Discrete Mathematics

Seb Arnold

October 1, 2016

Abstract

Notes from the class of Prof. Ueli Maurer at ETH Zürich.

1 Introduction

Abstraction will be often used during this class. It is a way of simplification and generalization. In fact, in Computer Science, we never think of each piece of the problem; instead of writing a program bit by bit, we use abstract programming languages that are easier for us to use.

Thanks to abstraction we can think of a program as a discrete mathamtic object. Doing so, we arrive at the point where we can prove that a program is correct or not, i.e. it always terminates with th desired output.

2 Mathematical Reasoning and Proofs

2.1 What is a proof ?

A proof of a statement S is a sequence of simple, easily verifiable, consective steps. it starts from a set of axioms (known to be true) and each step expands the set of proved statements, until the final step proves S.

You can make a proof using informal language, however we often use a more rigoruous, formal and pedantic type of proofs for two reasons:

1. Prevention of errors
2. Proof complexity and automatic verification

2.2 What is a proposition ?

Propositions are amthematical statements that are either true or false. Eg: 71 is a prime number. A statement like "It is raining" is not a proposition,

unless we assume the validity of this statement. (By common sense)

A proposition that is true is often called a theorem, lemma or corollary. The term *theorem* is often used for important results, *lemma* for intermediate ones, and a *corollary* is usualy a special case of a lemma or a theorem.

2.3 Logical Constants and Operators

- true $= 1 = \top$ and false $= 0 = \bot$.
- NOT A $= \neg A$ and A AND B $= A \wedge B$ and A OR B $= A \vee B$.
- A formula is an expression involving many operators.

2.4 Logical Equivalence and Basic Laws

Definition 2.1. *Two logical formulas are equivalent* $(F \equiv G)$ *if they correspond to the same function.*
Examples:

- $\neg(F \vee G) \equiv \neg F \wedge \neg G$
- $\neg(F \wedge G) \equiv \neg F \vee \neg G$

$A \rightarrow B$ is called an implication and is true on if A implies B, that is: $\neg A \vee B$.

The two -sided implication is defined as:

$$A \leftrightarrow B \equiv (A \wedge B) \vee (\neg A \wedge \neg B) \equiv (A \rightarrow B) \wedge (B \rightarrow A)$$

A *tautology* is a formula which is true for all truth assignments. If a formula is ture for at least one truth assignment, it is called satisfiable.

$F \Rightarrow G$ means that F implies G, that is $F \rightarrow G$ is true. Respectively if $F \leftrightarrow G$ is true, we write $F \Leftrightarrow G$.

2.5 Quantifiers

Until now, we have only dealt with *propositional logic* but this one is limited and we need quantifiers to go in the field of *predicate logic*.

The universe U is the set in which we want to reason.

Definition 2.2. *A k-ary predicate P on U is a function $U^k \to \{0,1\}$.*
Examples:

- *Unary (k = 1) predicate for $U = \mathbb{N}$: prime$(x) = \begin{cases} 1, & \text{if } x \text{ is prime.} \\ 0, & \text{otherwise.} \end{cases}$*
- *Binary (k = 2) predicate for $U = \mathbb{N}$: less$(x, y) = \begin{cases} 1, & \text{if } x < y. \\ 0, & \text{otherwise.} \end{cases}$*

2.6 Definition of $\exists$ and $\forall$

For a universe U, and predicate $P(x)$ we define:

- $\forall x : P(x)$ stands for: $P(x)$ is true for all $x \in U$,
- $\exists x : P(x)$ stands for: there exists an $x \in U$ for which $P(x)$ is true.

