarantee of goodwill, bla bla bla. You know the gist of it.

Elements of notation

The group operation for a group G will usually be denoted $\cdot_G$, and its neutral element will be e_G. The index will be removed when it can be inferred from context.

For now, I'll denote $\mathbf{n} = \{1, ..., n\}$, because it's clunky to type and it's my notes, goddamnit. I might change it back at the end.

Also sometimes I get caught up and I use the weird (though admittedly concise) notation:

$$\text{"... consider an } 0 \neq a \in A\text{"}$$

which is to be read as "consider an a in A such that it is non zero". Sorry for the confusion.

Contents

Chapter 1

Introduction

Week 1

Algebra rests on 3 basic principles, which are equivalent in nature.

(i). **Induction:** Let $S \subset \mathbb{N}$ such that $0 \in S$ and $n \in S \Rightarrow n+1 \in S$. Then, $S = \mathbb{N}$.

(ii). **Well-ordering principle:** For any non-empty $A \subset \mathbb{N}$, there exists an element a : $\forall b \in A, a \leqslant b$.

(iii). **Strong induction:** Let $S \subset \mathbb{N}$ such that $0 \in S$ and $\{0, ..., n\} \in S \Rightarrow n+1 \in S$. Then, $S = \mathbb{N}$.

It is well-established that these three principles are equivalent. Let us prove it.

Theorem 1.1. ***I*** $\Rightarrow$ ***WOP*** $\Rightarrow$ ***SI*** $\Rightarrow$ ***I***.

Proof. We will prove each induction separately.

(i). 1. $\Rightarrow$ 3. Let S be the construction from the strong induction definition, and let us consider $P(n) = \{0, 1, ..., n\} \subset S$. We can prove it by induction:

Base: $0 \in S$ by construction $\Rightarrow \{0\} \subset S$.

Induction: Let us prove that $P(k) \Rightarrow P(k+1)$ for some k.

$$\begin{aligned} \{0, 1, ..., k\} \subset S \text{ [by IH]} &\Rightarrow k \in S && \text{[by construction]} \\ &\Rightarrow k+1 \in S && \text{[by definition]} \\ &\Rightarrow \{0, 1, ..., k, k+1\} \in S \end{aligned}$$

Since it is hereditary and true for 0, it is true $\forall n \in \mathbb{N}$ by the induction principle.

Since $\{0, 1, ..., n\} \subset \mathbb{N}\ \forall n$, then $S = \mathbb{N}$.

(ii). $2 \Rightarrow 1$. Suppose $S \subset \mathbb{N}$ such that $0 \in S$ and $n \in S \Rightarrow n+1 \in S$. Consider $S' = \mathbb{N} \setminus S$, which we assume to be nonempty by absurd. By the well-ordering principle, we can pick a least element in $k \in S'$, which is by definition not in S. k cannot be zero, since $0 \in S$ by definition, but it can also not be non-zero, since $k \neq 0 \Rightarrow k = m+1$ for some $m < k$ (therefore not in S'). $m \in S$, so by construction, $m + 1 = k \in S$ as well, which is a contradiction. S' has to be empty, so $S = \mathbb{N}$.

(iii). $3 \Rightarrow 2$. Done in a Problem Set, found in appendix A.

□

Chapter 2

Primes

2.1 Divisors and primes

Definition 2.1. *Let $a, b \in \mathbb{Z}$. We say that a divides b (notate: $a|b$) if there exists $k \in \mathbb{Z}$ such that $b = ka$.*

Definition 2.2. *A number $p \in \mathbb{Z}$ is prime if $p > 1$ and the only numbers that divide it are itself and 1.*

Theorem 2.3. *Any $n > 1$ has a prime divisor.*

Proof. Let $S = \{n \in \mathbb{N} : n > 1 \wedge n \text{ has no prime divisors}\}$. We suppose S to be nonempty, meaning it contains a least element $k \in S$. k cannot be prime, since $k|k \; \forall k$. Therefore, it has to be true that $k = ab$ for $a, b < k \in \mathbb{N}$. Since k was the lest element, then, $a \notin S$, meaning that there exists a prime p such that $a = pt$ for $tin\mathbb{N}$. Therefore, $k = ab = ptb \Rightarrow p|k$, contradicting our construction of S. Therefore, S must be empty. □

Theorem 2.4. *Any $n > 1$ can be expressed by the product of primes.*

> This proof was done in a problem set, and can be found in the appendix.

Theorem 2.5. *The prime number factorization of a number is unique.*

Proof. Let $k = \prod^n p_i = \prod^m q_j$ two distinct prime sets. Suppose without loss of generality that $q_1 > p_1$ and let $t = (q_1 - p_1)q_2...q_m > 0$. Then:

$$\begin{aligned} t &= (q_1 - p_1)q_2...q_m \\ &= q_1 q_2...q_m - p_1 q_2...q_m \\ &= k - p_1 q_2...q_m > 0 \Rightarrow p_1|t \end{aligned}$$

We know that $p_1 \neq q_j$ for all j, so we focus on the only "weird" term:

$$\begin{aligned} (q_1 - p_1) &= sp_1 \\ \Rightarrow q_1 &= (s+1)p_1 \end{aligned}$$

Which is a contradiction because q_1 is supposed to be prime. Therefore, the prime factorization is unique. □

2.2 Integer arithmetic

Definition 2.6 (Euclidian division)**.** *Let $n \in \mathbb{Z}, d \in \mathbb{Z}^*$. There exists a unique pair $q, r \in \mathbb{Z}$ such that $n = qd + r$ with $0 < r < d$.*

Proof. **Existence.** Consider the set

$$S = \{n - kd\}_{k \in \mathbb{Z}} \cap \mathbb{N} = \{n - kd, kd \leqslant n\}_{k \in \mathbb{Z}}$$

We know that S is not empty, because:

▷ if $n >= 0$, then we set $k = 0$, meaning $n \in S$

▷ if $n < 0$, then we set $k = |n| + 1$, meaning $kd > |n|$ and $n + kd \in S$.

Since it's never empty, we can pick the least element of S by means of the well-ordering principle. Let's call it r. Therefore, we have $r = n - kd$ for some k. To prove $r < d$, we assume towards absurdity that $r >= d$, meaning that

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

meaning r wasn't minimal, which is a contradiction.

Uniqueness. Suppose $n = q_1 d + r_1 = q_2 d + r_2$. Without loss of generality, assume $q_1 > q_2$. Then:

$$(q_1 - q_2)d + r_1 = r_2 \geqslant d$$

Since r_1 and $q_1 - q_2$ are positive. This contradicts the definition of r_2, and is therefore absurd. □

Definition 2.7. *Let $a, b \in \mathbb{Z}$. We define the greatest common divisor (*gcd*) of two numbers as*

$$\gcd(a, b) = \max\{x \in \mathbb{Z} : x|a \wedge x|b\}$$

Theorem 2.8. *For $n, q \in \mathbb{Z}, d \in \mathbb{Z}^*$, such that $n = qd + r$, it is always the case that:*

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

Proof. By inspection of the relationship $n = qd + r$, it's clear that if $x|n \wedge x|d$ then $x|r$, and if $x|d \wedge x|r$ then $x|n$. □

> *Method* This induces a special algorithm to compute the gcd of two numbers! Let $d_1, d_2 \in \mathbb{Z}$. Then:
>
> $$\begin{aligned} d_1 &= q_1 d_2 + d_3 \\ d_2 &= q_2 d_3 + d_4 \\ &\;\;... \\ d_k &= q_k d_{k+1} + 0 \end{aligned}$$
>
> The relationship $\gcd(d_{i-1}, d_i) = \gcd(d_i, d_{i+1})$ holds down the tree, meaning that by the end
>
> $$\gcd(d_1, d_2) = d_{k+1}$$
>
> Additionally, we have:

> **Corollary 2.9.** *For any $a, b \in \mathbb{Z}^+$, there exist $x, y \in \mathbb{Z}$ such that*
>
> $$\gcd(a, b) = xa + yb$$
>
> This is obtained by running Euclid "up the tree".
> **Example 1.** *TODO*

Special consequence of corollary 2.9 is the following

Corollary 2.10. *If $a, b \in \mathbb{Z}^+$ are such that $d = \gcd(a, b)$, then the equation:*

$$c = ax + by$$

has solutions (x, y) if and only if $\exists\ k > 0 : c = kd$, and they can be found as the solutions in corollary 2.9 multiplied by k.

Final consequence of these facts is the well-known Bézout's theorem.

Theorem 2.11. *Two numbers $a, b \in \mathbb{Z}^+$ are relatively prime if and only if the equation*

$$1 = ax + by$$

has integer solutions.

Definition 2.12. *For any $n \in \mathbb{Z}^+$, Euler's totient function is defined as:*

$$\varphi(n) = \left|\left\{k \in \{1, ..., n\} : \gcd(k, n) = 1\right\}\right|$$

meaning the number of positive integers less than n that are coprime to it.

> *Properties* Properties of the totient function include:
>
> - ▷ $\varphi(p) = p - 1$ for any prime p.
> - ▷ $\varphi(pq) = (p - 1)(q - 1)$ for any pair of distinct primes p, q.
> - ▷ More generally, $\varphi(mn) = \varphi(m)\varphi(n)$ for any m, n coprime.

Chapter 3

Groups

Week 2

3.1 Base definitions

3.1.1 Groups and cosets

Definition 3.1. *A group is a set G with a binary operation $\cdot : G \times G \to G$, satisfying the following axioms:*

- ▷ *$\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*
- ▷ *There exists a neutral element e such that $a \cdot e = e \cdot a = a \ \forall a \in G$.*
- ▷ *For any $a \in G$ there exists an inverse a^{-1} such that $a^{-1} \cdot a = a \cdot a^{-1} = e$.*

We say that G is a finite group if $|G| < \infty$. In that case, we say that G is of order $|G|$. We say that G is abelian (or commutative) if $a \cdot b = b \cdot a \ \forall a, b \in G$.

Definition 3.2. *$H \subset G$ is a subgroup if it contains the neutral element e_G and if it is closed with respect to $\cdot_G$, meaning that for every $a, b \in H$, $a \cdot b \in H$, and to inverses.*

We can note that any group has a subgroup generated by a single element:

$$\langle g \rangle = \{e, g^1, g^2, \dots, g^{-1}, g^{-2}, \dots\}$$

Since $g^i \cdot g^j = g^{i+j}$ by definition of the group operation, this set is closed under it, meaning it is a subgroup.

Definition 3.3. *If it exists, the minimal $n \in \mathbb{N}^*$ such that $g^n = e$ is called the order of g. It is finite for every element in a finite group.*

Definition 3.4. *Let $H \subset G$ be a subgroup of G. The left coset of g with respect to H, denoted gH, is the following set:*

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

Theorem 3.5. *Let $H \subset G$ finite. Then:*

(i). Two left-cosets xH, yH are either disjoint ($xH \cap yH = \varnothing$) or equal.

(ii). For any element $g \in G$ there exists a left coset of H such that $g \in H$.

(iii). $|xH| = |H| \; \forall x \in G$

Proof. We will prove each part separately:

(i). Suppose xH, yH are such that $xH \cap yH \neq \varnothing$. This means that there exist h_1, h_2 such that $xh_1 = yh_2$. Therefore,

$$x = yh_2h_1^{-1} = yh_3 \in yH \Rightarrow xh = yh_3h \; \forall h \in H$$

This means that if there exists an element of xH that is in yH, then every element in xH can be written as an element in yH, meaning they are equal.

(ii). For any $g \in G$, one can construct $gH = \{e, g, g^2, ...\}$, which naturally contains g.

(iii). The mapping

$$\begin{aligned} f(h) : H &\to xH \\ h &\mapsto xh \end{aligned}$$

is surjective, by definition of $xH = \{xh, h \in H\}$, and it is also injective, since $xh_1 = yh_2 \Leftrightarrow h_1 = h_2$. This means it defines a bijection between H and xH, indicating they have the same cardinality.

> *Example* Let $G = (\mathbb{Z}, +, 0), H = 3\mathbb{Z} \subset \mathbb{Z}$. The left coset of 0 with respect to H is :
>
> $$\{0 + 3k\}_{k\in\mathbb{Z}} = H = \{3 + 3k\}_{k\in\mathbb{Z}}$$
>
> The left coset of 1 is
>
> $$\{1 + 3k\}_{k\in\mathbb{Z}} = \{1, 4, 7, -2, ...\}$$

□

Theorem 3.6 (Lagrange's theorem)**.** *Let G be a finite group, $H \subset G$ a subgroup. Then, $|H|$ divides $|G|$.*

Proof. Each $g \in G$ belongs to a left coset of H, which are either disjoint or equal. This means:

$$\begin{aligned} G &= \bigcup_{i=0}^{r} x_iH && \text{[disjoint union of finite \# of sets]} \\ \Rightarrow |G| &= \sum_{i=0}^{r} |x_iH| \\ \Rightarrow |G| &= \sum_{i=0}^{r} |H| && \text{[since } |xH| = |H|\text{]} \\ \Rightarrow |G| &= r|H| \end{aligned}$$

with $r \in \mathbb{N}$, meaning that $|H|$ divides $|G|$. □

Definition 3.7. *The number of left cosets of H of G is called the index of G:*

$$[G : H] = |G|/|H| \in \mathbb{N}^*$$

This means that the order of any element $g \in G$ (notated $\operatorname{ord}(g)$) divides the order of the group $|G|$, since every element generates a subgroup $\langle g \rangle$. Additionally, it implies

Corollary 3.8. $g^{|G|} = (g^{\operatorname{ord}(g)})^k = e^k = e$ *for some* k.

3.1.2 RSA and back to primes

Theorem 3.9 (Euler's theorem)**.** *Let* $a, n \in \mathbb{Z}^+$. *such that* $\gcd(a, n) = 1$. *Then,*

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

Proof. Consider $G = (\mathbb{Z}/n\mathbb{Z}, \cdot, 1)$. Then,

$$a^{\varphi(n)} = a^{|G|} \overset{3.8}{=} 1$$

□

Theorem 3.10 (Fermat's little theorem)**.** *Let* $a \in \mathbb{Z}^+$, *p prime such that p does not divide a. Then,* $a^{p-1} = 1$.

