School of Mathematical Sciences
PURE MTH 3007
Groups and Rings III, Semester 1, 2010

Outline of the course

Week 1 — Lecture 1 — Monday 1 March 2010.

---

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.

Note 1.2. A subgroup is a group.

Proposition 1.6. *(Properties of subgroups)*

(a) If $H \subset G$ then H is a subgroup if and only if $H \neq \emptyset$ and 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.

Week 1 — Lecture 2 — Tuesday 2nd March 2010.

Note 1.3. 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. If we have $H < H' < H''$ then we obviously have $H < H''$ but we usually omit that edge to stop the graph becoming too complicated.

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:

$$\begin{array}{c|cccc} & x_1 & x_2 & \cdots & x_n \\ \hline \\ x_1 & x_1x_1 & x_1x_2 & \cdots & x_1x_n \\ x_2 & x_2x_1 & x_2x_2 & \cdots & x_2x_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & x_nx_1 & x_nx_2 & \cdots & x_nx_n \end{array}$$

Note 1.4. 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 1.5. 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 1.6. Cyclic groups are abelian.

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

Note 1.7. 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 $d = 1, 2, \ldots$.

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.

Week 2 — Lecture 3 — Tuesday 9th March 2010.

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 $GF(n, p)$.

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.

Week 2 — Lecture 4 — Thursday 11th March 2010.

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 1.8. 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.

2. Cosets and Normal Subgroups

2.1. **Cosets.**

Definition 2.1. Let $H < G$. A *left coset* of H in G is a set of the form

$$xH = \{xh \mid h \in H\},$$

where x is an element of G. Similarly, a *right coset* is a set of the form

$$Hx = \{hx \mid h \in H\}.$$

Proposition 2.2. *Let $H < G$. Then*

(a) $|gH| = |H| = |Hg|$.
(b) If $x, y \in G$ *then either* $x^{-1}y \in H$ *and* $xH = yH$ *or* $x^{-1}y \notin H$ *and* $xH \cap yH = \emptyset$.
(c) If $x, y\ inG$ *then either* $yx^{-1} \in H$ *and* $Hx = Hy$ *or* $yx^{-1} \notin H$ *and* $xHx \cap Hy = \emptyset$.
(d) Every element of G *is in exactly one left coset of* H *and exactly one right coset of* H.
(e) G *is the disjoint union of the left (or right) cosets of* H.

Week 3 — Lecture 5 — Monday 15th March 2010.

Definition 2.3. If $H < G$, the *index* of H in G is the number of distinct left cosets of H in G. It is denoted $(G : H)$.

Theorem 2.4. *(Lagrange's Theorem) If* H *is a subgroup of a finite group* G *then*

$$(G : H) = \frac{|G|}{|H|}$$

and thus $|H|$ *divides* $|G|$.

Corollary 2.5. *If* x *is an element of the finite group* G, *then* $|x|$ *divides* $|G|$.

Corollary 2.6. *Every group of prime order is cyclic.*

2.2. **Normal subgroups.** If $H < G$ and $g \in G$, the left coset gH and the right coset Hg are in general not the same set. For example, consider $G = S_3 = \{1, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$ and the subgroup $H = \{1, (1\,2)\}$.

Left cosets of H	Right cosets of H
$1H = \{1, (1\ 2)\}$	$H1 = \{1, (1\ 2)\}$
$(1\ 2)H = \{(1\ 2), 1\}$	$H(1\ 2) = \{(1\ 2), 1\}$
$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$	$H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$
$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}$	$H(2\ 3) = \{(2\ 3), (1\ 2\ 3)\}$
$(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\}$	$H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 3)\}$
$(1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3)\}$	$H(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 3)\}$

Compare this example with what we get when we consider the subgroup $A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$:

Left cosets of A_3	Right cosets of A_3
$1A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$	$A_31 = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$
$(1\ 2)A_3 = \{(1\ 2), (2\ 3), (1\ 3)\}$	$A_3(1\ 2) = \{(1\ 2), (1\ 3), (2\ 3)\}$
$(1\ 3)A_3 = \{(1\ 3), (1\ 2), (2\ 3)\}$	$A_3(1\ 3) = \{(1\ 3), (2\ 3), (1\ 2)\}$
$(2\ 3)A_3 = \{(2\ 3), (1\ 3), (1\ 2)\}$	$A_3(2\ 3) = \{(2\ 3), (1\ 2), (1\ 3)\}$
$(1\ 2\ 3)A_3 = \{(1\ 2\ 3), (1\ 3\ 2), 1\}$	$A_3(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 3\ 2), 1\}$
$(1\ 3\ 2)A_3 = \{(1\ 3\ 2), 1, (1\ 2\ 3)\}$	$A_3(1\ 3\ 2) = \{(1\ 3\ 2), 1, (1\ 2\ 3)\}$

We see that $gA_3 = A_3\,g$ for every $g \in A_3$.

Definition 2.7. A subgroup H of a group G is *normal* if for all $g \in G$, $gHg^{-1} = H$.

We write $H \lhd G$. Equivalently, $H \lhd G$ if $gH = Hg$ for all $g \in G$.

Note 2.1. We saw in the above examples that $\{1, (1\,2)\} \not\lhd S_3$ and $A_3 \lhd S_3$.

Proposition 2.8.

(a) Whenever $(G : H) = 2,\ \ H \lhd G$. *In particular,* $A_n \lhd S_n$ *for* $n = 3, 4, 5, \ldots$.
(b) Every subgroup of an abelian group is normal.
(c) $\{1\} \lhd G$ *and* $G \lhd G$.
(d) If $H \lhd G$ *and* $K \lhd G$ *then* $H \cap K \lhd G$.
(e) If $N \lhd G$ *and* $N < H < G$ *then* $N \lhd H$.

2.3. **Conjugation.**

Definition 2.9. Let $g \in G$ and let $X \subset G$. Then the subset gXg^{-1} is called a *conjugate* of X in G. In particular, if $x \in G$, then the element gxg^{-1} is called a *conjugate* of x (in G).

Week 3 — Lecture 6 — Tuesday 16th March 2010.

Note 2.2.

(1) A conjugate of x has the same order as x. (Assignment 1)
(2) We say that x is *conjugate to* y if y is a conjugate of x, ie if there is some $g \in G$ with $y = gxg^{-1}$.

Proposition 2.10. *Conjugacy is an equivalence relation on G.*

Note 2.3. The equivalence class of x is called the *conjugacy class* of x and denoted $[x]$. The conjugacy classes partition G:

$$G = [1] \cup [x] \cup \ldots \cup [z].$$

2.3.1. *Centralizer.*

Definition 2.11. The *centralizer* $C_G(x)$ of x in G is the subgroup consisting of all elements of G that commute with x.

Thus, $C_G(x) = \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\}$.

Note 2.4.

(1) $\langle x \rangle < C_G(x)$.
(2) If G is abelian, then $C_G(x) = G$.

Proposition 2.12. *If $x \in G$ a finite group then $|[x]| = (G : C_G(x))$.*

2.3.2. *Centre.*

Definition 2.13. The *centre* $Z(G)$ of a group G is the subgroup of G consisting of all elements $x \in G$ that commute with *every* elements of G.

Thus, $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$.

Note:

(1) $Z(G) \lhd G$.
(2) $Z(G) = G$ if and only if G is abelian.
(3) $x \in Z(G)$ if and only if $[x] = \{x\}$, or equivalently $|[x]| = 1$.

2.3.3. *Simple groups.*

Definition 2.14. A group G is called *simple* if G has no proper non-trivial normal subgroups.

Week 4 — Lecture 7 — Monday 22nd March 2010.

Theorem 2.15. *An abelian simple group G with $|G| > 1$ must be isomorphic to C_p for some prime p.*

Definition 2.16. A group of order p^n, where p is prime, is called a *p-group*.

Lemma 2.17. *Let P be a p-group of order p^n, $n \geq 1$. Then $Z(P) \neq \langle e \rangle$. Thus P is not simple unless $n = 1$, that is $P \simeq C_p$.*

2.3.4. *Conjugates of a subgroup, and the normalizer.* If $H < G$, the conjugates of H are the subgroups gHg^{-1}, for $g \in G$.

Definition 2.18. The *normalizer* of a subgroup H of G is the subgroup

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Note 2.5. $N_G(H)$ is the largest subgroup of G in which H is normal. That is if $H \triangleleft N_G(H)$, and if $H \triangleleft K < G$ then $K < N_G(H)$.