Note that we can neste quantifiers together : $\forall x(P(x) \vee \exists y : Q(x, y))$ where P, Q are predicates. Note that

$$\neg\forall x : P(x) \equiv \exists x : \neg P(x) \text{ and } \neg\exists x : P(x) \equiv \forall x : \neg P(x)$$

2.7 Proof Patterns and Techniques

- Splitting into precondition and implication: $F \wedge (F \to G) \Rightarrow G$ (F true and $F \to G$ so G true).
- Direct Proofs of Implications: Is using a lot $\to$ by assuming F and dreiving G.
- Indirect Proofs of Implication: Using $F \to G$ by assuming $\neg G$ and deriving $\neg F : F \to G \equiv \neg G \to \neg F$.
- Proofs by Contradiction: In this case, we want to find a false statement G so that $\neg F \to G$ si true. Correct because $\neg G \wedge (\neg F \to G) \Rightarrow F$.
- Existence Proofs: Is a proof of statements of the form: $\exists x : P(x)$.
- Non-Existence Proofs: Statement of the form: $\neg\exists : P(x)$.
- Proofs by Counter-Example: We want to prove $\neg\forall x : P(x) \equiv \exists x : \neg P(x)$. An a for which $\neg P(a)$ is true is a counter-example.
- Proofs by Induction: This type of proof technique is one fo the most important and is used to prove statements of the form $\forall n : P(n)$ where $U = \mathbb{N}$. It consists of two steps:
  1. Prove $P(0)$
  2. Prove $\forall n : P(n) \to P(n + 1)$

3 Sets, Relations, and Functions

If $A = B \Leftrightarrow \forall x(x \in A \leftrightarrow x \in B)$.

$|A|$ is the *cardinality* of A, which is the number of elements in A. You can put a set in another set. In this case, to determine the equality of two sets, we look at everything except the order.

Example: Given $A = \{5, \{\{3\}, 4\}, \{7\}\}$, $B = \{5, \{\{3\}, 4\}, 7\}$, $C = \{\{\{3\}, \{4\}\}, 5, \{7\}\}$, and $D = \{\{4, \{3\}\}, 5, \{7\}\}$. Only A and D are equal.

Note:. $\{a, b\}$ is a set with 2 elements, whereas (a, b) is a pair !

Tip:. Remember that $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ (respectively: integers, rationals, reals, and complex)

The power set of A, $\mathcal{P}$, or 2^A, is the subset of all subsets of A: $\mathcal{P} := S|S \subseteq A$. $\bar{A} := \{x \in U|x \notin A\}$ is the complement of A. $B \setminus A$ or $B - A$ is the difference of B and A: $\{x \in B|x \notin A\}$

3.1 Cartesian Product of Sets

$$A \times B = \{(a, b)|a \in A \wedge b \in B\}$$

$$|A \times B| = |A| \times |B|$$

3.1.1 Russell's Paradox

Suppose a set $R = \{A|A \notin A\}$.

That is, R is a set that is not element of himself. Then we have either $R \in R$ or $R \notin R$. by Cantor's definition, $R \in R$. But the set R is defined as not being an element of himself so $R \notin R$. That's the paradox, $R \in R$ only if $R \notin R$.

The paradox was solved by Zermalo's axiomatization: Say the universe U of object can not be identified as a set.

3.2 Relations

Definition 3.1. *A relation ρ from A to B is a subset of $A \times B$.*

Instead of writing $(a, b) \in \rho$, we write $a\rho b$. For example, imagine a "married" relation, then $a\rho b$ means that a and b are married. Another example is

$A \subseteq \mathcal{P}(A)$ where $\subseteq$ is the relation.

Relations can be represented as a matrix:

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

You can imagine a relation that is $\leq \vee \geq$.

$\hat{\rho}$ is the inverse of the relation ρ. You can also compose relation, such as $\rho\sigma$ (or $\rho \circ \sigma$):

$$a\rho\sigma c \Leftrightarrow \exists b \in B : (a\rho b) \wedge (b\sigma c)$$

Similarly, $\rho\rho$ is denoted by ρ^2.