Proof. Consider $G = (\mathbb{Z}/p\mathbb{Z}, \cdot, 1)$. Then, $|G| = \varphi(p) = p - 1$. By Euler's theorem,

$$a^{\varphi(p)} = a^{(p-1)} = 1$$

□

> *RSA* The RSA cryptosystem for message transmission works as follows:
>
> (i). Choose two distinct large primes p, q.
>
> (ii). Compute $m = pq \Rightarrow \varphi(m) = (p - 1)(q - 1)$.
>
> (iii). Choose $e \leqslant m$ an encryption key such that $\gcd(e, \varphi(m)) = 1$.
>
> (iv). Use Euclid's algorithm to determine d such that $ed - k\varphi(m) = 1$ for some integer k.
>
> (v). The encoding key is the pair (m, e), and it can be published. To decode, you use the decoding key (m, d) which is to be kept private.
>
> To send a message x to someone, you need their public pair (m, e). You first compute $c \equiv x^e \bmod m$, which can be sent publicly. To decode, the person will use their private pair (m, d), computing $x \equiv c^d \bmod m \equiv x^{ed} \bmod m$.

Why is it the case that $x^{ed} \equiv x \bmod m$? Well... Week 3

Theorem 3.11. *Let p, q be two distinct primes, and $m = pq$. Let $e : \gcd(e, \varphi(m)) = 1$, and let $d \in \mathbb{Z} : ed - k\varphi(m) = 1$ for some $k \in \mathbb{Z}$. Then,*

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

for all $x \in \mathbf{m}\}$.

Proof. If $x = pt$ for some t, then trivially $x \equiv x^{ed} \equiv 0 \bmod p$. If x is not divisible by p, then we can rewrite

$$x^{ed} = x^{k\varphi(m)+1}$$

By Fermat's theorem, we know that $x^{p-1} \equiv 1 \bmod p$, meaning:

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

Meaning in both cases $x^{ed} \equiv x \bmod p$. By a symmetric argument, the same is true $\bmod q$, allowing us to conclude

$$\begin{aligned} x^{ed} - x &\equiv 0 \bmod pq \\ &\equiv 0 \bmod m \\ \therefore x^{ed} &\equiv x \bmod m \end{aligned}$$

□

> *RSA* As a quick example, let's consider an RSA system with the following characteristics:
>
> $$p = 3, q = 11 \Rightarrow m = pq = 33, \varphi(m) = (p-1)(q-1) = 20$$
>
> We choose $e = 7$ which is coprime with $\varphi(m)$. We compute d:
>
> $$\begin{aligned} 20 &= 7 \cdot 2 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ \Rightarrow 1 &= 7 - 6 \cdot 1 \\ &= 7 - (20 - 7 \cdot 2) \cdot 1 \\ &= \underbrace{7}_{e} \cdot \underbrace{3}_{d} - \underbrace{20}_{\varphi(m)} \end{aligned}$$

3.2 Homomorphisms

3.2.1 When the morphism is homo D:

> *Examples* Recall a few examples of groups:
>
> (i). $\mathbb{Z}/n\mathbb{Z} = \big\{[0], [1], ..., [n-1]\big\}$ with regular modular addition and 0 as the neutral element.
>
> (ii). $(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$ with modular multiplication and 1 as the neutral element. This is a group because
>
> $$\begin{aligned} \gcd(a, n) = 1 &\Leftrightarrow \exists x, y \in \mathbb{Z} : ax + ny = 1 \\ &\Rightarrow [a] \cdot [n] = [1] \bmod n \end{aligned}$$
>
> These are two abelian!

(iii). The n-th complex roots of unity!

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

If you define $q = e^{i\frac{2\pi}{n}}$, then the group can be defined as the generated group:

$$\sqrt[n]{1} = \langle q \rangle = \{1, q, q^2, ..., q^{n-1}\} \overset{not.}{=} C_n$$

C_n is defined as the cyclic group of order n, and it's easy to convince yourself of the fact that $(C_n, \cdot, 1)$ is "the same" as $(\mathbb{Z}/n\mathbb{Z}, +, 0)$, in the sense that they have similar enough structure that you could map one onto the other and back.

Definition 3.12. *A map $\phi : G \to H$ between two groups is said to be a group homomorphism if*

$$\phi(x \cdot_G y) = \phi(x) \cdot_H \phi(y) \ \forall x, y \in G$$

This formally defines the "structure-maintaining" constraint on ϕ, and it also implies that $\phi(e_G) = e_H$ and $\phi(x^{-1}) = \phi(x)^{-1}$

Definition 3.13. *A group homomorphism that can be inverted to a group homomorphism is called a group isomorphism. If $\phi : G \to H, \psi : H \to G$ are two group homomorphisms such that $\phi \circ \psi = \mathrm{Id}_H, \psi \circ \phi = \mathrm{Id}_G$, then G and H are said to be isomorphic groups (denoted $G \simeq H$).*

Definition 3.14. *A group automorphism is a group isomorphism from a group onto itself $\phi : G \to G$.*

Example The map

$$\begin{aligned} \phi : C_n &\to \mathbb{Z}/n\mathbb{Z} \\ q^i &\mapsto [i] \end{aligned}$$

is a bijection, with inverse

$$\begin{aligned} \phi^{-1} : \mathbb{Z}/n\mathbb{Z} &\to C_n \\ [i] &\mapsto q^i \end{aligned}$$

and it respects the bounds on the group operations:

$$\begin{aligned} \phi(q^i \cdot q^j) &= \phi(q^{i+j}) = [i+j] \\ \phi(q^i) \cdot \phi(q^j) &= [i] + [j] = [i+j] \end{aligned}$$

meaning that $C_n \simeq \mathbb{Z}/n\mathbb{Z}$.

3.2.2 Generators and Relations

We've seen that groups can be represented as a set of elements coupled with a binary operation on those elements. However, we can define another representation of a group, based on generators and relations:

Definition 3.15. *The set of generators of a group G is the minimal subset of elements of G such that any element of G can be written as a product of generators and their inverses.*

Definition 3.16. *A relation is an equation that is satisfied by every element of a group.*

Definition 3.17. *A presentation of a group G in generators and relations is an expression of the form :*

$$G = \langle S | R \rangle$$

With S a set of generators, and R a set of relations on elements of S, such that any other relation on G follows from them.

> *Example* For example, the cyclic group of order n, C_n, is generated by q, since every element can be written as q^k for some $0 < k < n$. Additionally, the relation $q^n = 1$ holds on q. This means that we can write:
>
> $$C_n = \{1, q^1, ..., q^{n-1}\} = \langle q | q^n = 1 \rangle$$

This representation allows us to define group homomorphisms in an easier way:

Proposition. *Let $G = \langle S | R_1 = 1, ..., R_k = 1 \rangle$, let H a group. We define a mapping $\phi : G \to H$ as follows:*

a) $\phi(s) \in H$ for every generator $s \in S$.

b) $\phi(x_1 \cdot_G x_2) = \phi(x_1) \cdot_H \phi(x_2)$ for any $x_1, x_2 \in G$.

Then, ϕ is a group homomorphism if and only if $R_1, ..., R_k$ are satisfied for any $\phi(s)$.

Week 4

Definition 3.18. *Let $\phi : G \to H$ a group homomorphism. The kernel of a group homomorphism is the set*

$$\ker \phi = \{g \in G : \phi(g) = e_H\} \subset G$$

Proposition. *Let $\phi : G \to H$ a group homomorphism. The kernel of ϕ is a subgroup of G.*

Proof. Let $a, b \in \ker \phi$. Then:

- ▷ $\phi(e_G) = e_H$ by definition of a group homomorphism, meaning that $e_G \in \phi$.
- ▷ $\phi(a \cdot b) = \phi(a) \cdot \phi(b) = e \cdot e = e$, meaning that $a, b \in \ker \phi \Rightarrow ab \in \ker \phi$.
- ▷ $\phi(a^{-1}) = (\phi(a))^{-1} = e^{-1} = e$, meaning that $a \in \ker \phi \Rightarrow a^{-1} \in \ker \phi$.

These three properties mean that $\ker \phi$ is a subgroup of G. □

Definition 3.19. *Let $\phi : G \to H$ a group homomorphism. The image of ϕ is the set $\phi(G) \subset H$.*

Proposition. *Let $\phi : G \to H$ a group homomorphism. The image $\phi(G) = \{\phi(g)\}_{g \in G} \subset H$ is a subgroup in H.*

Proof. Let $h_1, h_2 \in \phi(G)$. Then

- ▷ $\phi(e_G) = e_H$ by definition of a group homomorphism, meaning $e_h \in \phi(G)$.
- ▷ $h_1 h_2 = \phi(g_1) \cdot \phi(g_2) = \phi(g_1 g_2)$ for some $g_1, g_2 \in G$, meaning $h_1 h_2 \in \phi(G)$.
- ▷ $h_1^{-1} = \phi(g_1)^{-1} = \phi(g_1^{-1})$, meaning $h_1^{-1} \in \phi(G)$,

This means $\phi(G)$ is a subgroup of H. □

Definition 3.20. *A subgroup $H \subset G$ is a normal subgroup (notated $H \triangleleft G$) if $\forall h, \forall g$, we have $ghg^{-1} \in H$.*

For any group homomorphism $\phi : G \to H$, the kernel $\ker G$ is a normal subgroup of G. If you take any $g \in G, h \in H$, then we have:

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)(\phi(g))^{-1} = e$$

meaning that $ghg^{-1} \in \ker G$ as well.

Definition 3.21. *The group of rigid symmetries of a flat regular n-gon is called the dihedral group of order n, and it is denoted D_n.*

> *About symmetries* It is generated by a single rotation counterclockwise, leaving the shape self-similar but with vertices "shifted" by one to the left, and one "mirroring" of the shape per axis of symmetry.
>
> For example, for a square, we have: TODO: ADD IMAGE
>
> $$D_4 = \{1, r, r^2, r^3, r^4, s_1, s_2, s_3, s_4\}$$
>
> with r a counterclockwise rotation and s_i a reflection across the i-th axis. The group operation is concatenation of action: it's easy to see how two consecutive rotations r might yield a double rotation ($r \cdot r = r^2$) and how concatenating a rotation and a symmetry can be defined as rs_i
>
> This is group is not commutative: take a piece of paper, draw a labelled square, and you'll soon convince yourself of the fact that $rs \neq sr$, i.e. that a rotation followed by a mirroring does not yield the same result as the same mirroring followed by the same rotation.
>
> In general, $|D_n| = 2n$: due to the nature of our moves, if after a move we have n "free" spots where vertex 1 could have ended up, after we choose that one, there's only two spots for vertex 2 (either right before or right after it) before defining a full state for the figure. This means $|D_n| \leqslant 2n$, and since we can lay out $2n$ elements, then $|D_n| = 2n$.
>
> Playing around with the polygon shows the evident relation $srs = r^{-1}$, equivalent to $(sr)^2 = 1$. With this, we can write:
>
> $$\begin{aligned} D_n &= \langle r, s | r^n = 1, s^2 = 1, srs = r^{-1} \rangle \\ &= \{1, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\} \end{aligned}$$
>
> Thanks to our relations, we know that we can write any product of moves under the form $s^a r^b$ for some a, b.
>
> The two subgroups that are worth mentioning are:

> ▷ the group of rotations $R = \langle r \rangle = \{1, r, ..., r^{n-1}\}$, which defines two cosets, the coset of rotations $1R$ and the coset of all symmetries $sR = \{s, sr, ..., sr^{n-1}\}$. It is a normal subgroup, since $gr^k g^{-1} \in R$ no matter what g you use.
>
> ▷ the group of symmetries $K = \langle s \rangle = \{1, s\}$. This is not a normal subgroup, as $rsr^{-1} = sr^{-1}r^{-1} = sr^{-2} \notin K$.

3.3 Weirder groups

Proposition. *Let $H \triangleleft G$. We define the product on left cosets of H as*

$$(xH) \cdot (yH) = (xyH)$$

with eH the neutral element, and $x^{-1}H$ the inverse. This product is well-defined and it induces a group structure on the set of cosets.

Proof. We just have to check that the product does not depend on the choice of coset representatives: let $x' \in xH, y' \in yH$, let us check that $x'y' \in xyH$. We know that $x' = xh_1, y' = yh_2$ for some $h_1, h_2 \in H$. We can write:

$$x'y' = xh_1yh_2 = xy(y^{-1}h_1y)h_2 \overset{(*)}{=} xyh_3h_2 = xyh_4 \in xyH$$

where step $(*)$ is motivated by the fact that H is normal. Since $x'y' \in xyH$, the product is well defined. □

Definition 3.22. *The group of left cosets of $H \triangleleft G$ is called the the quotient group G/H.*

> *Example* The cosets of $R \triangleleft D_n = \{1R, sR\}$ form the quotient group D_n/R, with the operations between them being the product of their representatives and the neutral element being the coset of 1 wrt R. The operations are
>
> $$\begin{aligned}(1R)(1R) &= (1R)\\(1R)(sR) &= (sR)\\(sR)(1R) &= (sR)\\(sR)(sR) &= (1R)\end{aligned}$$
>
> This pattern seems a little familiar: this group is isomorphic to $C_2 = \langle t | t^2 = 1\rangle$ (which are the two square roots of unity!), with the mapping function
>
> $$\begin{aligned}\phi : R/D_n &\to C_2\\1R &\mapsto 1\\sR &\mapsto t\end{aligned}$$

Proposition. *In an abelian group G, every subgroup $H \subset G$ is normal.*

This is barely a theorem, and is easily proven as $ghg^{-1} = hgg^{-1} = h \in H$ for any g. Week 5

Definition 3.23. *S_n is the group of permutations of sets of n elements* **n**.

> *Properties* A permutation is an element of S_n, for which we'll see a few different representations; the group operation is composition between two elements; the neutral element is the trivial permutation that moves no element.
>
> For an element $s \in S_n$, we denote si the index on which it sends the number $i \in \mathbf{n}$
>
> In general, $|S_n| = n^1$.

.

