Important Definitions (in Chapter II: *Groups*)

Group (see Text p. 59 and p. 93)

A *group* is a set with a multiplication (given by a map $G\times G\to G$, $(a,b)\mapsto ab$ which satisfies the axioms

A1: For all $a,b,c \in G$, $(ab)c = a(bc)$

A2: There is an element $e\in G$ with the property that for all $a\in G$, $ea = a = ae$.

A3: For every $a\in G$ there is some $a'\in G$ with the property $aa' = e = a'a$.

FACT: There is only one element e satisfying A2, and for every $a\in G$ only one element a' satisfying A3 – usually denoted a^{-1}.

Order (see Text p. 70)

The *order of a group* G is the number of elements in G and denoted $|G|$.

The *order of an element* $a\in G$ is the smallest natural number n with $a^n = e$.

FACT: The order of the element $a\in G$ is equal to the order of the cyclic subgroup generated by a (see below).

Subgroup (see Text p. 95)

A subset S of G is a *subgroup* of G, in symbols $S\leqslant G$, if the following holds.

i) S contains the neutral element e of G,
ii) if a is in S, so is its inverse a^{-1},
iii) if both a and b are in S, so is the product ab.

Commuting elements (see Text p. 146, 151)

Let a,b be elements of a group G. We say a *commutes* with b if ab=ba.

The *centralizer* of an element $a\in G$ is the subgroup $C(a) = \{x\in G \mid x \text{ commutes with } a\}$

The *center* Z(G) of the group G is the subgroup $Z(G) = \{a\in G \mid C(a) = G\}$. In other words, the elements of the center commute with all elements of G.

Cyclic subgroups and cyclic groups. (see Text p. 164)

If $a\in G$ then $gp(a) = \{a^n \mid n\in\mathbb{Z}\}$ is the *cyclic subgroup* of G generated by a.

A group G is *cyclic* if it is generated by a single element. I.e., G contains an $a\in G$ with $G=gp(a)$.

FACT: Structure Theorem for cyclic groups: 1.Every cyclic group isomorphic to either $(\mathbb{Z},+)$ or $(\mathbb{Z}_m,+)$, where $\mathbb{Z}_m$ stands for the integers mod m.
2. All subgroups of a cyclic group are cyclic.

Generating subgroups (see Text p. 164)

Let $X\subseteq G$ be a subset of a group G. Then G contains a well defined smallest subgroup containing X. This subgroup denoted gp(X). It can explicitly be described as follows: Let $Y = X\cup X^{-1}$, where X^{-1} stands for the set of all inverses of the elements of X: then gp(X) consists of all finite products $y_1y_2...y_n$ with n an integer $\geqslant 0$ and all $y_i\in Y$. gp(X) is called *the subgroup of* G *generated by* X.

Conjugation (see Text p. 130-131)

Two elements a, b of a group G are *conjugate in* G if there is an element $t\in G$ with $tat^{-1} = b$.

If $S\leqslant G$ is a subgroup, and $t\in G$ then $tSt^{-1} = \{tst^{-1} \mid s\in S\}$ is also a subgroup, and we say that the two subgroups are *conjugate to each other*.

Conjugation in S_n: (Text 135 - 141)

Cosets (see Text p. 154 - 156)

Given is a group G and a subgroup $S \leqslant G$. For each $a \in G$ the subset $aS = \{as | s \in S\} \subseteq G$ is called the *left cosets of* S represented by a. Correspondingly, $Sa = \{sa | s \in S\} \subseteq G$ is the right coset represented by a. In general Sa and aS are different subsets of G. But taking a=e shows that S is both a left coset and a right coset mod S.
The number of left cosets is equal to the number of right cosets, is called the index of the subgroup S in G, and denoted $|G:S|$ or $|G/S|$.

Lagrange's Theorem: $|G| = |G:S||S|$.
As a consequence one finds that if S is a subgroup of a finite group G then $|S|$ is a divisor of $|G|$, that every group G with $|G|=p$ a prime is cyclic, and that for each element $a \in G$, $a^{|G|} = e$.

Normal subgroups and quotient groups. (see text p. 168 - 175)

A subgroup $N \leqslant G$ is said to be *normal in* G (or a *normal divisor of* G) if aN = Na for each $a \in G$.
An equivalent (and more insightful) way to say this is that for each $a \in G$ $aNa^{-1} \subseteq N$ – in other words: The subgroup N coincides with all its conjugate subgroups.
If N is a normal subgroup of G then one the set of all cosets $G/N = \{aN | a \in G\}$ carries the structure of a group: (aN)(bN) = abN, neutral element N, inverse $(aN)^{-1} = a^{-1}N$. G/N is the *quotient group* (*factor group*) of G mod N.

Homomorphisms (see text p. 97 – 100, 167, 174-175)

A *homomorphism* $f: G \rightarrow H$ between two groups G, H, is a map with the property that for all $a,b \in G$ we have f(ab) = f(a)f(b). f(G), the *image of* f, is a subgroup of H, and K = ker(f) **– the kernel of** f **–** is a normal subgroup of G.

Isomorphism Theorem: If $f: G \rightarrow H$ is a homomorphism with kernel K then putting If f'(aK) = f(a) for all $a \in G$ yields defines an injective homomorphism $f': G/K \rightarrow H$ which yiekds an isomorphism between G/K and f(G).