3.2.1 Properties of Relations

- Reflexivity: If $(a, a) \in \rho$, the relation is reflexive. Otherwise, $\forall a : a \not\rho a$ it is denominated as irrflexive. Examples: $\leq, \geq, =$.
- Symmetricity: If $(a, b) \in \rho \Leftrightarrow (b, a) \in \rho$ the relation is symmetric. Example: "married" relation, $\equiv_m$.
- Anti-symmetricity: If $(a, b) \in \rho \wedge (b, a) \in \rho \Rightarrow a = b$ the relation is anti-symmetric. Examples: $\leq, \geq$.
- Transitivity: if $(a, b) \in \rho \wedge (b, c) \in \rho \Rightarrow (a, c) \in \rho$ the relation is transitive. Examples: $\leq, \geq, \equiv_m$

An *equivalence relation* isa relation that is reflexive, symmetric and transitive. Example: $\equiv_m$ on $\mathbb{Z}$. For an equivalence relation θ on $A \ni a$, the set of elements of A that are equivalent to a is called the *equivalence class* of a and is denoted as

$$[a]_\theta := \{b \in A | b\theta a\}$$

A trivial example is the equality relation (=) for which equivalence classes are all singleton sets $\{a\} \forall a \in A$.

Theorem 3.1. *The set A/θ of equivalence classes of an equivalence relation θ on A is a partition of A.*

A *partial order* is a relation that is transitive, reflexive, and anti-symmetric. A set A with a partial order $\preceq$ is called a poset, and is denoted: $(A; \preceq)$. Examples: $\leq$ and $\geq$. Of course, if any two elements of A are comparable, the set

is called *totally ordered.* A *well-ordered* set is ordered and every non-empty subset has a least element. (finite totally ordered $\rightarrow$ well ordered)

In a poset, an element b is said to *cover* a if: $a \prec b$ and there is no c such that $a \prec c$ and $c \prec b$. A *Hesse-Diagram* is a directed graph, whose vertices are elements of A and en edge from a to b means that b covers a. Example: $\{2, 3, 4\}$ with $\leq$.

3.2.2 Chains in Posets

A *chain* is a totally ordered subset $C \subseteq A$ of a poset $(A; \preceq)$. Example: $(\{1, 2, 3, 4, 8\}, 1)$, $\{2, 4, 8\}$ is a chain. An *anti-chain* is a subset $B \subseteq A$ whose 2 distinct elements are incomparable. Example: $(\{1, 2, 3\}; 1)$, $\{2, 3\}$ is an anti-chain.

3.2.3 Combination of Posets and Lexicographic Order

For given posets $(A; \preceq)$ and $(B; \sqsubseteq)$, the relation $\leq_{\text{lex}}$ defined on $A \times B$ by

$$(a_1, b_1) \leq_{\text{lex}} (a_2, b_2) :\Leftrightarrow a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \sqsubseteq b_2)$$

is a partial order relation.

3.2.4 Special Elements in Posets

Let $(A; \preceq)$ be a poset and $S \subseteq A$ be same subset of A. Then

1. $A \in S$ is a minimal (maximal) element of S if there exists no $b \in S$ with $b \prec a$ ($b \succ a$).
2. $a \in S$ is the least (greatest) element of S if $a \preceq b$ ($asucceqb$) for all $b \in S$.
3. $a \in A$ is a lower (upper) bound of S if $a \preceq b$ ($asucceqb$) for all $b \in S$.
4. $a \in A$ si the greatest lower bound (least upper bound) of S if a is the greatest (least) element of the set of all lower (upper) bounds of S.

3.3 Functions

See the mathematical analysis notes for more details.

4 Combinatorics and Counting

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Theorem 4.1.

$$|A_1 \cup \cdots \cup A_n| \geq \sum_{i=1}^{n} - \sum_{i \leq i_1 \leq i_2 \leq n} |A_{i_1} \cap A_{i_2}|$$

4.1 Drawing Elements from a Set

The problem is to count how many ways there are to select k elements from a set of cardinality n.

	Ordered	Unordered
With Repetitions	n^k	$\frac{(n+k-1)!}{k!(n-1)!} = \binom{n+k-1}{k}$
Without Repetitions	$n^{\underline{k}} = \frac{n!}{n-k}!$	$\frac{n^{\underline{k}}}{k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$

4.2 The Double Counting Principle

Imagine you want to count the subset of $A \times B$. Two approaches are possible: counting for each $a \in A$ the number m_a of $b \in B$ so that $(a, b) \in S$, or the other way around. Then:

$$|S| = \sum_{a \in A} m_a = \sum_{b \in B} m_b$$

4.3 Binomial Coefficients

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Approximation of the Binomial Coefficient: $(\frac{n}{k})^k \leq \binom{n}{k}^k < (\frac{e \cdot n}{k})^k$

or: $\binom{n}{k} \approx 2^{nh}$

5 Graph Theory

5.1 Basic Concepts

$G = (V, E)$ is a graph with V vertices (nodes) and E edges.