We introduce a new notation for elements of S_n. In the meantime, let us denote a permutation as two lists: the first is the input one, and the second is the result of applying the permutation once. On S_4, the trivial permutation would look like:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Consider an arbitrary element $\rho \in S_n$, of order k, and construct $\langle \rho \rangle = \{1, \rho, ..., \rho^{k-1}\}$. Take $x \in \mathbf{n}$: then we can construct the orbit $\operatorname{Orb}_\rho x := \{x, \rho x, ...\}$. This orbit is unique to each x: if there were two x_1, x_2 such that their orbits aren't disjoint, there would exist i, j such that

$$\rho^i x_1 = \rho^j x_2 \Leftrightarrow \rho^{i-j} x_1 = x_2 \Rightarrow x_2 \in \operatorname{Orb}_\rho x_1$$

This implies that $\operatorname{Orb}_\rho x_2 \subset \operatorname{Orb}_\rho x_1$, and we can find $\operatorname{Orb}_\rho x_1 \subset \operatorname{Orb}_\rho x_2$ pretty symmetrically: this means $\operatorname{Orb}_\rho x_1 = \operatorname{Orb}_\rho x_2$.

Definition 3.24. *We say that $\pi \in S_n$ is a cycle if it has a single non-trivial (containing more than a single element) orbit. The length of this non-trivial orbit is said to be the length of the cycle.*

Therefore, we have that

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

is a cycle because $\operatorname{Orb}_\rho 1 = \operatorname{Orb}_\rho 2 = \{1, 2\}$ is its only nontrivial orbit, but

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

isn't because it has two nontrivial orbits, $\operatorname{Orb}_\rho 1 = \operatorname{Orb}_\rho 2 = \{1, 2\}$ and $\operatorname{Orb}_\rho 3 = \operatorname{Orb}_\rho 4 = \{3, 4\}$. A cycle of length k, will be notated as such:

$$\pi \in S_n : (x, \pi(x), \pi^2(x), ..., \pi^{k-1}(x))$$

taking x an arbitrary element such that the orbit $\operatorname{Orb}_\pi x$ is nontrivial.

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

would be notated as $\rho = (12)$.

This means that the cycle

$$(i_1, i_2, ..., i_k)$$

is the permutation that sends $i_1 \mapsto i_2, i_2 \mapsto i_3, ..., i_k \mapsto i_1$, and leaves every other element unchanged.

[1] This follows from CS101. I didn't pass that class, but I hear it's where we saw it first.

Proposition. *Let S_n be the group of permutations on* $\mathbf{n}$*. Then, disjoint cycles commute in S_n under composition.*

Proof. Let π_1, π_2 two disjoint cycles of nontrivial orbits O_1, O_2. This means that $O_1 \cap O_2 = \varnothing$. We are looking to prove $\pi_1\pi_2(x) = \pi_2\pi_1(x) \forall x \in \mathbf{n}$. To do that, we split the posisble cases:

1. $x \notin O_1 \cup O_2$. Then, $\pi_1\pi_2(x) = \pi_2\pi_1(x) = x$ since x feels no action from either.

2. $x \in O_1 \Rightarrow x \notin O_2$. Then $\pi_1\pi_2(x) = \pi_1(x) = y \in O_1$, and $\pi_2\pi_1(x) = \pi_2(y) = y$.

2. $x \in O_2 \Rightarrow x \notin O_1$. Using a similar argument, the two expressions are equal.

Therefore, if two cycles in S_n are disjoint, then their product is commutative. □

> *Method* Computation of the product of two cycles is done right to left. Consider (12) and (23). We evaluate their product:
>
> $$(12)(23)$$
>
> - ▷ 3 is mapped to 2 by the second cycle, and 2 is mapped to 1 by the first: this means that 3 is mapped to 1.
> - ▷ 2 is mapped to 3 by the second cycle, which is left untouched by the first, meaning 2 is mapped to 3.
> - ▷ 1 is untouched by the second, and mapped to 2 by the first, meaning 1 is mapped to 2.
>
> We see a single apparent cycle within this mapping, meaning that the result is the nontrivial (123).
>
> Consider now (1435)(326): we describe it more concisely, but the idea is the same:
>
> $$6 \to 3 \to 5;\ 2 \to 6;\ 3 \to 2;$$
> $$5 \to 1;\ 4 \to 3;\ 1 \to 4$$
>
> We pick any number to start : (143265).
>
> Last example: consider (1435)(321). Then, we have:
>
> $$1 \to 3 \to 5;\ 2 \to 1 \to 4;\ 3 \to 2$$
> $$4 \to 3;\ 5 \to 1$$
>
> Picking a random start, we try proceeding. If we hit a cycle before we're done, that means that there is still at least a number we haven't hit: we start from it, and keep going. In this case (15)(243).

Theorem 3.25 (Unproven[2])**.** *Any permutation $\sigma \in S_n$ can be written as the product of disjoint cycles, uniquely, up to the order of cycles used.*

[2] Meaning that it will not be proven here. you can find the proof in the teacher's summaries.

Definition 3.26. *The notation of $\sigma \in S_n$ as the product of disjoint cycles is called the cycle notation of σ. The lengths of these disjoint cycles is called the cycle type of σ.*

Proposition. *The cycle notation for $\pi\rho\pi^{-1}$ can be obtained from the cycle notation for ρ by replacing each i in ρ with $\pi(i)$.*

Proof. We have $\pi\rho\pi^{-1}(\pi(x)) = \pi\rho\pi^{-1}\pi(x) = \pi\rho(x)$. Now, we suppose ρ is a cycle:

$$\begin{aligned} \rho &: i \to \rho(i) & \rho &: (i, \rho(i), \rho^2(i), ...) \\ \pi\rho\pi^{-1} &: \pi(i) \to \pi\rho(i) & \pi\rho\pi^{-1} &: (\pi(i), \pi\rho(i), ...) \end{aligned}$$

□

Definition 3.27. *$s \in S_n$ is a transposition if it is a two-cycle, of the form (ij).*

Proposition. *Every k-cycle can be written as the product of $(k-1)$ transpositions.*

Proof. We prove this by induction:

Base: $k = 2$ is trivial, $k = 3$ is unpacked easily as $(123) = (13)(12)$.

Induction: Suppose $(123...k) = (1k)...(13)(12)$. We consider :

$$(1\ k+1)(123...k) \overset{(1)}{=} (123...k\ k+1) \overset{(2)}{=} (1k)...(13)(12)$$

where we obtain (1) by direct computation of the product and (2) by direct application of the induction hypothesis.

□

As a direct result of this, we can say that S_n is generated by the transpositions $\{(ij)\}_{i<j}$: since every permutation is the product of disjoint cycles, and every cycle is the product of transpositions, then every permutation is the product of transpositions, which might not be disjoint.

Theorem 3.28. *The product of an odd number of transposition cannot be equal to the product of an even number of transpositions.*

Proof. The proof of this can be found by considering the number of inversions present after a given permutation. Consider the state after the permutation σ as:

$$s_1 s_2 ... i m_1 m_2 ... m_k ... k e_1 e_2 ...$$

Now, consider $(ij)\sigma$ and any m_k.

▷ If $i < m_k, j < m_k$ or $m_k < i, m_k < j$, then swapping i and j does not contribute to the amount of inversions $\Rightarrow \pm 0$ inversions;

▷ If $i < m_k < j$ or $j < m_k < i$, then swapping i and j changes the inversion state between i and m_k, and between m_k and $j \Rightarrow \pm 2$ inversions.

Additionally, since $i \neq j$, swapping them adds or removes an inversion, as well, in such a way that in total, an additional transposition changes the number of inversions by 1.

Therefore, it is impossible to obtain the same number with $2k$ and $2k'+1$ transpositions, no matter the values of $k, k' \in \mathbb{N}$. □

Definition 3.29. *We use the number of inversions in a given permutation to define its sign as*

$$\operatorname{sgn}\sigma = (-1)^{\operatorname{inv}\sigma} = \begin{cases} 1 & ,\sigma \textit{ has an even number of inversions} \\ -1 & ,\sigma \textit{ has an odd number of inversions} \end{cases}$$

This can easily be shown to verify $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$...: $\operatorname{sgn} : S_n \to \{0, 1\}$ is a group homomorphism! Recalling that the kernel of an homomorphism is a subgroup, we get that

$$A_n = \ker \operatorname{sgn} \triangleleft S_n = \{\sigma \in S_n : \operatorname{inv}\sigma \text{ is even}\}$$

A_n is called the alternating group, and it is of size $n!/2$ (can be shown by Lagrange.)

Proposition. *Let $g, h \in S_n$, consider $ghg^{-1} \in S_n$. If h is the product of disjoint cycles of lengths $\{l_1, l_2, ..., l_n\}$, then ghg^{-1} is the product of disjoint cycles of same length set. Therefore, any element that is the product of disjoint cycles of given lengths can be obtained from another of same lengths by conjugation with another element.*

Proof. Let us consider a single cycle ρ_l of length l. Then, we have that

$$\rho_l = (i_1 i_2 ... i_l) \Rightarrow g\rho_l g^{-1} = (g(i_1)...g(i_l))$$

is a cycle of the same length! This being said, we consider h as the product of disjoint cycles, with their relative lengths:

$$h = \rho_{l_1}...\rho_{l_r} \Rightarrow ghg^{-1} = (g\rho_{l_1}g^{-1})...(g\rho_{l_r}g^{-1}) = \gamma_{l_1}...\gamma l_r$$

where we introduce neutral elements in the product under the form $e = gg^{-1}$. Therefore, we see here that the action is obtained by mapping every element in every cycle of h to the corresponding element in the new cycles γ. □

We can use conjugates to define classes:

Definition 3.30. *The conjugacy class of h, $\{ghg^{-1}\}_{g\in S_n}$ is the set of all elements conjugated to h in S_n. More informally, as we've seen, it's the set of all elements that have the same cycle type as h.*

> *Conclusion* This allows us to more formally define the idea that S_n is the disjoint union of the classes of elements that have same cycle type. These conjugacy classes are in bijection with the partitions of the integer n, of the form:
>
> $$\{\{i_1, ..., i_k\} : n = i_1 + ... + i_k, i_1 \geqslant ... \geqslant i_k\}$$
>
> with $\{i_1, ..., i_k\}$ corresponding to the cycle lengths of the elements in the class. For example, take the partitions of the number 4, matched with the corresponding

> elements in S_4:
>
> $$\{4\} \to \{(1234), (2143), ...\}$$
> $$\{3,1\} \to \{(123), (234), ...\}$$
> $$\{2,2\} \to \{(12)(34), (24)(13), ...\}$$
> $$\{2,1,1\} \to \{(12), (13), (32), ...\}$$
> $$\{1,1,1,1\} \to \{e\}$$

3.4 Actions of groups on sets

3.4.1 Orbits and stabilizers

Definition 3.31. *Let a finite group G, and a finite set E. We say that G acts on E by permutations if one can define the product $g \cdot x$ for any $g \in G, x \in E$ in such a way that*

$$e \cdot x = x \ \forall x \in E$$
$$g_1 g_2 \cdot x = g_1 \cdot (g_2 \cdot x) \ \forall g_1, g_2 \in G, x \in E$$

We also define the orbit of $x \in E$ under the action of G as the subset

$$\text{Orb}_x = \{g \cdot x\}_{g \in G} \subset E$$

Proposition. *Let E a finite set, $x, y \in E$, G a finite group. Then,*

$$\text{Orb}_x = \text{Orb}_y \ \ ou \ \ \text{Orb}_x \cap \text{Orb}_y = \varnothing$$

> Proof of this was done in a problem set, and can be found in the appendix.

Since every element of E belongs to some orbit (at the very least Orb_x), we can write

$$E = \bigcup_{i=0}^{k} \text{Orb}_{x_i}$$

with a set of orbit representatives $\{x_i\}_{i=0}^{k}$. If we consider the case of G acting on itself by conjugation, then the orbit of h in G is the conjugacy class $C_h = \{ghg^{-1}\}_{g \in G}$. This yields, similarly,

$$G = \bigcup_{i=0}^{k} C_{h_i}$$

which is not very interesting group for an abelian group as $C_h = ghg^{-1}{}_{g \in G} = \{gg^{-1}h\}_{g \in G} = \{h\}$, meaning they are all disjoint as they contain a single element.

Definition 3.32. *Let G, E be a finite group and a finite set, respectively, such that G acts on E. The stabilizer of x is the set:*

$$\text{Stab}_x = \{g \in G : g \cdot x = x\}$$

It is a subgroup of G.

Theorem 3.33 (Orbit-Stabilizer Theorem)**.** *Let G be a finite group acting on E a finite set, let $x \in E$. Then,*

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

Proof. Consider the left cosets with respect to $H = \operatorname{Stab}_x$. We have a bijection μ between $gH_{g\in G}$ and Orb_x. We define it as:

$$\mu : gH \mapsto g \cdot x$$

This mapping is surjective, because every g appears in a left coset of H. To prove it is injective, we consider two g, f such that $\mu(gH) = \mu(fH) \in Orb_x$:

$$g \cdot x = f \cdot x \Rightarrow f^{-1}g \cdot x = x \Rightarrow f^{-1}g \in \operatorname{Stab}_x \Rightarrow f^{-1}gH \subset H$$

This means $gH \subset fH$. Symmetrically, we establish $fH \subset gH$, meaning $fH = gH$. This implies μ is injective, meaning that the number of left cosets of H is the same as the number of elements in the orbit of x. Using the formula for the number of left cosets, we get

$$|Orb_x| = \#\text{ of left } H\text{-cosets} = [G : H] = [G : \operatorname{Stab}_x]$$

□

Definition 3.34. *The center of a group is the set of all elements that commute with every $g \in G$:*

$$\begin{aligned} Z(G) &= \{x \in G : g \cdot x = x \cdot g \ \forall g \in G\} \\ &= \{x \in G : g \cdot x \cdot g^{-1} = x \ \forall g \in G\} \end{aligned}$$

It is also the set of all 1-element conjugacy classes of G.

Theorem 3.35. *Using the center, we define the class equation of G, for a finite group G:*

$$|G| = |Z(G)| + \sum_{i=0}^{r} C_{x_i} = |Z(G)| + \sum_{i=0}^{r} [G : G_{x_i}]$$

Where G_{x_i} is the stabilizer of x_i with respect to conjugation.

