School of Mathematical Sciences
PURE MTH 3007
Groups and Rings III, Semester 1, 2009

Week 1 Summary

Week 1 — Lecture 1 — Tuesday 3 March.

---

1. Introduction (Background from Algebra II)

1.1. Groups and Subgroups.

Definition 1.1. A *binary operation* on a set G is a function $G \times G \to G$ often written just as juxtoposition, i.e $(x, y) \mapsto xy$.

Definition 1.2. A *group* is a set G with a binary operation $G \times G \to G$, $(x, y) \mapsto xy$, a function $G \to G$, $x \mapsto x^{-1}$ called the *inverse* and an element $e \in G$ called the *identity* satisfying:
(a) $(xy)z = x(yz) \quad \forall x, y, z, \in G$
(b) $ex = x = xe \quad \forall x \in G$, and
(c) $xx^{-1} = e = x^{-1}x \quad \forall x \in G$.

Definition 1.3. Let G be a group.
(a) For $x, y \in G$ we say that x and y *commute* if $xy = yx$.
(b) If every x, y in G commute we call G an *abelian* group.

Proposition 1.4. *(Basic properties of groups).*
(a) The identity is unique. That is if $f \in G$ and $fx = x = xf$ for all $x \in G$ then $f = e$.
(b) If $x \in G$ then x^{-1} is unique. That is if $xy = e = yx$ then $y = x^{-1}$.
(c) Any bracketing of a multiple product $x_1x_2 \cdots x_n$ gives the same outcome so no bracketing is necessary.
(d) Cancellation laws hold. That is if $ax = ay$ then $x = y$ and if $xa = ya$ then $x = y$.

Definition 1.5. If $H \subset G$ we say that H is a *subgroup* of G if:
(a) $\forall x, y \in H$ we have $xy \in H$,
(b) $\forall x \in H$ we have $x^{-1} \in H$ and
(c) $e \in H$.

Note 1.1. If H is a subgroup of G we write $H < G$. If $H < G$ and $H \neq G$ we say that H is a proper subgroup of G.

Proposition 1.6. *(Properties of subgroups)*
(a) If $H \subset G$ then H is a subgroup if and only if for all $x, y \in H$ we have $xy^{-1} \in H$.
(b) $\langle e \rangle < G$ and $G < G$.
(c) If H and K are subgroups of G then $H \cap K$ is a subgroup of G.

Note 1.2. Sometimes it is useful to draw the *subgroup lattice* of a group G. This is a directed graph whose nodes are the subgroups of G with H and H' joined by a directed edge if $H < H'$. We usually draw this vertically with G at the top and $\langle e \rangle$ at the bottom.

Definition 1.7. If G is a group and has a finite number of elements we call it a *finite group*. The number of elements is called the *order* of G and denoted $|G|$. If G is not a finite group we call it an *infinite group* and say it has *infinite order*.

If $G = \{x_1, \ldots, x_n\}$ is a finite group the *multiplication table* of G is formed from all the products:

	x_1	x_2	$\cdots$	x_n
x_1	x_1x_1	x_1x_2	$\cdots$	x_1x_n
x_2	x_2x_1	x_2x_2	$\cdots$	x_2x_n
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_n	x_nx_1	x_nx_2	$\cdots$	x_nx_n

Note 1.3. If $x \in G$ then we write $x^0 = e$, $x^k = xx \cdots x$ where there are k x's in the product and $x^{-k} = (x^{-1})^k$.

Definition 1.8. If G is a group and $x \in G$ we say that x has *order* n if n is the smallest non-negative integer for which $x^n = e$. We denote the order of x by $|x|$. If $x^n \neq e$ for all n we say that x has *infinite* order.

Definition 1.9. If G is a group and $X \subset G$ we define $\langle X \rangle$ to be the smallest subgroup of G containing X and called it the *subgroup generated* by X.

Note 1.4. If $X \subset G$ then $\langle X \rangle$ consists of all arbitrary products of elements of X with arbitrary integer powers.

Definition 1.10. If G is a group with $X \subset G$ and $\langle X \rangle = G$ we say that X *generates* G. If X is finite we say that G is *finitely generated*.

Definition 1.11. If G is a group which is generated by one element $x \in G$ we call G *cyclic*.

Note 1.5. Cyclic groups are abelian.

Theorem 1.12. *Any subgroup of a cyclic group is cyclic.*

Note 1.6. If $G \simeq \langle x \rangle$ has finite order n then the subgroups of G are exactly the subsets $\langle x^d \rangle$ where $d|n$. If $G = \langle x \rangle$ is infinite then each $\langle x^d \rangle$ is a subroup for $d = 1, 2, \ldots$.