The *neighborhood* of a vertex v is $\Gamma(v)$ which is the set of vertices linked through an edge to v.

A *directed graph* consists of a graph with directed edges. ie, if $(u, v) == (v, u)$ the graph is undirected, but if it is not it is directed.

The *degree of freedom* of a vertex v, $\deg(v) = |\Gamma(v)|$ is the number of edges connected to v. Similarly, there is an in-degree $\deg^-(v)$ (edges directed entering v) and an out-degree $\deg^+(v)$ (edges leaving v).

- Directed Graphs: $\sum_{v \in V} \deg^-(v) = \deg^+(v) = |E|$
- Undirected Graphs: $\sum_{v \in V} \deg(v) = 2|E|$

Two *isomorphic* graphs are denoted $G \cong H$, which means that renaming the vertices of G results in H, according to a relation π.

5.2 Complete Graphs

on n vertices, K_n, are simple graphs, where all vertices are connected altogether.

Definition 5.1. *A cycle C_n consists fo n vertices connected cyclically.*

Definition 5.2. *A wheel W_n is a cycle, with an additional vertex, the center.*

Definition 5.3. *A star S_n is a graph, where all vertices are connected to and only to the center.*

The *adjacency matrix* $A_G = [a_{ij}]$ is a binary $N \times N$ matrix, where: $a_{i,j} = \begin{cases} 1 \text{ if } \{v_i, v_j\} \in E \\ 0 \text{ otherwise.} \end{cases}$

Note that it is easily doable to apply this principle for both directed and undirected graphs.

5.3 Paths and Cycles

Definition 5.4. *A walk is a sequence of consecutive connected vertices.*

Definition 5.5. *An Hamiltonian cycle is a cycle which visits all vertices. If there is an Hamiltonian cycle, the graph is called Hamiltonian.*

Definition 5.6. *A path is a walk where all vertices are distinct.*

Definition 5.7. *A tour is a walk where every edges are distinct.*

Definition 5.8. *A Euler tour is a tour containing all the edges of the graph. An undirected graph is Eulerian if and only if each vertex has even degree. A directed graph is Eulerian if and only if the in/out degree for each vertex are equal.*

5.4 Trees

Definition 5.9. *A tree is an undirected graph with no cycle.*

For a graph G with n vertices, the following are all equivalent: G is a tree $\equiv G$ has $n-1$ edges and no cycle $\equiv G$ has $n-1$ edges and is connected.

Definition 5.10. *A forest is the union of several trees with disjoint vertex set.*

5.5 Planar Graph

Definition 5.11. *A planar graph can be drawn in the plane with no edges crossing.*

Any planar graph G divides the plane into r regions, where $r = |E| - |V| + 2$. This fact is known as Euler's formula.

If you merge vertices or delete edges from a graphand the result is not planar, then the original graph is not planar.

5.6 Graph Coloring

Coloring a graph means to cut the set V into k subsets so that no two vertices or the same color are connected. $\chi(G) \leq 4$ for every planar graph G. You can also edge-color a graph (two linked edges can not be of the same color). $\chi'(G) =$ min possible colors.

6 Number Theory

The greatest common divisor (gcd, *ggd auf Deutsch*) is denoted by (a, b). The *ideal generated* by a and b is the set:

$$(a, b) := \{ua + vb | u, a, v, b \in \mathbb{Z}\}$$

6.1 Factorization into Primes

Every integer can be written as the product of primes.

For any $a, b, m \in \mathbb{Z}$ with $m \geq 1$:

$$a \equiv_m R_m(a) \text{ and } a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$$

Let $a \equiv_m b$ and $c \equiv_m d$ then: $a + c \equiv_m b + d$ and $ac \equiv_m bd$.
Example: $7^{100} \equiv_{24}? \rightarrow R_{24}(7^{100}) = R_{24}(7^{100}) = R_{24}((7^2)^{50}) = R_{24}(1^{50}) = 1$

If $ax \equiv_m 1$ then $x \equiv_m a^{-1}$.