Proposition 2.19. *If H is a subgroup of a finite group G then the number of distinct conjugates of H in G equals $(G : N_G(H))$.*

3. Homomorphisms and Factor Groups

3.1. **Homomorphisms.**

Definition 3.1. If G and H are groups, a *homomorphism* from G to H is a function $f : G \to H$ such that

$$f(xy) = f(x)f(y)$$

for all $x, y \in G$.

Week 4 — Lecture 8 — Tuesday 23rd March 2010.

Proposition 3.2. *If $f : G \to H$ is a homomorphism, then*

(1) $f(e) = e$.
(2) $f(g^{-1}) = (f(g))^{-1}$.
(3) *The* image *of f,* $\mathrm{im}(f) = f(G) = \{f(g) \mid g \in G\}$, *is a subgroup of H.*
(4) *The* kernel *of f,* $\ker f = \{g \in G \mid f(g) = e\}$, *is a normal subgroup of G.*
(5) *A homomorphism f is one to one if and only if* $\ker f = \langle e\rangle$. *So f is an isomorphism if and only if* $\ker f = \{e\}$ *and* $\mathrm{im}(f) = H$.

Proposition 3.3. *Let $f : G \to H$ be a homomorphism of groups. If $K \subset G$ define $f(K) = \{f(k) \mid k \in K\} \subset H$ and if $L \subset H$ define $f^{-1}(L) = \{g \in G \mid f(g) \in L\} \subset G$. We have:*

(a) *If $K < G$ then $f(K) < H$.*
(b) *If $L < H$ then $f^{-1}(L) < G$.*
(c) *If $K \triangleleft G$ and f is onto then $f(K) \triangleleft H$.*
(d) *If $L \triangleleft H$ then $f^{-1}(L) \triangleleft G$.*

3.2. **The factor group.** Let $N \triangleleft G$. Consider the set

$$G/N = \{gN \mid g \in G\}$$

of left cosets of N in G. This set is a group under the operation

$$gNhN = (gh)N.$$

This group is called the *factor or quotient group* of G by N. Its order is $|G|/|N| = (G : N)$.

Theorem 3.4. (Homomorphism Theorem) *Let $f : G \to H$ be a homomorphism. Then the groups $G/\ker f$ and $f(G)$ are isomorphic.*

Theorem 3.5. *Let $N \triangleleft G$. Then the function $f : G \to G/N$ given by $f(g) = gN$ is a homomorphism with kernel N.*

Week 4 — Lecture 9 — Thursday 25th March 2010.

3.3. **Related results.**

Lemma 3.6. *Let G be a group such that $G/Z(G)$ is cyclic. Then G is abelian.*

Corollary 3.7. *$G/Z(G)$ cannot be cyclic of order greater than one.*

Lemma 3.8. *Every group of order p^2 is abelian.*

Theorem 3.9. *Let $N \lhd G$. Then there is a 1-1 correspondence between subgroups of G containing N and subgroups of G/N, namely*

$$\text{if } N < H < G \text{ then } H \leftrightarrow H/N.$$

Every subgroup of G/N is of form H/N for some subgroup H of G containing N.

Also, $H \lhd G$ if and only if $H/N \lhd G/N$.

3.4. **Composition series.**

Definition 3.10. Let $N \lhd G$. Then N is called a *maximal normal subgroup* of G if the only normal subgroup of G that properly contains N is G itself.

Then N is a maximal normal subgroup of G if and only if G/N is simple.

Definition 3.11. A *composition series* of a group G is a sequence of subgroups

$$\{e\} = N_{k+1} \lhd N_k \lhd \ldots \lhd N_2 \lhd N_1 \lhd N_0 = G,$$

such that each N_{i+1} is a maximal normal subgroup of N_i. That is, each factor group N_i/N_{i+1} is simple.

Theorem 3.12. *The* Jordan-Hölder Theorem *states that for any composition series, the number of factors k and the set of factor groups $\{N_i/N_{i+1} \mid i = 0, 1, \ldots, k\}$ is unique.*

3.5. **The derived group.**

Let X be a subset of G. Then $H = \langle X \rangle$ denotes the smallest subgroup of G containing X. We say that H is *generated* by X. Then H is the set of all products of the form $x_i^{n_i} \ldots x_j^{n_j}$, where $x_i, \ldots, x_j \in X$ and $n_i, \ldots, n_j \in \mathbb{Z}$.