Proof. We know that G is the disjoint union of its conjugacy classes

$$|G| = \sum_{i=0}^{m} |C_{x_i}| = \underbrace{\sum_{i=0}^{r} |C_{x_i}|}_{\text{conj. cl. of size 1}} + \underbrace{\sum_{j=0}^{s} |C_{x_j}|}_{\text{conj. cl. of size} \neq 1}$$

$$\Rightarrow |G| = |Z(G)| + \sum_{j=0}^{s} |C_{x_j}| = |Z(G)| + \sum_{j=0}^{s} |[G : G_{x_i}]|$$

Since the size of the conjugacy class is the number of left cosets of stabilizer subgroup. □

Application A group of order p^n with p prime has nontrivial center.

Proof.

$$|G| = |Z(G)| + \sum_{j=0}^{s} |[G : G_{x_i}]|$$

where $|G| = p^n$, which is divisible by p, and $[G : G_{x_i}] = |G|/|G_{x_i} = p^n/|G_{x_i}| > 1$, meaning it is divisible by p as well. This implies $|Z(G)|$ is also divisible by p, and since it contains e, it cannot be 0. Therefore, it has to be a nontrivial multiple of p. □

Week 7

3.5 Classifying finite abelian groups

Finite groups split into two categories:

	Abelian	Non-Abelian
Definition	$ab = ba\ \forall a, b \in G$	$\exists a, b \in G : ab \neq ba$
Normal Subgroups	All subgroups	$H \lhd G : gHg^{-1} \in H\ \forall g \in G$
Conjugacy classes	$\lvert C_i\rvert = 1 \forall C_i$	$\exists C_i : \lvert C_i\rvert > 1$
Class equation	$\lvert G\rvert = \lvert Z(G)\rvert$	$\lvert G\rvert = \lvert Z(G)\rvert + \sum_{i<r} \lvert C_i\rvert$
Examples	All cyclic groups C_n	D_n and S_n.

That being said:

Theorem 3.36 (Cauchy)**.** *Let G be a finite group such that a prime p divides its order $|G|$. Then, G has an element of order p.*

Proof. We will prove this in the case where G is an abelian group. The other case is done in a problem set, and can be found in the appendix.

If G is abelian, then let G the counterexample of smallest order. Consider a nontrivial element $g \in G$, such that its order $k = \text{ord}(g)$ is not divisible by p. If it was, we would have $g^{kp} = 1 \Rightarrow g^k$ has order p.

Next, we consider the normal subgroup $\langle g \rangle$, which contains k elements. Looking at the quotient group, we have:

$$G/\langle g \rangle \Rightarrow p \text{ divides } |G/\langle g \rangle| = |G|/\langle g \rangle < |G|$$

This means that there exists an element $h \in G/\langle g \rangle$ such that its order in the quotient group is p. Since $h \in \langle g \rangle$, then $h^p = g^s$ for some s. Let i be the order of g^s in G:

$$(h^p)^k = (g^s)^k = 1$$

meaning that the order of $h^k \in G$ is p, contradicting our assumptions. □

Definition 3.37. *G is simple if it has no proper nontrivial normal subgroup.*

Corollary 3.38. *If G is simple, finite and abelian, then it is isomorphic to a cyclic group of prime order.*

Proof. Consider $|G| = p_1^{n_1}...p_k^{n_k}$. By Cauchy's theorem, there has to be an element of order p_1 within G. Let's call it g. therefore, $\langle g\rangle$ is a normal subgroup of G of size p_1.

$\langle g\rangle$ is a proper subgroup only if there exists an element in G that is not in $\langle g\rangle$, meaning that G is not simple if and only if $|G| > |\langle g\rangle| = p_1$. This means that for G to be simple it has to be of order p_i.

Therefore, $G = \langle g\rangle = C_p$. □

3.5.1 Direct product on groups

Definition 3.39. *Let G, H two groups. Then, their direct product is the set of pairs $G\times H = \{(g,h) : g \in G, h \in H\}$, with the multiplication operation defined such that*

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$$
$$(e_G, e_H) \textit{ is the neutral element}$$
$$(g_1^{-1}, h_1^{-1})(g_1, h_1) = (e_G, e_H)$$

This means that it satisfies the group axioms.

> *Examples* Let's consider the cyclic groups, for now. Let $C_2 = \langle a|a^2 = 1\rangle, C_3 = \langle b|b^3 = 1\rangle$. Then,
>
> $$C_2 \times C_3 = \{(g, h) : g \in C_2, h \in C_3\} = \{(1, 1),(a, 1),(1, b),(1, b^2),(a, b),(a, b^2)\}$$
>
> In this group, $t = (a, b)$ is a generator, and it is of order 6. However, it is not always the case that $C_n \times C_m \simeq C_{mn}$: take $C_2 \times C_2 = \{(1, 1),(a, 1),(1, b),(a, b)\}$, where every nontrivial element has order 2. This means that it cannot be isomorphic to C_4.
>
> To be more general: let $(a, b) \in C_n \times C_m$, such that $\text{ord}(a) = n, \text{ord}(b) = m$. Then, we know that
>
> $$(a, b)^s = (a^s, b^s) = (1, 1) \Rightarrow \text{ord}(a)|s, \text{ord}(b)|s \Rightarrow s = \text{lcm}(n, m)$$

Proposition. *$C_n \times C_m \simeq C_{nm} \Leftrightarrow \gcd(n, m) = 1$. In that case, $C_n \times C_m$ is cyclic.*

Proof. If $\gcd(n, m) = 1 \Leftrightarrow \text{lcm}(n, m) = nm = \text{ord}((a, b))$. This implies $|C_n \times C_m| = nm \Rightarrow C_n \times C_m \simeq C_{nm}$ is cyclic. If $\gcd(n, m) = d > 1$, then $\text{lcm}(n, m) = \frac{nm}{d} = \text{ord}((a, b)) < nm$. Therefore, There is no element of order nm in $C_n \times C_m$, meaning that it is not a cyclic group □

Corollary 3.40. *Let C_n a cyclic group such that $n = p_1^{k_1}...p_r^{k_r}$ is the prime factorization of n. Then,*

$$C_n \simeq C_{p_1^{k_1}} \times ... \times C_{p_r^{k_r}}$$

Proof. $C_n \simeq C_{p_1^{k_1}} \times C_m$, with $m = p_2^{k_2} \times ... \times p_r^{k_r}$, by means of the previous proposition, since $\gcd(p_1^{k_1}, m) = 1$ by definition. This can be repeated on C_m to get the decomposition. □

Properties Some properties of the direct product include:

a $G \times H \simeq H \times G$ through the isomorphism $\phi : (g,h) \mapsto (h,g)$.

b $H, G \subset G \times H$, since $\{(1,h), h \in H\} \simeq H \subset G \times H$.

c $G \times H$ is abelian if and only if H, G are abelian.

d If $G \supset H, K$ such that

- ▷ $H \cap K = \{e\}$
- ▷ $\forall h \in H, k \in K : hk = kh$
- ▷ $HK = \{hk\}_{h \in H, k \in K} = G$

then $G \simeq H \times K$, through the map $\phi : H \times K \to G : \phi(k,h) = hk$.

This induces a theorem to classify finite abelian groups.

Theorem 3.41. *Let G be a finite abelian group. Then, G is isomorphic to a direct product of cyclic groups of prime power orders.*

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

With $\{p_i\}_{i=1}^m$ m primes not necessarily distinct. This presentation is unique up to the order of factors.

Proof. Let $G = \langle g_1, ...g_k | R_1, ..., R_l \rangle$, with $\{g_i\}_{i=1}^k$ the generators and $\{R_i\}_{j=1}^l$ the relations. The relations are of the form:

$$\begin{cases} R_1 : g_1^{n_{11}} g_2^{n_{12}} ... g_k^{n_{1k}} = 1 \\ \quad \vdots \\ R_l : g_1^{n_{l1}} g_2^{n_{l2}} ... g_k^{n_{lk}} = 1 \end{cases}$$

which we can encode in a rectangular, $\mathbb{Z}^{l \times k}$ matrix :

$$\begin{pmatrix} n_{11} & \dots & n_{1k} \\ \vdots & \ddots & \vdots \\ n_{l1} & \dots & n_{lk} \end{pmatrix}$$

On which we can do the following operations without changing the group G:

- ▷ Adding integer multiples of one row to another: since each line evaluates to 1, then adding a line to another does not change its value, but it does change the coefficients.

$$\begin{cases} x^a y^b = 1 \\ x^d = 1 \end{cases} \Rightarrow \begin{pmatrix} a & b \\ d & 0 \end{pmatrix} = \begin{pmatrix} a+d & b \\ d & 0 \end{pmatrix} \Rightarrow \begin{cases} x^{a+d} y^b = x^a x^d y^b = x^a y^b = 1 \\ x^d = 1 \end{cases}$$

- ▷ Adding integer multiples of one column to another: column addition is equivalent to changing the generators in the representation of G.

- ▷ Swapping two columns or rows: equivalent to reordering the generators.

Applying these operations, one can reduce $|n_{11}|$ as much as possible, meaning to the gcd of all elements in the first row and column[3]. Using this we can rewrite the original matrix as :

$$\begin{pmatrix} n_{11} & 0 & \dots & 0 \\ 0 & n_{22} & \dots & n_{2k} \\ \vdots & & \ddots & \vdots \\ 0 & n_{l2} & \dots & n_{lk} \end{pmatrix}$$

repeating on submatrices, we end up on the following matrix:

$$\begin{pmatrix} n_{11} & 0 & \dots & 0 \\ 0 & n_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & n_{rr} \end{pmatrix}, r = \min l, k$$

which defines the same group, as

$$G = \langle g_1 ... g_3 | g_1^{n_{11}} = 1, ..., g_r^{n_{rr}} = 1 \rangle$$

which means that $G_i = \langle g_i \rangle$ are cyclic subgroups of G.

Moreover, for any $i \neq j$, $G_i \cap G_j = \{1\}$ if $i \neq j$, $g_i g_j = g_j g_i$ since G is abelian, and $\{h_1 ... h_r\} = G$, meaning that by property d,

$$G \simeq C_{n_{11}} \times C_{n_{22}} \times ... \times C_{n_{rr}}$$

Each $C_{n_{ii}}$ can be rewritten as its prime factorization, as we know. Therefore, expanding it out:

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

Which is what we wanted to prove. □

Corollary 3.42. *If $|G| = p^n$, with p a prime, then G is the direct product of cyclic groups*

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

such that $p^{i_1 + i_2 + ... + i_k} = p^n$. Therefore, all possible abelian groups of order p^n are in bijection with the partitions of n.

> *Example* Take $p = 2, n = 3, G$ abelian:
>
> $$|G| = 8 = 2^3; \text{Partitions of 3} : (3), (2,1), (1,1,1)$$
>
> This is therefore isomorphic to $G_1 \simeq C_{2^3}, G_2 \simeq C_{2^2} \times C_2, G_3, G_3 \simeq C_2 \times C_2 \times C_2$, which are all pairwise nonisomorphic.

.

Definition 3.43. *The numbers $(p_1^{n_1}, ..., p_m^{n_m})$ are called the elementary divisors of G.*

[3] This is due to the fact that all of the operations end up looking like repeated addition and subtraction, which are multiplication and division. The only way to minimize an element is therefore by ensuring it divides every other element. I think? idk it's a little handwavy but it works

Theorem 3.44. *A finite abelian group $G \simeq C_{d_1} \times ... \times C_{d_n}$, with C_{d_i} cyclic for any i, and $d_n | d_{n-1}, ..., d_2 | d_1$, $|G| = d_1 d_2 .. d_n$. The numbers $(d_1, ..., d_n)$ are called the invariant factors of G. The determine it uniquely.*

Method The algorithm to determine all abelian groups of a given order is as follows:

(i). Decompose $|G| = n = \prod_j p_j^{k_j}$ into its prime factors, and find partitions for each power. For each partition of k_i, there is a unique group of order $p_i^{k_i}$:

$$k_i = a_1 + ... + a_i \Rightarrow = C_{p_i^{a_1}} \times C_{p_i^{a_i}}$$

The possible groups are the direct products of all possible groups of orders $p_i^{k_i}$. Therefore, we get G in the form of a direct product of cyclic groups of prime power orders, which we call the elementary divisors of G.

(ii). To find the decomposition of G in terms of the invariant factors, for each group above we write $C_{p_i^{a_i}}$ with the same p_i in the same line, in decreasing order of a_i. Then, each column gives a direct product of cyclic groups with coprime orders $\Rightarrow$ the direct product of each column is cyclic!

The orders of these groups $(d_1, d_2, ..., d_n)$ are called the invariant factors of G. By construction, $d_n | d_{n-1} | ... | d_1$.

Therefore, it is possible to determine an abelian group in two different representations.

Example For example, we can consider $|G| = 72 = 2^2 3^2$. Then, $p_1 = 2, p_2 = 3$, and we have the following partitions of the exponents:

$$\begin{aligned} 3 &: (3), (2,1), (1,1,1) \\ 2 &: (2), (1,1) \end{aligned}$$

Therefore, we consider the following splits, using products of vertically aligned items[4]:

$C_{2^3} \times$	$C_{2^3} \times$	$C_{2^2} \times C_2 \times$	$C_{2^2} \times C_2 \times$	$C_2 \times C_2 \times C_2 \times$	$C_2 \times C_2 \times C_2$
C_{3^2}	$C_3 \times C_3$	C_{3^2}	$C_3 \times C_3$	C_{3^2}	$C_3 \times C_3$
C_{72}	$C_{24} \times C_3$	$C_{36} \times C_2$	$C_{12} \times C_6$	$C_{18} \times C_2 \times C_2$	$C_6 \times C_6 \times C_2$

The elementary divisors correspond to the partitions of the powers, so they are :

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

and the invariant factors are given by the powers of this awful construction, so

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

[4] There was, physically, no better way of having this fit together. Sorry.