For every prime p and every a not divisible by p: $a^{p-1} \equiv_p 1$.

6.2 Chinese Remainder Theorem

For several equations

$$\begin{cases} x \equiv_{m_1} a_1 \\ \dots \\ x \equiv_{m_r} a_r \end{cases}$$

where $0 \leq a_i \leq m_i$ and $1 \leq i \leq r$ and m_i are pairwise co-prime, x has a unique solution:
$0 \leq x \leq M = \prod_i^r m_i$.

Example: $R_{35}(2^{1000}) =? \rightarrow 2^4 \equiv_5 1$. As $2^3 \equiv_7 1 \rightarrow 2^{1000} \equiv_7 2$. So $2^{1000} \equiv_{35} 16$ as 16 is the only integer $x \in [0, 34]$ with $x \equiv_5 1$ and $x \equiv_7 2$.

6.3 Pigeonhole Principle

> If a set of n objects is paritioned into $k < n$ sts, then at least one set has $\lceil \frac{n}{k} \rceil$ objects.

The trick with the pigeonhole principle is to understnd when to use it. Usually when the problem is about the length of a set/subset it is the right one. Or more generally when we have to break things into parts. (Yes, that's vague.)

6.4 Countable and Uncountable

Some definitions

1. If there is a bijection between two sets A and B, the have the same cardinality which is denoted $A \sim B$
2. $A \preceq B$ if $\exists C \in B : A \sim C$ and $A \prec B$ if $A \preceq B$ and $A \not\sim B$.
3. A is countable if $A \preceq \mathbb{N}$ and uncountable otherwise.

Note:. To show countability of A provide an inkection $A \to \mathbb{N}$.

Some other facts:

- $\{0,1\}^*$ is countable (translate to binary, with 1 on front)
- $\mathbb{N} \times \mathbb{N}$ is countable, hence $\mathbb{Q}$ is countable.
- $\{0,1\}^\infty$ is uncountable. (Semi-infinite string of 1's and 0's)

Theorem 6.1. *If A and B are countable, then $A \times B$ is countable.*

7 Modern Algebra

7.1 Well-Ordering Principle

> "Every non-empty set of positive integers contains a smallest element."

The gcd is a linear combination: $\forall a, b \neq 0 \exists s, t \in \mathbb{N} : \gcd(a,b) = as + bt$. Moreover, $\gcd(a,b)$ isthe smallest positive integer of $as + bt$.

Theorem 7.1. $a \mod n \equiv b \mod n \Leftrightarrow n|(a-b)$

Definition 7.1. *An equivalence relation R on a set S is a set of ordered pairs of elements of S such that R is reflexive, symmetric and transitive.*

Definition 7.2. *A partition of a set S is a collection of non-empty disjoint subsets of S whose union is S.*

Definition 7.3. *A one-to-one (ie, injective) function imples that $\forall a, b : f(a) = f(b) \Leftrightarrow a = b$.*

Definition 7.4. *An onto function (ie, surjective) from A to B implies that $\forall b \in B \exists a \in A : f(a) = b$.*

7.2 Groups

Definition 7.5. *A binary operation on a set G is a function that assigns each ordered pair of elements of G one element of G.*

Definition 7.6 (Group). *Let G be a set together with a binary operation (usually multiplication) that assigns to each ordered pair (a, b) an element ab in G. We say G is a group under this operation if the following 3 properties are satisfied.*

- *Associativity:* $(ab)c = a(bc) \forall a, b, c \in G$
- *Identity:* $\exists e \in G : ae = ea = a, \forall a \in G$
- *Inverses:* $\forall a \in G \exists b \in G : ab = ba = e$

Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all groups under the addition operation.