Week 1 — Lecture 2 — Wednesday 4th March.

1.2. Examples of Groups.

(1) The integers $\mathbb{Z}$, the rationals $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are all abelian groups under addition.
(2) The sets of $n \times n$ matrices, $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ are abelian groups under matrix addition.
(3) $\mathbb{Z}^\times = \mathbb{Z} - \{0\}$ is not a group under multiplication but $\mathbb{Q}^\times$, $\mathbb{R}^\times$ and $\mathbb{C}^\times$ are.
(4) $GL(n, \mathbb{R})$ the set of all invertible matrices in $M_n(\mathbb{R})$ is a group as is $GL(n, \mathbb{C})$.

Example 1.1. (The quaternion group.) Let $\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$ and define the multiplication by letting the identity be 1 and assuming that -1 commutes with everything else and that also

$$ij = -ji = k, jk = -kj = i, ki = -ik = j, i^2 = j^2 = k^2 = -1 \quad \text{and} \quad ijk = -1.$$

This group $\mathbb{H}$ is called the quaternion group. It is not abelian and has order 8.

Example 1.2. (Integers modulo n.) Define $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ and define a binary operation on it by using addition modulo n. That is we add x and y to get $x + y$ and then calculate the remainder modulo n. This makes $\mathbb{Z}_n$ into an abelian group which is cyclic and generated by 1.

Proposition 1.13. *The set $\mathbb{Z}_p^\times = \mathbb{Z}_p - \{0\}$ is a group under multiplication if and only if p is prime.*

Definition 1.14. A *field* is a set $\mathbb{F}$ with two binary operations $+, \cdot$ such that
(a) $(\mathbb{F}, +)$ is an abelian group
(b) $(\mathbb{F}^\times, \cdot)$ is an abelian group, where $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$
(c) $a(b + c) = ab + ac$ for all $a, b, c \in \mathbb{F}$.

Some examples of fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ where p is prime. The latter example is also denoted $GF(p)$.

1.2.1. *Matrix groups.*

The set $GL(n, \mathbb{F})$ of all invertible $n \times n$ matrices over a field $\mathbb{F}$ is a group under matrix multiplication.

Some subgroups of $GL(n, \mathbb{F})$ are $SL(n, \mathbb{F})$, scalar matrices and diagonal matrices. We denote $GL(n, \mathbb{Z}_p)$ also by $GF(n, p)$.

Week 1 — Lecture 3 — Friday 6th March.

1.2.2. *Permutation groups.*

Definition 1.15. A *permutation* on n letters is a $1-1$, onto function from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$.

For a given n, the set of all these forms a group S_n under composition of functions called the *symmetric group* on n letters.

Recall

(1) I will use composition of functions so if $\alpha, \beta \in S_n$ then $\alpha\beta$ is defined by $\alpha\beta(k) = \alpha(\beta(k))$.
(2) $|S_n| = n!$
(3) Each element of S_n can be written as a product of disjoint *cycles*. This decomposition is unique up to the order of writing the cycles.
(4) The group S_n is not abelian if $n \geq 3$.
(5) A *transposition* is a cycle of length 2. Every permutation can be written as a product of transpositions.
(6) A permutation is called *even* or *odd* according to whether it is the product of an even or odd number of transpositions. The set of all *even* permutations in S_n is a group, the *alternating group* A_n on n letters, and $|A_n| = \frac{n!}{2}$.
(7) A cycle of even length is an odd permutation and a cycle of odd length is an even permutation.

Definition 1.16. A *permutation group of degree n* is a subgroup of S_n.

1.2.3. *Symmetry groups.* The symmetries of the square form a group of order 8, the *dihedral* group D_4. Similarly, the symmetries of the regular n-gon form a group of order $2n$, the nth dihedral group D_n. Clearly $D_n < S_n$, so D_4 is another example of a permutation group of degree 4.

1.3. **Isomorphism.**

Definition 1.17. Two groups G and H are called *isomorphic* if there is a $1-1$, onto function $\phi \colon G \to H$ such that for all $x, y \in G$ we have $\phi(xy) = \phi(x)\phi(y)$.

Note 1.7. We call such a ϕ an isomorphism. If G and H are isomorphic, we write $G \simeq H$.

Proposition 1.18. *Assume that $\phi \colon G \to H$ is an isomorphism and that $x \in G$. Denote the identities of G and H by e_G and e_H. Then*

(a) $\phi(e_G) = e_H$.
(b) $\phi(x^{-1}) = (\phi(x))^{-1}$
(c) $|G| = |H|$
(d) Either x and $\phi(x)$ are both of infinite order or they have equal finite order.
(e) If G is abelian so is H.