Chapter 4

Rings and fields

Week 8

4.1 One to rule them all

Definition 4.1. *A ring is a set A with two operations defined on it: $+$ and $\cdot$, in such a way that*

(i). *A is an abelian group with respect to $+$, containing a neutral element 0.*

(ii). *$\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, et il $\exists 1 \in A : 1 \cdot a = a \cdot 1$.*

(iii). *$\cdot$ is both left- and right-distributive over $+$: $a \cdot (b + c) = ab + ac, (a + b) \cdot c = ac + bc$.*

> *Examples* Let us consider some examples:
>
> ▷ $\mathbb{Z} : \langle +, \cdot, 0, 1 \rangle$ is a ring! Though it doesn't contain any multiplicative inverses, it fits the definitions nicely.
>
> ▷ $A = \mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2}, a, b \in \mathbb{Z}\}$ contains 0 and 1. Additionally:
>
> $$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in A$$
> $$-a - b\sqrt{2} \in A$$
> $$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + \sqrt{2}(ad + bc) \in A$$
>
> ▷ $\mathbb{Q}[\sqrt{2}]$ is a ring. Proof of this is left as an exercice to the reader.

In this course, we will consider only commutative rings, such that $ab = ba \forall a, b \in A$.

Definition 4.2. *$a \in A$ is a zero divisor if there exists an $0 \neq x \in A$ such that $ax = 0$.*

Most rings we are used to do not have any nontrivial zero divisors. Let us consider another one:

> *Example* Consider:
>
> $$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], ..., [n-1]\}$$
>
> It is isomorphic to the cyclic group of order n, meaning it is an abelian group

> with respect to addition. $\cdot$ is associative, and $[1]$ is its neutral element wrt multiplication.
>
> Consider now an element $[a] \in \mathbb{Z}/n\mathbb{Z}$.
>
> ▷ If $\gcd(a, n) = d > 1$, then we can write
>
> $$[a] \cdot \left[\frac{n}{d}\right] = [1]$$
>
> meaning that a is a nontrivial zero divisor of the ring.
>
> ▷ If a, n are coprime, then by Bezout's theorem
>
> $$\exists x, y : ax + ny = 1 \Rightarrow [a][x] = [1] \Rightarrow [a]^{-1} = [x]$$
>
> Additionally, if we consider $[b] : [b] \cdot [a] = 0$, then we have
>
> $$[b] \cdot [a] = [0] \Rightarrow [b] \cdot [a] \cdot [x] = [0] \Rightarrow [b] \cdot [1] = [0] \Rightarrow [b] = [0]$$
>
> Meaning that $[a]$ cannot be a zero divisor of the ring.
>
> This means that an element of $\mathbb{Z}/n\mathbb{Z}$ is either invertible, or a zero divisor.

Definition 4.3. *A ring that has no nontrivial zero divisors is called an integral domain.*

Definition 4.4. *A commutative ring where all nonzero elements have a multiplicative inverse is called a field.* $\forall 0 \neq a \in A \exists a^{-1} \in A : aa^{-1} = a^{-1}a = 1$

Corollary 4.5. *$\mathbb{Z}/n\mathbb{Z}$ either has nontrivial zero divisors ($\Leftrightarrow n$ is not prime) or it is a field and an integral domain ($\Leftrightarrow n = p$ for some prime p).*

Proof. If it has no nontrivial zero divisors, that means that there is no $[a] \in \{[1], ..., [n-1]\}$ such that $\gcd(a, n) > 1$. Therefore, n has no divisors other than itself and 1, and it must be a prime p by definition. If that's the case, then $\forall [b] \neq 0, \gcd(b, p) = 1 \Rightarrow [b]$ has a multiplicative inverse, meaning that $\mathbb{Z}/n\mathbb{Z}$ is a field. □

Proposition. *A field is an integral domain. An invertible element is not a zero divisor.*

Proof. Suppose $ab = 0$ in a field A such that $a \neq 0$. This means that there exists a $a^{-1} \in A$ such that $aa^{-1} = 1$. This means that :

$$\begin{aligned} ab = 0 &\Leftrightarrow a^{-1}ab = a^{-1} \cdot 0 \tag{4.1} \\ &\Leftrightarrow 1 \cdot b = 0 \tag{4.2} \\ &\Leftrightarrow b = 0 \tag{4.3} \end{aligned}$$

meaning a cannot be a zero divisor. This means that if all non-zero elements in A are invertible, then A cannot have nontrivial zero divisors. This is equivalent to saying that if A is a field, then it is an integral domain, proving our proposition. □

> *Remark* The converse isn't true! $\mathbb{Z}$ is an integral domain, but $2 \in \mathbb{Z}$ does not have a multiplicative inverse.

This allows the following characterization:

$$\text{Fields} \subset \text{Integral Domains} \subset \text{Commutative Rings}$$

And for the following statements on $\mathbb{Z}/n\mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} \text{ integral domain} \Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ field} \Leftrightarrow n = p \text{ prime}$$

4.2 Less than ideal

Definition 4.6. *Let A be a commutative ring. $I \subset A$ is an ideal if it has the following properties:*

- ▷ *it is a subgroup with respect to $+$, i.e: it contains 0, $-a$ for any $a \in I$, and it is closed wrt $+$.*
- ▷ $\forall x \in A, a \in I : x \cdot a \in I$.

> *Examples* Let's have a look at some examples
>
> - ▷ $\{0\} \subset A, A \subset A$ are ideals for any commutative ring A. That is not very interesting.
> - ▷ Consider $\mathbb{Z}$. Then, $2\mathbb{Z} = \{2a, a \in \mathbb{Z}\}$ is an ideal! It's easy to verify it is a subgroup for $+$, and we have that, for any $x \in \mathbb{Z}, 2a \cdot x \in 2\mathbb{Z}$. This is true for any $d \in \mathbb{Z}$.

Definition 4.7. *We say that an ideal $I \subset A$ is proper if $I \neq A$, and nontrivial if $I \neq 0$.*

> *Properties* Let $I, J \subset A$ two ideals. Then:
>
> (i) if $1 \in I$, then $I = A$.
> *This is due to the properties of ideals: $\forall x \in A, 1 \cdot x \in I \Rightarrow x \in I \Rightarrow I = A$*
>
> (ii) $I \cap J$ is an ideal
> *Again, easy to verify applying properties of ideals: let $x, y \in I \cap J$.*
>
> $$\begin{gathered} x + y \in I, J \Rightarrow x + y \in I \cap J \\ -x \in I, J \Rightarrow -x \in I \cap J \\ 0 \in I, J \Rightarrow 0 \in I \cap J \end{gathered}$$
>
> *Meaning it is a subgroup. Also, for any $a \in A$, we have that $ax \in I, ax \in J$, which means $ax \in I \cap J$. This makes it an ideal!*
>
> (iii) $I + J = \{i + j\}_{i \in I, j \in J}$ is an ideal.
>
> (iv) $I \cdot J = \{\sum_{i=1}^{k} x_i y_i\}_{x_i \in I, y_i \in J}$ is an ideal.[1]
>
> (v) $I \cup J$ is not necessarily an ideal
> *More often than not, it is not an additive subgroup: consider $I = 2\mathbb{Z}$, $J = 3\mathbb{Z}$*

We can verify some fun properties on integer ideals. Let $A = \mathbb{Z}, I = 6\mathbb{Z}, J = 10\mathbb{Z}$. Then:

[1] Proofs to (iii) and (iv) are left as exercice to the reader, as they are similar to that of (ii).

▷ **Intersection:** We have:

$$\begin{aligned} I \cap J &= \{z \in \mathbb{Z} : z = 6n \wedge z = 10m, n, m \in \mathbb{Z}\} \\ &= \{\text{common multiples of 6 and 10}\} \\ &= \{\text{all multiples of} \operatorname{lcm}(6,10) = 30\} \\ &= 30\mathbb{Z} \end{aligned}$$

▷ **Addition:** We have:

$$\begin{aligned} I + J &= \{6n + 10m\}_{n,m \in \mathbb{Z}} \\ &= \{\gcd(6,10)k, k \in \mathbb{Z}\} && \text{[By Bezout]} \\ &= 2\mathbb{Z} \end{aligned}$$

▷ **Product:** We have:

$$\begin{aligned} I \cdot J &= \left\{ \sum_{i=1}^{k} 6x_i \cdot 10y_i, x_i, y_i \in \mathbb{Z} \right\} \\ &= \left\{ 60 \sum_{i=1}^{k} x_i y_i, x_i, y_i \in \mathbb{Z} \right\} \\ &= 60\mathbb{Z} \end{aligned}$$

From which we can conclude!

Theorem 4.8. *Let $I = n\mathbb{Z}, J = m\mathbb{Z}$ two ideals of $\mathbb{Z}$. Then:*

$$\begin{aligned} I \cap J &= \operatorname{lcm}(n,m)\mathbb{Z} \\ I + J &= \gcd(n,m)\mathbb{Z} \\ I \cdot J &= (n \cdot m)\mathbb{Z} \end{aligned}$$

> *Example* Consider $A = \mathbb{R}[x]$ all polynomials on one variable with real coefficients[2]. This forms a ring as is trivial to verify. Then, we consider the following:
>
> $$\begin{aligned} I &= \{(x+5)f(x), f(x) \in \mathbb{R}[x]\} \\ J &= \{(x^2+2)f(x), f(x) \in \mathbb{R}[x]\} \end{aligned}$$
>
> which are comprised of all polynomials divisible by $(x+5)$ and (x^2+2), respectively. Then, we have:
>
> $$\begin{aligned} I \cap J &= \{(x+5)(x^2+2)f(x), f(x) \in \mathbb{R}[x]\} \\ I \cdot J &= \left\{ \sum_{i=0}^{k} (x+5)f_i(x) \cdot (x^2+2)g_i(x) \right\} = \{(x+5)(x^2+2)f(x)\} \\ I + J &= \{(x+5)f(x) + (x^2+2)g(x)\} \end{aligned}$$
>
> We can find $f(x), g(x)$ such that $(x+5)f(x) + (x^2+2)g(x) = 1 \in \mathbb{R}[x]$ (constant

> polynomial of value 1). For example, take
>
> $$(x+5)(x-5)\left(\frac{-1}{27}\right) - (x^2+2)\left(\frac{-1}{27}\right) = (x^2-25-x^2-2)\left(\frac{-1}{27}\right) = 1$$
>
> Can we do that for any pair of polynomials in $\mathbb{R}[x]$?

Week 9

Definition 4.9. *Let $S \subset A$. Let I be the minimal ideal containing S. Then, we denote $I = (S)$ the ideal generated by the set S. It means:*

$$(S) = \left\{ \sum_i s_i a \right\}_{s_i \in S, a \in A}$$

I is called principal if $I = (x) = \{xa, x \in I\}_{a \in A}$ is generated by a single element.

> *Examples* A and $\{0\}$ are principal, being generated by 1 and 0 respectively. Additionally, $n\mathbb{Z} = (n)$ is principal.

Proposition. *A is a field $\Leftrightarrow$ $A, \{0\}$ are the only ideals in A*

Proof. We prove both directions separately:

- $\Rightarrow$ A is a field, consider an ideal I that isn't $\{0\}$ and an element $a \in I$, which is not 0. Since we're in a field, and it is non-zero, there exists $a^{-1} \in A$. By definition of an ideal, we have that $aa^{-1} \in I \Rightarrow 1 \in I \Rightarrow I = A$.
- $\Leftarrow$ Let A be a ring such that A, $\{0\}$ are its only ideals. Therefore, we consider an $0 \neq a \in A$, and the ideal it generates. Since $a \neq 0$,we know that it must generate A, and that there must exist a $y \in A$ such that $ya = 1$, meaning that $y = a^{-1}$ by definition, and A is a field as a consequence of its existence.

□

4.3 Quotient rings

Definition 4.10. *An equivalence relation $\sim$ on a set E is a relation such that for any $a, b, c \in E$, we have:*

- ▷ *$a \sim a$, meaning it is reflexive*
- ▷ *$a \sim b \Leftrightarrow b \sim a$, meaning it is symmetric*
- ▷ *$a \sim b, b \sim c \Rightarrow a \sim c$, meaning it is transitive*

A congruence relation $\sim$ on a commutative ring A is an equivalence relation such that for any $a, b, c, d \in A$

$$\begin{cases} a \sim b \\ c \sim d \end{cases} \Rightarrow \begin{cases} a + c \sim b + d \\ ac \sim bd \end{cases}$$

[2] If you want to see me get pedantic about notation for life half a page, go look at appendix C.

Proposition. *If $I \subset A$ is an ideal, then the relation :*

$$a \sim b \Leftrightarrow (b-a) \in I$$

is an equivalence relation, and if it is a congruence relation, then the set $I = \{a \in A : a \sim 0\}$ is an ideal in A.

Proof. We first check all of the properties of an equivalence relation. We have:

- ▷ Any ideal contains the 0 element, meaning that $(a-a) \in I \Rightarrow a \sim a$. This makes $\sim$ reflexive.
- ▷ I must be an additive subgroup of A. Therefore, it must contain $b-a$ and $-(b-a) = a-b$, meaning that if $a \sim b$, then $b \sim a$. $\sim$ is therefore symmetric.
- ▷ Consider $a, b, c \in A$ such that $a \sim b, b \sim c$. Therefore, this means that $c-b \in I, b-a \in I$. Now, consider that $c-a = (c-b)+(b-a)$ is the sum of two elements of I: since I is an additive subgroup, that must mean that $c-a \in I$, meaning $a \sim c$. Therefore $\sim$ is transitive.

Now that we have checked the properties of an equivalence relation, we must check those for a congruence relationship: consider $a \sim b, c \sim d$ in A. Then:

$$\begin{cases} (b+d)-(a+c) = (b-a)+(d-c) \in I \\ bd-ac = (b-a)(d-c) = e(b-a) \in I \end{cases}$$

Where the last step is motivated by the fact that $e = d-c$ is an element of A, and by the definition of an ideal. This concludes the proof of the first part of the theorem.