7.2.1 Properties of Groups

Theorem 7.2. *In a group, there is only one identity element.*

Theorem 7.3. *In a group, the laws of cancelation hold. This means $ba = ca \rightarrow b = c$ and $ab = ac \rightarrow b = c$.*

Theorem 7.4. *Each element of a group G has a unique inverse in G.*

Theorem 7.5. *For a group, elements a and b, $(ab)^{-1} = b^{-1} \cdot a^{-1}$.*

7.2.2 Finite Groups and Subgroups

Definition 7.7. *The number of elements of a group is called its order, denoted $|G|$.*

Definition 7.8. *The order of an element g - denoted $|g|$ - in a group G is the smallest positive integer such that $g^n = g \cdot \cdots \cdot g = e$ where $\cdot$ is the law in the group. If there is no such integer, its order is infinity.*

Definition 7.9. *If a subset of a group G is itself a group under the operation of G, we say that H is a subgroup of G.*

Proving Subgroups Instead of testing a subgroup with every property of a group, one of these 3 tests is sufficient

1. If $ab^{-1} \in H, \forall a, b \in H$ then H is a subgroup.
2. If $ab \in H, \forall a, b \in H$ and $a^{-1} \in H, \forall a \in H$, then H is a subgroup.

3. If H is closed under the operataion of G, then H is a subgroup.

Definition 7.10. *Let $< x >$ denotes the set $\{x^n | n \in \mathbb{Z}\}$. In particular, there are all the negative numbers and also 0 as values for n. ($x^0 = e$)*

Theorem 7.6. *Let G be a group and $a \in G$. Then $< x >$ is a subgroup of G.*

Definition 7.11. *The center $Z(G)$ is the subset of elements in G so that $Z(G) = \{a \in G : ax = xa, \forall x \in G\}$.*

Theorem 7.7. *The center of a group is a subgroup.*

Definition 7.12. *Let a be a fixed element of a group G. The centralizer of a in G denoted $C(a)$ is defined as $C(a) = \{g \in G | ga = ag\}$.*

Theorem 7.8. *For each a in a group G, the centralizer of a is a subgroup of G.*

7.3 Cyclic Groups

Definition 7.13. *A group is called cyclic if there is an element $a \in G :< a >= G$.*

Theorem 7.9. *Let G be a group. If $|a| = \infty \rightarrow a^i = a^j$ if and only if $i = j$. But if $|a| = n \rightarrow a^i = a^j$ if and only if $n|i - j$.*

Theorem 7.10. *For any group element a, $|a| = | < a > |$.*

Corollary 7.10.1. *Let G be a group and a an element of order n. If $a^k = e \rightarrow n|k$.*

Theorem 7.11. *In a finite cyclic group, the order of an element divides the order of the the group.*

Theorem 7.12. *Every subgroup of a cyclic group is cyclic. Morever, if $| < a > | = n$, then the order of any subgroup of $< a >$ is a divisor of n. And for each positive divisor k of n, the group $< a >$ has exactly one subgroup of order k - namely $< a^{n/k} >$*

Thanks to the above theorem, we can easily find every subgroup of a cyclic group and know its order.

7.4 Isomorphisms

Definition 7.14. *An isomorphism ϕ from a group G to H is a one-to-one (injective) function from G to H that preserves the group operation. That is: $\phi(a \cdot b) = \phi(a) \cdot \phi(b), \forall a, b \in G$. If there is an isomorphism from G onto H, we say that G and H are isomorphic and write $G \approx H$.*

7.4.1 Properties of Isomorphisms

Suppose that phi is an isomorphism from G to H. Then

1. ϕ carries the identity of G to the identity of H.
2. For every integer n and for every group element a in $G, \phi(a^n) = \phi(a)^n$.
3. For any elements a and b in G, a and b commute if $\phi(a)$ and $\phi(b)$ commute.
4. $G =< a >$ iff $H =< \phi(a) >$.
5. $|a| = |\phi(a)|$.
6. $x^k = b$ (with fixed k and b) has the same number of solutions in G as $x^k = \phi(b)$ in H.
7. If G is finite, then G and H have the same number of elements of every order.

Suppose ϕ is an isomorphism from G to H. Then

1. ϕ^{-1} is an isomorphism from H to G.
2. G is Abelian iff H is Abelian.
3. G is cyclic iff H is cyclic.
4. If K is a subgroup of G, then $\phi(K) = \{\phi(k)|k \in K\}$ is a subgroup of H.

