MATH10111 - KEY DEFINITIONS, WEEKS 7-12

Counting

Let $n \in \mathbb{N}$. Define $\mathbb{N}_n = \{1, 2, \ldots, n\} = \{k : k \in \mathbb{N}, k \leq n\}$.

Let A be a finite set and $n \in \mathbb{N}$. We say A has *cardinality* n, and write $|A| = n$, if there is a bijection $f : \mathbb{N}_n \to A$. Define $|\emptyset| = 0$.

If $|A| = n$ for some $n \in \mathbb{N} \cup \{0\}$, then we say that A is *finite*. Otherwise we say A is *infinite*.

We say A is *countably infinite* if there is a bijection $f : \mathbb{N} \to A$.

We say sets A and B are *disjoint* if $A \cap B = \emptyset$.

Inclusion-exclusion principle: If A and B are finite sets, then $|A \cup B| = |A| + |B| - |A \cap B|$.

For $n \in \mathbb{N}$, define $n! = n(n-1)\ldots 2.1$. Define $0! = 1$.

Let A be a set and $r \in \mathbb{N} \cup \{0\}$. An *r-subset* of A is a subset $X \subseteq A$ with $|X| = r$. Write

$$\mathcal{P}_r(A) = \{X \subseteq A : |X| = r\}.$$

Write $\begin{pmatrix} n \\ r \end{pmatrix}$ for the cardinality of $\mathcal{P}_r(A)$. We call $\begin{pmatrix} n \\ r \end{pmatrix}$ a *binomial coefficient*, or "*n choose k*".

The *Binomial Theorem* states that if $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$, then

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

The Euclidean algorithm

The *Division Theorem* states that if $a, b \in \mathbb{Z}$ with $b > 0$, then there are unique integers q and r such that $a = qb + r$ and $0 \leq r < b$. Call r the *remainder*.

Let $a \in \mathbb{Z}$. Define $D(a) = \{d : d \in \mathbb{Z}, d|a\}$.

The *greatest common divisor* of a and b, written $gcd(a, b)$, is the maximal integer in the set $D(a) \cap D(b)$. In other words, $d = gcd(a, b)$ satisfies $d|a$ and $d|b$, and if $c \in \mathbb{Z}$ such that $c|a$ and $c|b$, then $c \leq d$.

The *Euclidean algorithm*:

Let $a, b \in \mathbb{N}$ with $a > b$. Using the Division Theorem, define natural numbers $a_0, a_1, a_2, \ldots$ as follows.

$a_0 = a$, $a_1 = b$.

If $a_0 = q_1 a_1 + r_1$, where $0 \leq r_1 < a_1$, then define $a_2 = r_1$ if $r_1 \neq 0$, otherwise $gcd(a_0, a_1) = a_1$.

If $a_1 = q_2 a_2 + r_2$, where $0 \leq r_2 < a_2$, then define $a_3 = r_2$ if $r_2 \neq 0$, otherwise $gcd(a_0, a_1) = a_2$.

Continue in this way, so if $a_{n-2} = q_{n-1} a_{n-1} + r_{n-1}$, where $0 \leq r_{n-1} < a_{n-1}$, then define $a_n = r_{n-1}$ if $r_{n-1} \neq 0$, otherwise $gcd(a_0, a_1) = a_n$.

Since $a_0 > a_1 > a_2 > \cdots > a_n$, this process must come to an end (i.e., there is a zero remainder). Suppose $a_{n-1} = a_n q_n$. Then $gcd(a, b) = a_n$.

The calculations involved in the Euclidean algorithm may be used in reverse to find integers $s, t \in \mathbb{Z}$ such that $gcd(a, b) = sa + tb$.

Congruence of integers

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. We say that a and b are *congruent modulo* n if and only if $n | a - b$. In this case we write $a \equiv b \mod n$.

A *linear congruence* is an equation of the form $ax \equiv b \mod n$ to which we wish to find solutions $x \in \mathbb{Z}$.

Relations

Let A be a set with $A \neq \emptyset$. A *relation* R on A is a subset of $A \times A$.
For $x, y \in A$, we write xRy if $(x, y) \in R$ and $x \not R\ y$ if $(x, y) \notin R$.

R is *reflexive* if $\forall\ x \in A,\ xRx$.
R is *symmetric* if $\forall\ x, y \in A,\ xRy \Rightarrow yRx$.
R is *transitive* if $\forall\ x, y, z \in A$, xRy and $yRz \Rightarrow xRz$.

R is an *equivalence relation* if it is reflexive, symmetric and transitive.