Then, consider $a \sim 0, b \sim 0$. We have: $a+b \sim 0, 0 \sim 0, -a \sim 0$, which completes the subgroup requirement, as well as $x \sim x \Rightarrow a \cdot x \sim 0 \cdot x \Rightarrow a \cdot x \sim 0 \Rightarrow \{a \in A : a \sim 0\}$ is an ideal! □

Proposition. *Let A be a commutative ring, $\sim$ a congruence relation over A such that $1 \not\sim 0$. Then, the set of congruence classes $A/\{x \in A : x \sim 0\} := A/\sim$ is a commutative ring.*

Proof. Notate $\overline{a} = \{x \in A : x \sim a\}$. Define $\overline{a} + \overline{b} = \overline{a+b}$, $\overline{a} \cdot \overline{b} = \overline{ab}$. These are well-defined thanks to the properties on $\sim$. Most importantly, $\overline{1} \in A/\sim$. □

> *Example* Consider the ring of polynomials with real coefficients $\mathbb{R}[x]$. Let $I = \langle(x^2-4)\rangle$, and consider the commutative ring $B = \mathbb{R}[x]/I$. Within it, we have:
>
> $$\overline{(x+2)} \cdot \overline{(x+1)} = \overline{x^2+3x+2} = \overline{x^2+3x+2} - \overline{x^2-4} = \overline{3x+6}$$
>
> where the step in red is justified as a way to find the remainder of the function by the defined congruence relation. Another example:
>
> $$\overline{x} \cdot \overline{x} = \overline{x^2} = \overline{4}$$
>
> through a similar process as earlier. One can also look for the zero divisors (recall definition 4.2) within this ring. Consider:
>
> $$\overline{(x+2)(x-2)} = \overline{(x^2-4)} = \overline{0}$$

> since $(x+2), (x-2)$ are non-zero, but their product is, this means that they are zero divisors, and that B is not an integral domain.
>
> As an exercice, one can show that any element in B can be written under the form $\overline{ax+b}, a, b \in \mathbb{R}$.

Definition 4.11. *Recall the definition of a principal ideal (Definition 4.9). A commutative ring where every ideal is principal is called a principal ring. An integral domain where every ideal is principal is called a principal integral domain (PID).*

This means that any field is a PID, since it only has two ideals, and they are both principal (A is generated by 1, 0 is generated by 0).

Proposition. *$\mathbb{Z}$ is a PID.*

Proof. If $I = \{0\}$, then $I = (0)$. Suppose then that $I \neq \{0\}$. Therefore, there exists an $0 \neq a \in I$, such that $a \in I, -a \in I \Rightarrow |a| \in I$. Consider d the smallest positive element in I. Then, for any $n \in I$, by euclidean division, $n = kd + r, 0 \leqslant r \leqslant d - 1 \Rightarrow r \in I$. Since d is the smallest positive integer in I, then it must be the case that $r = 0$, by definition of the ideal. Therefore, $I = (d)$. □

4.4 Ring homomorphisms

Definition 4.12. *Let A, B two commutative rings. Then, $f : A \to B$ is a ring homomorphism if, for $a, b \in A$ and well-defined operations*

$$f(a+b) = f(a) + f(b)$$
$$f(ab) = f(a)f(b)$$
$$f(1_A) = 1_B$$

Proposition. *Let $f : A \to B$ be a ring homomorphism. Then,* $\ker f$ *is an ideal, and* $\operatorname{im} f$ *is a subring.*

Definition 4.13. *A subring is a subset of a ring that is a ring with respect to the same operations and constants as the superset.*

> *Examples* Consider C an arbitrary subring of $\mathbb{Z}$. Then, it must contain $0, 1$, and be defined over the same $+, \cdot$. Therefore, since it must be closed under addition, it must contain -1, as well as
>
> $$\underbrace{1 + 1 + ... + 1}_{n}$$
>
> for any $n \in \mathbb{Z}$. This means that $C = \mathbb{Z}$.
>
> For a more interesting example, take a ring homomorphism $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, with $n, m, \in \mathbb{N}$. We can make a few observations about it.
>
> ▷ f cannot map to a proper subring of $\mathbb{Z}/m\mathbb{Z}$. We know that $[1]_m \in \operatorname{im} f$,

> meaning that
>
> $$\underbrace{[1]_m + ... + [1]_m}_{k \text{ times}} = [k]_m \in \operatorname{im} f \forall k < m$$
>
> Therefore, $\operatorname{im} f = \mathbb{Z}/m\mathbb{Z}$.
>
> - ▷ $f([n]_n) = f([0]_n) = [0]_m$, but also, $f([n]_n) = f([1]_n \cdot n) = [1]_m \cdot n = [n]_m$, meaning that $[n]_m = 0 \Rightarrow n \equiv 0 (\operatorname{mod} m)$, which implies $m|n$.
> - ▷ Additionally, f is such that $[1]_n \overset{f}{\mapsto} [1]_m$, meaning that $[k]_n \overset{f}{\mapsto} [k]_m$ for any k. This implies that f is unique.
>
> In conclusion:
>
> **Proposition.** *There exists a ring homomorphism $f : \mathbb{Z}/n\mathbb{Z} \to \mathbf{Z}/m\mathbb{Z}$ if and only if $m|n$. In that case, then f is unique, and its image is equal to $\mathbb{Z}/m\mathbb{Z}$.*

Now for A Quick Tour of This Land's Characteristic Rings.

Let A a ring. There exists only a single ring homomorphism $\tau : \mathbb{Z} \to A$. This is due to the fact that $\tau(0) = 0, \tau(1) = 1_A \Rightarrow \tau(k) = \tau(1 + 1 + ... + 1) = 1_A + ... + 1_A = k \cdot 1_A \in A$. Therefore, the mapping is uniquely determined, and $\tau(n \cdot k) = \tau(n) \cdot \tau(k)$.

There are two possibilities to characterize the kernel of this transformation, either $\ker \tau = (0)$, or $\ker \tau = (d)$ with $d \geqslant 2$: in short, it cannot be 1.[3]. Let us formalize this:

Definition 4.14. *Let A be a ring, τ the unique homomorphism from the integers to it. Then, the characteristic of A is*

$$c_A = \begin{cases} 0 & , \ker \tau = 0 \\ d & , \ker \tau = d \geqslant 2 \end{cases}$$

> *Examples* The characteristic of the real numbers is 0, since the field homomorphism:
>
> $$\begin{aligned} \tau : \mathbb{Z} &\to \mathbb{R} \\ n &\mapsto n \end{aligned}$$
>
> maps 0 (and only 0) to 0. Therefore, its kernel is $\{0\}$, and $C_{\mathbb{R}} = 0$. A similar argument gives us that $C_{\mathbb{Z}} = 0$, and we can consider
>
> $$\begin{aligned} \tau : \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ k &\mapsto [k]_n \end{aligned}$$
>
> Which maps every multiple of n to 0. Therefore, $\ker \tau = (n)$, and $C_{\mathbb{Z}/n\mathbb{Z}} = 0$.

Proposition. *A is an integral domain $\Rightarrow c_A = 0$ or $c_A = p$ a prime.*

Proof. Suppose $c_A = m \cdot k$ for $m, k > 1$. Then, $\tau(m) \cdot \tau(k) = \tau(m \cdot k) = 0 \in A$, meaning that there are two nontrivial zero divisors in A. □

This holds for fields as well, since they are integral domains necessarily.

[3] This makes sense in accordance to the definition of a ring homomorphism: $\tau(1) \neq 0$ for any τ

Definition 4.15. *Let A, B be two rings. Then, the* direct product *is given by $A \times B = \{(a,b), a \in A, b \in B\}$. It has ring structure, with neutral elements $(0_A, 0_B), (1_A, 1_B)$, and component wise operations.*

> *Examples* Consider the ring $A = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, and let us compute its characteristic. We first describe the homomorphism:
>
> $$\tau : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$
>
> such that $\tau(1) = ([1]_n, [1]_m)$. Therefore, we know that
>
> $$\tau(k) = ([k]_n, [k]_m) = ([0]_n, [0]_m) \Leftrightarrow k \equiv 0 \pmod{n} \wedge k \equiv 0 \pmod{m}$$
>
> The characteristic is the smallest element of such form: $c_A = \text{lcm}(n, m)$.
>
> This can be generalized to the characteristic of any product of two rings A, B: $c_{A\times B} = \text{lcm}(c_A, c_B)$. This lets us construct fields of prime characteristics, but that aren't fields:
>
> $$A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$
>
> has prime characteristic $c_A = \text{lcm}(p, p) = p$, but has non-trivial zero divisors as well:
>
> $$(0, 1) \cdot (0, 1) = (0, 0)$$
>
> Which means it is not an integral domain.

> *Method* Let's compute more characteristics!
>
> Let $B = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then, using $\tau(k) = (k, [k]_n)$, we can see that the kernel of τ must be equal to $\{0\}$, since no other term will leave a 0 in the first spot. Since $\ker \tau = (0)$, then $c_B = 0$.
>
> Let $D = \mathbb{Z}/n\mathbb{Z}[x]$ be the ring of polynomials over x with coefficients in $\mathbb{Z}/n\mathbb{Z}$. The homomorphism must be such that $\tau(1) = [1]_n$, meaning that $\tau(k) = [k]_n = 0 \Leftrightarrow n|k$. This means that $\ker \tau = (n)$, meaning that $c_D = n$.

4.5 The Chinese Remainder Theorem

Week 10

Theorem 4.16 (Chinese Remainder Theorem)**.** *Let A be a commutative ring, $I, J \subset A$ two ideals such that $I + J = A$. Then, there exists a ring isomorphism*[4]

$$f : A/(I \cap J) \xrightarrow{\sim} A/I \times A/J$$
$$f([x]_{I\cap J}) \mapsto ([x]_I, [x]_J)$$

Proof. We will first prove that f is a homomorphism, before proving its bijectivity.

(1) f is a ring homomorphism. This can be shown by checking ring operations on it, which is easy and tedious after pointing out that we map 1 to $([1]_I, [1]_J)$.

[4] A ring isomorphism is a ring homomorphism that is bijective (inversible).

(2) We want to show that f is surjective by showing that for any $a_1, a_2 \in A$, there exists an $a \in A$ such that $a \equiv a_1 (\operatorname{mod} I)$ and $a \equiv a_2 (\operatorname{mod} J)$. Since $I + J = A$, then we can write, for $i \in I, j \in J$:

$$a_1 - a_2 = -i + j \Leftrightarrow a_1 + i = a_2 + j := a \in A$$

which by construction gives us an $a \in A$ with the properties we want. This implies that for any $x \in A$, we can define $f(x) = ([x]_I, [x]_J)$, which is surjective.

(3) To prove that f is injective, We consider another b such that $b \equiv a_1 (\operatorname{mod} I) \equiv a_2 (\operatorname{mod} J)$. Then, there exist i', j' such that $b = a_1 + i' = a_2 + j'$, meaning $b - a = i - i' = j - j' \in I \cap J$. This is means that it has reminder 0 in A[5], meaning that our map is injective.

Therefore, f is surjective and injective: therefore, is a bijective ring homomorphism, and by definition is a ring isomorphism. □

Over $\mathbb{Z}$, this motivates a new corollary.

Corollary 4.17. *Let $n, m \in \mathbb{Z}$ coprime. Then, for any $a_1, a_2 \in \mathbb{Z}$, there exists an a such that it is equivalent to a_1 mod n, and a_2 mod m. The set of solutions is given by $\{a + nm\mathbb{Z}\}$.*

Proof. By Bezout's theorem, there exist $x, y \in \mathbb{Z}$ such that

$$xm + yn = 1 \Rightarrow (m) + (n) = \mathbb{Z}$$

This allows us to apply the CRT directly, showing that the a we are looking for exists. The set of solutions is therefore equal to $\{a + nm\mathbb{Z}\}$, applying Theorem 4.8 to $I \cap J$ after recognizing that $\gcd(n, m) = 1 \Rightarrow \operatorname{lcm}(n, m) = nm$. □

> *Some more* We can also generalize this result over more than two congruences! For $d_1, ..., d_r \in \mathbb{Z}$ that are pairwise coprime. Then, for any set of congruences $a_1, ..., a_r \in \mathbb{Z}$, there exists an $a \in \mathbb{Z}$ such that
>
> $$\begin{cases} a \equiv a_1 \pmod{d_1} \\ a \equiv a_2 \pmod{d_2} \\ ... \\ a \equiv a_r \pmod{d_r} \end{cases}$$
>
> This choice of a is unique up to the ideal $(d_1 ... d_r)$, meaning that the set of solutions is given by $\{a + (d_1 ... d_r)\mathbb{Z}\}$.
>
> Proof of this can be done by induction over r.

Proposition. *If $A \simeq B$ are isomorphic, then their groups of units are isomorphic, as well. The units of a ring are its invertible elements with respect to multiplication. We notate this $A^* \simeq B^*$.*

[5] This is handwavy, but I mean. It's not any less clear than the proof in the course, and it's the best explanation I've found. I'll update the document once I find better.

As a corollary to this, one can verify the formula that $\varphi(nm) = \varphi(n)\varphi(m)$ when n and m are equal!. In fact, by CRT, we can write

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

which means that their groups of units are isomorphic as well. Additionally, we have that

$$(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

Therefore, we get :

$$\varphi(nm) = |\,(\mathbb{Z}/nm\mathbb{Z})^*\,| = |\,(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^*\,| = |\,(\mathbb{Z}/n\mathbb{Z})^*\,||\,(\mathbb{Z}/m\mathbb{Z})^*\,| = \varphi(n)\varphi(m)$$

4.6 Polynomial Rings

Definition 4.18. *Let A be a commutative ring. Then, we define the ring of polynomials on A as*

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

with the usual polynomial addition and multiplication. Since it contains 0 and 1, it is a well defined ring, and it is commutative by definition of addition and multiplication.

Definition 4.19. *If $f \in A[x]$ is nonzero, then we define the degree of $f(x) = a_0 + \ldots + a_n x^n$ as the largest n such that $a_n \neq 0$. We then write $\deg(f) = n$. If $f = 0$, then $\deg(f) = -\infty$ by convention*[6].