Definition 7.15. *An isomorphism from a group onto itself is called an automorphism.*

7.5 Group Homomorphisms

Definition 7.16. *A homomorphism ϕ from a group G to H is a function from G into H that preserves the group operation: $\phi(a \cdot b) = \phi(a) \cdot \phi(b), \forall a, b \in G$.*

Note:. Note that the difference with an isomorphism lies in the fact that homomorphisms don't have to be injective. (one-to-one)

Definition 7.17. *The kernel of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G|\phi(x) = e\}$. The kernel of ϕ is denoted by* $\ker(\phi)$.

7.5.1 Properties of Homomorphisms

Let ϕ be a homomorphism from a group G to a group H and let g be an element of G. Then

1. ϕ carries the identity of G to the identity of H.
2. $\phi(g^n) = \phi(g)^n$ for all $n \in \mathbb{Z}$.
3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.
4. $\ker(\phi)$ is a subgroup of G.
5. $\phi(a) = \phi(b)$ iff $a\ker(\phi) = b\ker(\phi)$.
6. If $\phi(g) = g'$ then $\phi^{-1}(g') = \{x \in G | \phi(x) = g'\} = g\ker(\phi)$.

Let ϕ be a homomorphism from G to H and let J be a subgroup of G. Then

1. $\phi(J) = \{\phi(j)|j \in J\}$ is a subgroup of H.
2. If J is cyclic, then $\phi(J)$ is cyclic.
3. If J is Abelian, then $\phi(J)$ is Abelian.
4. If $|\ker(\phi)|$ then ϕ is an n-to-one mapping from G onto $\phi(G)$.
5. If $|J| = n$, then $|\phi(J)|$ divides n.
6. If K is a subgroup of H, then $\phi^{-1}(K) = \{k \in G|\phi(k) \in K)\}$ is a subgroup of G.
7. If ϕ is onto and $\ker(\phi) = \{e\}$, then ϕ is an isomorphism from G to H.

7.6 Rings

Definition 7.18. *A ring R is a set with 2 binary operations, addition (usually the common addition law) and multiplication (also the common law) such that $\forall a, b, c \in R$:*

- $a + b = b + a$
- $(a + b) + c = a + (b + c)$
- *There is an additive identity 0. That is, there is an element 0 in R, such that $a + 0 = a, \forall a \in R$.*
- *There is an element $-a \in R : a + (-a) = 0$*
- $a(bc) = (ab)c$
- $a(b + c) = ab + ac$ *and* $(b + c)a = ba + ca$

Note: Multiplication is not necessarily commutative.

7.6.1 Properties of Rings

Let $a, b, c \in R$, R is a ring. Then:

- $a0 = 0a = 0$
- $a(-b) = (-a)b = -(ab)$ (Thank to distributivity)
- $(-a)(-b) = ab$
- $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$

Furthermore, if R has a unity element 1, then:

- $(-1)a = -a$
- $(-1)(-1) = 1$

Theorem 7.13. *If a ring has a unity it is unique. If a ring element has a multiplicative inverse, it is unique.*

7.6.2 Subrings

Definition 7.19. *A subset S of a ring is a subring of R if S is itself a ring wit the operations of R.*

Subring Test A non-empty subset S of a ring R is a subring if S is closed under subtraction and multiplication. That is, if $a - b$ and ab are in S whenever a and b are in S.

7.7 Integral Domains

Integral domains are particular rings, with some more properties to be immitate the integers.

Definition 7.20. *A zero-divisor is a non-zero element a of a commutative ring such that there is a non-zero element $b \in R$ with $ab = 0$.*

Definition 7.21. *An integral domain is a commutative ring with unity and no zero-divisor.*

Theorem 7.14. *a, b, c are in an integral domain if $a \neq 0 \wedge ab = ac \rightarrow b = c$*

Definition 7.22. *A field is a commutative ring with unity in which every non-zero element is a unit.*

Theorem 7.15. *A finite integral model is a field.*

Corollary 7.15.1. *For every prime p, $\mathbb{Z}_p$ the ring of integers $\mod p$ is a field.*

Definition 7.23. *The characteristic of a ring R is the least positive integer n such that $nx = 0, \forall x \in R$. If no such integer exists, we say it is 0.*
The characteristic of R is dnoted by char (R).