Let R be an equivalence relation on a set A. The *equivalence class* of a is

$$R_a = \{x \in A : aRx\}.$$

Let A be a non-empty set. A *partition* of A is a collection of non-empty subsets A_i of A (where $i \in I$ and I is called an *index set*) such that
(i) $\bigcup_{i \in I} A_i = A$ and
(ii) $\forall\ i, j \in I$, either $A_i = A_j$ or $A_i \cap A_j = \emptyset$.

The equivalence classes for an equivalence relation on a set A form a partition of A.

Integers modulo n

Let $n \in \mathbb{N}$. Define $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.

Define addition $\oplus$ on $\mathbb{Z}_n$ as follows: Let $a, b \in \mathbb{Z}_n$. By the division theorem, there are $q \in \mathbb{Z}$ and $r \in \mathbb{Z}_n$ such that $a + b = qn + r$. Define $a \oplus b = r$.

Define multiplication $\odot$ on $\mathbb{Z}_n$ as follows: Let $a, b \in \mathbb{Z}_n$. By the division theorem, there are $q_1 \in \mathbb{Z}$ and $r_1 \in \mathbb{Z}_n$ such that $ab = q_1 n + r_1$. Define $a \odot b = r_1$.

Binary operations

Let S be a set. A *binary operation* $*$ on S is a function

$$* : S \times S \to S.$$

For $a, b \in S$, write $a * b$ instead of $*(a, b)$.

Write $(S, *)$ for a set S equipped with a binary operation $*$.

A binary operation on a finite set may be defined by its *multiplication table*. Label the rows and columns by elements of S. Let $\alpha, \beta \in S$. The entry in the row labeled by α and column labeled by β is $\alpha * \beta$.

Let $*$ be a binary operation on a set S.

$*$ is *commutative* if $\forall\ a, b \in S, a * b = b * a$.

$*$ is *associative* if $\forall\ a, b, c \in S, (a * b) * c = a * (b * c)$.

An element $e \in S$ is an *identity element* for S (with respect to $*$) if

$$\forall\ a \in S,\ e * a = a * e = a.$$

[Note that if an identity element exists, then it is unique.]

Groups

Let G be a non-empty set and $*$ a binary operation on G. We say that $(G, *)$ is a *group* if the following hold:

(G1) $*$ is associative;

(G2) G has an identity element e with respect to $*$;

(G3) $\forall\ g \in G,\ \exists h \in G,\ g * h = h * g = e$.

Note that given $g \in G$, the element h defined in **(G3)** is unique. It is called the *inverse* of g and is denoted by g^{-1}.

A group $(G, *)$ is *commutative* if $*$ is commutative.

Let $p \in \mathbb{N}$ be prime. Define $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. Then $(\mathbb{Z}_p^*, \odot)$ is a commutative group.

Permutations and the symmetric group

Let $n \in \mathbb{N}$. Denote by S_n the set of all permutations of $\mathbb{N}_n$ (that is, bijections $\mathbb{N} \to \mathbb{N}$.

S_n forms a group under composition of functions.

There are two frequently used notations for permutations.

Let $f \in S_n$. For $i \in \mathbb{N}_n$, write $f(i) = r_i$. Then we may write

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ r_1 & r_2 & r_3 & \cdots & r_n \end{pmatrix}.$$

A more concise notation is via *cycles*.

In S_n, write $(\alpha_1 \alpha_2 \cdots \alpha_r)$ for the element $f \in S_n$ such that $f(\alpha_1) = \alpha_2$, $f(\alpha_2) = \alpha_3$, $f(\alpha_3) = \alpha_4$,...,$f(\alpha_{r-1}) = \alpha_r$, $f(\alpha_r) = \alpha_1$, and $f(\alpha) = \alpha$ for all $\alpha \in \mathbb{N}_n \setminus \{\alpha_1, \ldots, \alpha_r\}$. We call $(\alpha_1 \alpha_2 \cdots \alpha_r)$ a *cycle* of *length* r.

Cycles $(\alpha_1 \alpha_2 \cdots \alpha_r)$ and $(\beta_1 \beta_2 \cdots \beta_s)$ are called *disjoint* if

$$\{\alpha_1, \ldots, \alpha_r\} \cap \{\beta_1, \ldots, \beta_s\} = \emptyset.$$

Every element of S_n may be written as a product of disjoint cycles. When writing an element as a product of disjoint cycles, we often omit cycles of length one.

Fields

Let F be a non-empty set and let $+$ and $*$ be binary operations on F. We say $(F, +, *)$ is a *field* if the following are satisfied:

(F1) $(F, +)$ is a commutative group (write 0 for the identity element);

(F2) $(F \setminus \{0\}, *)$ is a commutative group (write 1 for the identity element);

(F3) $\forall\ a, b, c \in F$, $a * (b + c) = a * b + a * c$ ($*$ is *distributive* over $+$).