Proposition. *Let f, g be two polynomials. Then,*

$$\deg(f+g) \leqslant \max\{\deg f, \deg g\}$$
$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

Proof. Direct computation. □

Proposition. *Let A be an integral domain. Then $A[x]$ is an integral domain, and its units are the units of A.*

Proof. We can first check to see whether or not it is an integral domain. To do this, consider two polynomials such that their product is 0:

$$f \cdot g = 0 \Leftrightarrow \deg f + \deg g = -\infty$$
$$\Rightarrow \deg f = -\infty \text{ or } \deg g = -\infty$$
$$\Rightarrow f = 0 \text{ or } g = 0$$

Then, we consider the units:

$$f \cdot g = 1 \Leftrightarrow \deg f + \deg g = 0$$
$$\Rightarrow f = a_0, g = b_0 \in A : a_0 \cdot b_0 = 1$$

□

[6] To convince yourself of why, consider the (intuitive) property of two polynomials P, Q: $\deg(P \cdot Q) = \deg P + \deg Q$. In this case, since $0 \cdot P = 0$, we want $\deg(P \cdot 0) = \deg P + \deg 0 = \deg 0$, which is only matched if $\deg 0 = -\infty$.

Theorem 4.20 (Euclidean division in a polynomial ring)**.** *Let F a field, $f, d \in F[x]$ of degree $\geqslant 1$. Then, there exist $q, r \in F[x]$ such that*

$$f(x) = d(x)q(x) + r(x)$$

and either $r = 0$ or $\deg r < \deg d$.

Proof. There are multiple cases:

- ▷ If $\deg f < \deg q$, then $f(x) = 0 \cdot d(x) + f(x)$, meaning $f = r$.
- ▷ If $\deg f >= \deg q$, then we have:

  $$f(x) = a_0 + ... + a_m x^m$$
  $$d(x) = b_0 + ... + b_n x^n, n \leqslant m$$

  meaning that we can rewrite

  $$f(x) - d(x) \cdot \frac{a_m}{b_n} x^{m-n} = p_1(x)$$

  such that p_1 is of smaller degree than f. If $\deg p_1 \geqslant \deg d$, repeat:

  $$f(x) - d(x) \cdot \frac{a_m}{b_n} x^{m-n} \cdot \frac{a_{m-1}}{b_n} x^{m-n-1} \cdot ...$$

  Until you end up at a form such that $\deg(f - dq) < \deg d$. Since the degree is strictly decreasing at every step, this is guaranteed to happen at some point, and therefore, the process terminates.

□

> *Method* This is much easier to do as a polynomial long division! I'll put resources here on how to do it and how to do it fast, since there is literally no cool way to typeset them^0.

Definition 4.21. *A commutative ring A is called an Euclidean domain if it is an integral domain and there exists a function $\nu : A \smallsetminus \{0\} \to \mathbb{N}$ such that $\forall a, b \in A, b \neq 0\ \exists q, r \in A$: $a = qb + r$ and either $r = 0$ or $\nu(r) < \nu(b)$.*

> *Examples* Let us consider some examples:
>
> (1) $\mathbb{Z}$ with $\nu(n) = |n|$.
>
> (2) Any field: $a = bq + 0$.
>
> (3) $\mathbb{F}[x]$ over a field $\mathbb{F}[x]$, with $\nu(f) = \deg(f)$.

Proposition. *A Euclidean domain is a PID.*

Proof. Let E a Euclidean domain, $I \subset E$ an ideal within E. If $I = \{0\}$, then $I = (0)$. If it isn't, then consider an element d within it, non-zero, such that $\nu(d)$ is minimal over I. Suppose $a \in I$. Therefore, there exists q, r such that $a = qd + r$. Since r is I, then either $\nu(r) < \nu(d)$, which is impossible, since it contradicts our definition of d, or $r = 0$. Therefore, $r = 0$, meaning $a = qd$, meaning $I = (d)$ which makes E a PID. □

Theorem 4.22 (Unproven)**.** *If F is a field, then $F[x]$ is a Euclidean domain.*

Week 11

Definition 4.23. *Let A be a commutative ring. We say that a divides b for $a, b \in A$ if there exists $c \in A : b = ac$. Over an integral domain, we also define:*

- *The gcd of a, b, is d such that it divides a and b, and $(c|a \wedge c|b) \Rightarrow c|d \ \forall c$*
- *The lcm of a, b, is l such that a and b divide it, and $(a|m \wedge b|m) \Rightarrow l|m \ \forall m$*

In general, these two are not unique.

Proposition. *Let A be an integral domain. If d_1, d_2 are two* gcd*s of a, b, then $d_1 = xd_2$, with $x \in A^*$ a unit, and if l_1, l_2 are two* lcm*s of a, b, then $l_1 = yl_2$, with $y \in A^*$ a unit.*

Proof. We only prove the case for the gcd: the argument is similar for the lcms. Since we are in an integral domain, we know that there exist x, z such that $d_1 = xd_2, d_2 = zd_1$. This means that

$$d_1 = xd_2 = xzd_1 \Rightarrow d_1(1 - xz) = 0 \overset{d_1 \neq 0}{\Rightarrow} xz = 1$$

meaning that x and z are two units. □

Definition 4.24. *Let A be an integral domain. Then, we say that $a, b \in A$ are associates if there exists a unit $u \in A^*$ such that $a = bu$.*

> *Remark and examples* Associates generate the same ideals in a PID!
>
> If $g = uf$, then $g \in (f)$, meaning $(g) \subset (f)$. Similarly and symmetrically, we have that $f = gv \Rightarrow f \in (g) \Rightarrow (f) \subset (g)$. Since we have mutual inclusion, we get $(f) = (g)$.
>
> In $\mathbb{Z}$, the units are ± 1, meaning that two integers n, m are associates only if they are equal or relative opposites $(n = -m)$. This implies $(m) = (-m)$.
>
> In $F[x]$, with F a field, the units are $F \setminus \{0\}$. Therefore, two polynomials f, g are associates if they are a non zero constant apart, $f = \alpha g, \alpha \in F^*$.

> *Properties* Let $a, b \in A$, A a Euclidean domain. Then, we have:
>
> 1. $\gcd(a, b)$ can be found by successive euclidean division:
>
> $$\begin{cases} a = q_1 b + r_1 \\ b = q_2 r_1 + r_2 \\ \ldots \end{cases}$$
>
> 2. $(a) + (b) = (\gcd(a, b))$
> 3. $(a) \cap (b) = (\operatorname{lcm}(a, b))$
> 4. $\gcd(a, b) = 1 = \gcd(a, c) \Rightarrow \gcd(a, bc) = 1$
> 4. $\gcd(a, b) = 1 \Rightarrow \operatorname{lcm}(a, b) = ab$

[6] Read: I lack the time to typeset this properly

4.6.1 CRT but again

Theorem 4.25 (CRT over Euclidean domains)**.** *Let E be a Euclidean domain, and consider $m_1, ..., m_r \in E : \gcd(m_i, m_j) = 1, i \neq j$. Then, the function:*

$$\begin{aligned} f : E/(m_1...m_r) &\to E/m_1 \times ... \times E/m_r \\ [x]_{(m_1...m_r)} &\mapsto ([x]_{(m_1)}, ..., [x]_{(m_r)}) \end{aligned}$$

is a ring homomorphism

> *Sketch of proof* The proof follows a few basic steps.
>
> 1) It is a ring isomorphism by construction
> 2) We verify surjectivity by induction over the factors: first, we construct a_{12} such that it is equivalent to a_1 mod m_1 and a_2 mod m_2. To do this, we had to use the fact that $\gcd(m_1, m_2) = 1 \Rightarrow (m_1) + (m_2) = E$. Therefore, we can construct a_{123} such that it is equivalent to $a_{12} \bmod m_1 m_2$ and $a_3 \bmod m_3$, using the fact that $\gcd(m_3, m_1 m_2) = 1$. Continue doing this until every congruence is met! Then, we get an $a_{12...r}$ which maps to our original $(a_1, ..., a_r)$, meaning our function is surjective.
> 3) We verify injectivity by considering an $a, b : a \equiv a_i (\operatorname{mod} m_i), b \equiv a_i (\operatorname{mod} m_i) \; \forall i$. Therefore, we have
>
> $$a - b \in \bigcap_r (m_i) = (\operatorname{lcm}(m_1...m_r)) = (m_1...m_r)$$

Corollary 4.26. *Let F be a field, $\{f_1, ..., f_r\}$ a family of polynomials of $F[x]$ such that their pairwise* gcd *is 1. Then,*

$$F[x]/(f_1...f_r) \simeq F[x]/f_1 \times F[x]/f_2 \times ... \times F[x]/f_r$$

Definition 4.27. *A polynomial is said to be monic if its leading coefficient (the coefficient of the highest power of x) is equal to 1.*

> *Remark* The gcd of two polynomials is defined up to a nonzero constant factor. There exists a *unique* gcd that is monic, but an infinite number of gcds that are multiples of the original.

Application: Systems of polynomial congruences

> *Exercice* Let $\mathbb{F}_3$ a field, and consider $\mathbb{F}_3[x]$. Find all the solution of the following

> system of congruences:
>
> $$\begin{cases} f(x) \equiv x+1 \ (\mathrm{mod}(x^2+1) = g_1) \\ f(x) \equiv 1 \ (\mathrm{mod}(x) = g_2) \\ f(x) \equiv -x \ (\mathrm{mod}(x^2-1) = g_3) \end{cases}$$

The three functions can be verified to have pairwise gcd equal to 1, more often than not by finding $a, b \in \mathbb{F}_3 : ag_i + bg_j = 1, i \neq j$.

$$\begin{cases} x^2+1+x(2x) = 1 \\ (x^2-1)\cdot 2 + x(x) = 1 \\ (x^2+1)\cdot 2 + (x^2-1) = 1 \end{cases}$$

Therefore, by the Chinese Remainder Theorem, there exist solutions to the system, and they are of the form $a + (g_1 g_2 g_3)$.

How do we find the $a \in \mathbb{F}_3[x]$ to solve this? First, take any two congruences:

$$\begin{cases} f \equiv x+1 \ (\mathrm{mod}(x^2+1)) \\ f \equiv 1 (\mathrm{mod}(x)) \end{cases}$$

We need to find h, g such that

$$(x^2+1)h(x) + x + 1 = xg(x) + 1 \Rightarrow (x^2+1)h(x) - xg(x) = -x$$

We can verify that $h = 1, g = 2x$ gives us $(x^2+1)\cdot 1 + x \cdot (2x) = 1$, meaning that we have

$$f(x) = (x^2+1)(-x) + x + 1 = -x^3 + 1 \equiv x + 1 \ (\mathrm{mod}(x^3+x))$$

Since $\gcd(x^3+x, x^2-1)$, this can be used as a new congruence!

$$\begin{cases} f(x) \equiv x+1 \pmod{x^3+x} \\ f(x) \equiv -x \pmod{x^2-1} \end{cases}$$

We finish in the same way:

$$\begin{aligned} h(x)(x^3+x) + x + 1 &= g(x)(x^2-1) - x \\ h(x)(x^3+x) - g(x)(x^2-1) &= x - 1 \\ x(x^3+x) + (-x^2+1)(x^2-1) &= -1 \\ \Rightarrow \underbrace{x(-x+1)}_{h(x)}(x^3+x) + \underbrace{(-x^2+1)(-x+1)}_{-g(x)}(x^2-1) &= x - 1 \end{aligned}$$

We replace all of this in our definition, as we did earlier:

$$\begin{aligned} f(x) &= x(-x+1)(x^3+x) + x + 1 \\ &= x(-x^4 - x^2 + x^3 + x) + x + 1 \\ &= -x^5 - x^3 + x^4 + x^2 + x + 1 \\ &\equiv x^4 - x^3 + x^2 + 1 \pmod{x^5 - x} \\ &\equiv x^4 + 2x^3 + x^2 + 1 \pmod{x^5 - x} \end{aligned}$$

giving us our solution!

Method How do you solve a system of congruences?

Consider the system

$$f \equiv h_1 \pmod{g_1} f \equiv h_2 \pmod{g_2}$$

Since $\gcd(g_1, g_2) = 1$ There exist t_1, t_2 such that

$$t_1 g_1 + t_2 g_2 = 1$$

Meaning that $f = h_1 t_2 g_2 + h_2 t_1 g_1$ is a solution[7]! This can be generalized to r equiations: let $G = g_1 ... g_r, G_i = G/g_i$. Therefore, $\gcd(G_i, g_i) = 1$, meaning that for any i; we can find $t_i, s_i : t_i G_i + s_i g_i = 1$. Therefore, our f is a linear combination:

$$f = \sum_{i=1}^{r} h_i G_i t_i$$

which satisfies the right congruences.

Definition 4.28. *An element c of a ring A is irreducible if it is non-zero, not a unit, and $c = ab$ with either $a \in A^*$ or $b \in A^*$.*

Definition 4.29. *$I \subset A$ is maximal if there is no ideal $J \subset A$ such that $I \subsetneq J \subsetneq A$*

Theorem 4.30. *Let A a principal ideal domain. Then, $p \in A$ is irreducible if and only if $p \neq 0$ and $(p) \subset A$ is maximal.*

Proof. We will prove both directions separately.

($\Rightarrow$) p is irreducible. Suppose that there exists a proper subset $J \subsetneq A$ such that $(p) \subsetneq J$. Since A is a PID, then $J = (d)$, meaning that we can write $p = dt$. Since p is irreducible

- either d is a unit, but that would mean that $(d) = (1) = A$, which contradicts the fact that J is a proper subset of A;
- or t is a unit, in which case p and d are associates, and $(d) = (p)$, which contradicts the condition $I \subsetneq J$.

This means that (p) must be maximal.

($\Leftarrow$) $(p) \subset A$ is maximal. Suppose that p is not irreducible, meaning that there exist y, z that aren't units and that are such that $p = yz$. This means $(p) \subset (y) \subsetneq A$. Let's assume towards contradiction that $(p) = (y)$. Then, $y = pt \Rightarrow p = yz = ptz \Rightarrow p(1 - tz) = 0$. This implies either that $p = 0$ (which is impossible as we assume it isn't) or that $tz = 1$ which is only possible if z is a unit, which we said was not the case.

Therefore, if there exist $y, z \notin A^* : p = yz$, then $(p) \subsetneq (y) \subsetneq A$, which contradicts our assumption that (p) was maximal. Therefore, p is irreducible.

□

[7] You can verify the congruences easily.