Example: The subring $\{0, 3, 6, 9\}$ of $\mathbb{Z}_R$ has characteristic 4.

Theorem 7.16. *Let R be a ring with unity 1. If 1 has finite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.*

Theorem 7.17. *The characteristic of an integral domain is either 0 or prime.*

7.8 Ring Homomorphism

Definition 7.24. *A ring homomorphism ϕ from a ring R to a ring S is a mapping from R to S that preserves the 2 ring operations. For all $a, b \in R$*

$$\phi(a + b) = \phi(a) + \phi(b) \text{ and } \phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

Note:. A ring homomorphism that is bijective is an isomorphism.

7.8.1 Properties of Ring Homomorphisms

let ϕ be a ring homomorphism from R to S. Let A be a subring of R, then

- $\forall r \in R$ and $n > 0, \phi(nr) = n \cdot \phi(r)$ and $\phi(r^n) = (\phi(r))^n$.
- $\phi(A) = \{\phi(a) | a \in A\}$ is a subring of S.
- If R is commutative, then $\phi(R)$ is commutative.
- If R has unity 1, $S \neq \{0\}$ and ϕ is surjective, then $\phi(1)$ is the unity of S.
- ϕ is an isomorphism iff ϕ is surjective and $\ker(\phi) = \{r \in R | \phi(r) = 0\} = \{0\}$
- If ϕ is a surjective isomorphism, then ϕ^{-1} is a surjective isomorphism.

7.9 Polynomial Rings

Definition 7.25. *Let R be a commutative ring. The set of formal symbols*

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 | a_i \in R, n > 0\}$$

is called the ring of polynomials over R in the indeterminate x. Two elements $a_n x^n + \cdots + a_0$ and $b_m x^m + \cdots + b_0$ are considered equal iff $a_i = b_i, \forall i > 0$.

Note:. In $\mathbb{Z}_3[x], 5x = 2x$ but $x^5 \neq x^2$. This means you only reduce the coefficient and not the exponent.

Definition 7.26. *Let R be a commutative ring. Then Multiplication and addition will work the same way as usual.*

Theorem 7.18. *If D is an integral domain, then $D[x]$ is an integral domain.*

Theorem 7.19. *Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x) \cdot q(x) + r(x)$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. That's the division algorithm for $F[x]$.*

Theorem 7.20. *Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.*

Theorem 7.21. *Let F be a field, $a \in F$ and $f(x) \in F[x]$. Then a is a zero of $f(x)$ iff $x - a$ is a factor of $f(x)$.*

Theorem 7.22. *F a field, $f(x) \in F[x]$ and if $\deg(f(x))$ is 2 or 3, then $f(x)$ is reducible over F iff $f(x)$ has a zero in F.*

Theorem 7.23. *Let $f(x) \in \mathbb{Z}$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.*

7.9.1 Irreducibility Tests

Theorem 7.24. *Let p prime, $\bar{f}(x) \in \mathbb{Z}_p[x]$, obtained from $f(x)$ by reducing coefficients. If $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.*

Theorem 7.25. *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there is a prime p: $p \not| a_n, p|a_{n-1}, \ldots, p|a_0$ and $p^2 \not| a_0$, then $f(x)$ is irreducble over $\mathbb{Q}$.*

7.10 Fields

Fields are widely used, and especially in linear algebra. As a matter of fact, a vectorspace is just an abelian group with respect to the following conditions: $\forall a, b \in F, \forall u, v \in G$ where F is a field, G is a group

1. $a(v + u) = av + au$
2. $(a + b)v = av + bv$
3. $a(bv) = (ab)v$
4. $1v = v$

Note:. For the definition of a field, refer to the section on Integral Domains.

Definition 7.27. *A field E is an extension field of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F.*

Theorem 7.26. *Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. Then there is an extension field E of F where $f(x)$ has a zero.*