Theorem 4.31. *Let A be a Euclidean domain. Then, $I \subset A$ is maximal $\Leftrightarrow A/I$ is a field $\Leftrightarrow I = (d) : d$ is irreducible.*

Corollary 4.32. $\mathbb{F}[x]/(f)$ *is a field if and only if f is irreducible.*

Week 12

Proposition. *Let A be a Euclidean domain. Then, $I \subset A$ maximal $\Leftrightarrow A/I$ is a field.*

Proof. We prove each implication separately:

- $\Leftarrow$ If $I = (0)$, then $A/I = A/(0) = A$ is a field, meaning that any $b \neq 0$ is a unit in a. Therefore, $A = (b)$ for that b, meaning that (0) is maximal. Otherwise, if $I = (a) \neq (0)$, then if (a) is not maximal, there exists b such that $(a) \subsetneq (b) \subsetneq I$, meaning that $a = bt : b, t$ not units. Therefore, $[b]_a \cdot [t]_a = [a]_a = [0]_a$, meaning that $A/(a)$ is not a field.
- $\Rightarrow$ Consider an $a \in A$ such that (a) is maximal, Suppose that $[b]$ is both non-zero and not invertible in $A/(a)$. Then, $[b]$ generates a proper ideal of A that contains (a), meaning a is not maximal.

□

This means that over polynomial rings, $F[x]/f$ is a field if and only if f is irreducible within $F[x]$.

> *Properties* Some properties of polynomial rings over a field F:
>
> (i). $F[x]$ is a Euclidean domain, so it is a PID. This means that every ideal I is generated by a single $f \in F[x]$.
>
> (ii). $F[x]/f$ is a field if and only if f is irreducible, meaning that it is equal to $f = gh$, where at least one between g and h is a polynomial of degree 0.
>
> (iii). We can use CRT over $F[x]$, meaning that we can solve systems of congruence modulo pairwise coprime polynomials.
>
> (iv). $(f) + (g) = (\gcd(f, g)); (f) \cap (g) = (\operatorname{lcm}(f, g))$. In these expressions, gcd and lcm are defined up to a unit, but there always exists a single monic solution.

Rapid fire theorems! When is $f \in F[x]$ irreducible?

> *Theorems*
> **Proposition.** *Any polynomial of degree 1 is irreducible.*
>
> *Proof.* $f = gh, \deg(f) = \deg(g) + \deg(h) = 1 \Rightarrow \deg(g) = 1, \deg(h) = 0$ or vice versa. At least one of h, g is a nonzero constant, meaning it is a unit. □
>
> **Proposition.** *A polynomial of degree 2 or 3 is irreducible only if it has no roots in F.*
>
> *Proof.* $f = gh, \deg f = \deg g + \deg h = 2$ or 3. Therefore, in order for f to be irreducible, then it has to be the case that at least one of g, h is of degree 1, therefore being such that:
>
> $$g(x) = ax + b \overset{a \neq 0}{=} a\left(x + \frac{b}{a}\right) \Rightarrow g\left(-\frac{b}{a}\right) = f\left(-\frac{b}{a}\right) = 0$$

□

Proposition. *Let $f(x) = \sum_n a_i x^i$ of degree $n+1$, with integer coefficients, considered over the rationals. Let $\alpha = \frac{r}{s}$ a root of f. Then, $s|a_n, r|a_0$.*

Proof. To convince yourself of this, consider:

$$f\left(\frac{r}{s}\right) \cdot s^n = \overbrace{a_n r^n + \mathrlap{\underbrace{\phantom{a_{n-1}r^{n-1}s + ... + a_1 r s^{n-1} + a_0 s^n}}_{s|}} a_{n-1}r^{n-1}s + ... + a_1 r s^{n-1}}^{r|} + a_0 s^n = 0$$

This means that $r|a_0$ and $s|a_n$. □

Proposition (Eisenstein criterion)**.** *Consider $f(x) = \sum_n a_i x^i$ with integer coprime coefficients ($\gcd(a_0, ..., a_n) = 1$). Suppose that p is a prime such that $p|a_i, 0 \leqslant i \leqslant n-1, p \not| a_n, p^2 \not|$. Then, f is irreducible in $\mathbb{Q}[x]$.*

Examples Let us consider some examples:

(i). Let $g(x) = 2x^3 + 4x^2 + 11x + 1$, over $\mathbb{Q}[x]$. If r/s is a root, then $r|1$, and $s|2$. Therefore, $r \in \{\pm 1\}, s \in \{\pm 1, \pm 2\}$. This means that

$$\frac{r}{s} \in \{\pm\frac{1}{2}, \pm 1\}$$

meaning that we just have to check these two options. Checking these directly gives that they are not roots, meaning that this function is irreducible.

(ii). Consider

$$f(x) = 7x^6 + 21x^4 + 12x^2 + 12x^2 - 9x + 3 \in \mathbb{Q}[x]$$

We verify that 3 divides every coefficient except the leading one, and its square does not divide the last coefficient. As such, by Eisenstein, f is irreducible in $\mathbb{Q}[x]$.

(iii). $g(x) = x^k - p \in \mathbb{Q}[x]$ is always irreducible by Eisenstein. However, that is not the case for $x^{2k} - p^2$, since $p^2|p^2$.

4.6.2 Quotient polynomial rings

Proposition. *If $f \in F[x]$ s irreducible, and of degree n, then any element $F[x]/(f)$ is of the form $\sum_{n-1} a_i \overline{x}^i$, with $a_i \in F, \overline{x}^i = \{x^i + f(x)g(x)\}_{g \in F[x]}$.*

To convince yourselves of this, consider $a(x) = f(x)q(x) + r(x)$. Then, $f(x)q(x) \in (f)$, and $r(x)$ is of degree necessarily smaller or equal to $n-1$.

Proposition. *If F is a finite field such that $|F| = q, f$ is an irreducible polynomial of degree n in $F[x]$, then $K = F[x]/f$ has q^n elements.*

Examples Consider $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, and consider $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ of degree 3. Then $f(0) = 1 = f(1) \Rightarrow f$ has no roots in the field, meaning it has to be irreducible. Consider now $K = \mathbb{F}_2[x]/(f)$. Then, this is a field, of size $|K| = 2^3 = 8$, where every element is of the form $a\overline{x}^2 + b\overline{x} + c, a, b, c \in \mathbb{F}_2$. Additionally, we have that

$$\gcd(x, x^3 + x^2 + 1) = 1 \Rightarrow \exists\ h, g : xg(x) + (x^3 + x^2 + 1)h(x) = 1$$

We find that $x(x^2 + x) + (x^3 + x^2 + 1) = 1$ in $\mathbb{F}_2$, meaning that the inverse of $\overline{x}$ is $(\overline{x})^{-1} = (\overline{x}^2 + \overline{x})$.

Another example: let $F = \mathbb{R}, f(x) = x^2 + 1$. It is irreducible since there are no roots in $\mathbb{R}$. Therefore, $\mathbb{R}[x]/(x^2 + 1)$ is a field, vector space of dimension 2 over $\mathbb{R}$ of the form $\{a + b\overline{x}, a, b \in \mathbb{R}\}$ and such that $(\overline{x})^2 = -1$. This means that $\mathbb{R}/(x^2 + 1) \simeq \mathbb{C}$.

4.7 Finite fields

Proposition. *A field K is finite if its characteristic is a prime p. Additionally, it contains a subfield that is isomorphic to $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

It either contains exactly $|K| = p$ elements, in which case it is isomorphic to $\mathbb{F}_p$, or it contains $|K| = p^n$ elements, making it a vector space over $\mathbb{F}_p$

Proposition. *The group of units of a finite field is cyclic.*

Proof. Let $|K|^* = n$. K^* is finite abelian, meaning $K^* \simeq C_{d_1} \times ... \times C_{d_s}$, with $d_1|d_2...$. Then, $m = d_s$ is the maximum order of any element in K^*. Since the order of an element is necessarily smaller than that of its group, we have that $\text{ord}(k) \leqslant \text{ord}(K^*) \Rightarrow m \leqslant n$.

Therefore, we have that $t^m = 1$ for any $t \in K^*$, meaning that the elements of K^* are solutions to $t^m - 1 = 0$. A polynomial of degree m has at most m solutions in a field[8], which gives us $n \leqslant$

Therefore, $n = m$. □

Theorem 4.33. *Let p a prime, n a positive natural. Then, there exists a field $K : |K| = p^n$ and an irreducible polynomial $f \in \mathbb{F}_p[x]$ such that $\mathbb{F}_p[x]/(f) \simeq K$. If g is another irreducible polynomial of degree n over the same $\mathbb{F}_p[x]$, then $\mathbb{F}_p[x]/(f) \simeq \mathbb{F}_p[x]/(g) \simeq K$.*

Conclusions We have:

(i). For any prime p and $n \geqslant 1$, there exists a unique field $\mathbb{F}_{p^n}$ of $p * n$.

(ii). $n = 1 \Rightarrow$ this unique field is isomorphic to $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$.

(iii). $n > 1 \Rightarrow$ we can construct it as a quotient $\mathbb{F}_{p^n}/(f)$, with f an n-degree polynomial over $\mathbb{F}_p$.

Corollary 4.34. *Over $\mathbb{F}_p$, there exists an irreducible polynomial of any degree $n \in \mathbb{N} : n \geqslant 1$. This is not the case in characteristic 0, as the only irreducible polynomials over $\mathbb{R}$ are of degree 1 or 2, for example, and in those over $\mathbb{C}$ are of degree 1 only.*

[8] This is not the case in any ring!

Definition 4.35. *A field where the only polynomials are of degree 1 is said to be algebraically closed.*

Appendix A

Proofs from exercise sets

This barely needs such pompous titles but oh well. It's fun.

A.1 Theorem 1.1

Proposition. *Strong Induction $\Rightarrow$ Well-ordering principle.*

Proof. We can prove this by induction. Suppose there exists a subset $Y \subset \mathbb{N}$ such that it contains no least element. Consider $P(n) = "n \notin Y"$.

> **Base:** If 0 was in Y, then it would be its least element, since there are no smaller elements of $\mathbb{N}$. As such, it cannot be that $0 \in Y$, meaning $P(0)$ is true.
>
> **Induction:** Assume $P(k)$ is true for any $k \in \{0, 1, ..., n\}$. Then, if it was in Y, $n+1$ would be its smallest element, since every smaller element is not in Y. As such, $P(n+1)$ holds as well. Since P is hereditary and true for 0, it is true for any $n \in \mathbb{N}$.

□

A.2 Theorem 2.4

Proposition. *Any $n > 1$ can be expressed by the product of primes.*

Proof. Consider $S = \{n \in \mathbb{N} : n > 1 \wedge n \text{ does not have a prime factorization}\}$. Then, we take the smallest element in this set, k. k cannot be a prime, so there exists $a, b < k$ such that $k = ab$. However, a and b cannot be in S, since they are smaller than k. This means that $a = \prod {p_{a,k}}^{a_k}, b = \prod {p_{b,k}}^{b_k}$, meaning that their product is the product of primes. Therefore, k cannot be in S, so S has to be empty. □

A.3 Theorem 3.4.1

Proposition. *Let E a finite set, $x, y \in E$, G a finite group. Then,*

$$\text{Orb}_x = \text{Orb}_y \ \textit{ ou } \ \text{Orb}_x \cap \text{Orb}_y = \varnothing$$

Proof. Assume that there exists an $s \in Orb_x : s \in Orb_y$. Then, there exist $g_x, g_y \in G$ such that

$$s = g_x \cdot x = g_y \cdot y \Leftrightarrow x = g_x^{-1} g_y \cdot y = g \cdot y$$

meaning that $x \in \mathrm{Orb}_y$, which in turn means $\mathrm{Orb}_x = \mathrm{Orb}_y$. Therefore, if there is an intersection between two orbits, then they must be the same. □

Appendix B

Elliptic curves

Consider the equation

$$\Gamma : y^2 = x^3 + ax + b$$

for rational pairs $(x, y) \in \mathbb{Q}^2$. This is an elliptic curve. The set of points on this curve has group structure! We introduce the relation $P + Q = -R$ for three points P, Q, R colinear on the curve. Therefore, the relationships that follow from it are as follows:

] The neutral 0 element is at infinity (when there aren't three intersections with the curve, for example).

$P + 0 = 0 + P = P \ \forall P$

$-P$ is the point obtained from P by symmetry wrt. the x axis.

The group operation is therefore defined, in the general case, geometrically: to compute $P + Q$, you draw a line through P and Q, and you denote the intersection with the curve R. Then, $P + Q := -R$. For edge cases, we have:

- If P and Q are each other's reflection across the x axis, then $P + Q = 0$ (since there's no third intersection with the curve, we take the point at infinity).
- If $P = Q$, then you pick the line tangent to Γ at Q, find its intersection with Γ, denoted $2Q$. Then, $Q + Q = -2Q$.

This induces a specific algorithm to factorize a number $n \in \mathbb{N}$.

(i). Define an elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}/n\mathbb{Z}$, and pick a point $P = (x_0, y_0)$ on it.

(ii). Compute $i!P$ up to some integer $k > 0$. If we take the example of $3!P$, then we can show the process:

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

This involves finding the slopes of tangent lines to the curve, as well as their integer intersections. This so

Appendix C

Jack gets pedantic about notation for like half a page

Now. Professor Lachowska is a doctor in mathematics, and also potentially a good dozen of orders of magnitudes smarter than me. So this is by no means a way for me to claim I'm better than her. However.

When you say that $\mathbb{R}[x]$ is the set of all polynomials of one variable over coefficients in $\mathbb{R}$, what you're doing in computer science terms is you're defining a type. An element of that set essentially follows the rules of that type. The way the type $\mathbb{R}[x]$ is typically notated is $\mathbb{R} \to \mathbb{R}$, and we define an element of that type as $f : \mathbb{R} \to \mathbb{R}$.

$f(x)$ means the application of $f : \mathbb{R} \to \mathbb{R}$ to the number $x : \mathbb{R}$, and it is therefore a real value, $f(x) : \mathbb{R}$.

What Prof. Lachowska says is: "Nah, I'll do my own thing". $f(x)$ is the polynomial, and f does not exist. This makes notation heavier and not standard.

Why does she do that? I'm not sure. Does it matter? Not really. Am I bitter about it? Yes.

And it's my textbook, so I get to write this page.