Definition 3.13. The commutator of the elements $g, h \in G$ is $[g, h] = ghg^{-1}h^{-1}$. The *derived group* or *commutator subgroup* of G is the group

$$G' = [G, G] = \langle [g, h] \mid g, h \in G \rangle.$$

Week 5 — Lecture 10 — Monday 29th March 2010.

Note 3.1.

(1) Elements g and h commute if and only if $[g, h] = e$.
(2) $[g, h]^{-1} = [h, g]$.
(3) $G' = \{e\}$ if and only if G is abelian.

Proposition 3.14. *Let G be a group and G' its commutator subgroup. Then:*

(a) $G' \lhd G$.
(b) G/G' is abelian.
(c) If $N \lhd G$ and G/N is abelian, then $G' < N$. Thus G' is the smallest normal subgroup of G with abelian factor group.

4. Products of Groups

4.1. **The isomorphism theorem.**

Let H and K be subgroups of the group G. We define

$$HK = \{hk \mid h \in H, k \in K\}.$$

Then $HK < G$ if and only if $HK = KH$.

In particular, if $H \lhd G$ *or* $K \lhd G$ then $HK < G$.

If $HK < G$, then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Theorem 4.1. (The Isomorphism Theorem) *Let H and K be subgroups of G with $H \lhd G$. Then $HK/H \simeq K/H \cap K$.*

Week 5 — Lecture 11 — Tuesday 30th March 2010.

4.2. **Direct products of groups.** Let H and K be groups. Then we can make the cartesian product

$$H \times K = \{(h,k) \mid h \in H, k \in K\}$$

into a group, called the *(external) direct product* of H and K, by defining

$$(h,k) \cdot (h',k') = (hh', kk')$$

for all $h, h' \in H, k, k' \in K$. Then $H \times K$ has subgroups

$$\begin{aligned} H_0 &= \{(h,e) \mid h \in H\} \simeq H, \\ K_0 &= \{(e,k) \mid k \in K\} \simeq K. \end{aligned}$$

Proposition 4.2. *Let H and K be groups as above. Then:*

(1) $H_0 \cap K_0 = \{(e,e)\} = \{e\}$.
(2) For all $h \in H, k \in K$ we have $(h,e) \cdot (e,k) = (h,k) = (e,k) \cdot (h,e)$. Hence $G = H_0 K_0$.
(3) We write (h,e) as h and (e,k) as k, and identify H_0 and K_0 with H and K. Then every $g \in G$ can be written uniquely as $g = hk$ for $h \in H, k \in K$.
(4) $H \lhd G$ and $K \lhd G$.
(5) $|G| = |H \times K| = |H|.|K|$.
(6) $G/H \simeq K$ and $G/K \simeq H$.

4.3. **The internal direct product.**

Definition 4.3. A group G is *decomposable* if it is isomorphic to a direct product of two proper non-trivial subgroups. Otherwise G is indecomposable.

If G is decomposable then G has subgroups H and K such that

(i) $H \cap K = \{e\}$
(ii) $G = HK$
(iii) $hk = kh$ for all $h \in H, k \in K$.

Then we write $G = H \times K$ and say that G is the *(internal) direct product* of H and K.

Equivalently, if (iii)′ is the statement:

(iii)′ $H \lhd G$ and $K \lhd G$

then (i), (ii) and (iii)′ imply that $G = H \times K$.

Week 5 — Lecture 12 — Tuesday 30th March 2010.

---

5. Finitely generated abelian groups

5.1. The fundamental theorem.

Definition 5.1. A group G is *finitely generated* if there is some finite subset X of G such that $G = \langle X \rangle$.

Thus $G = \langle x_1, ..., x_n \rangle$, the set of all finite products of the x_is and their inverses.

Definition 5.2. If every element of a group G has finite order then G is called a *torsion group*. If only the identity e has finite order then G is called a *torsion-free group*. If G is an abelian group, then the subgroup of G consisting of all elements of finite order is called the *torsion subgroup* of G and denoted $\mathrm{Tor}(G)$.

Theorem 5.3. (Fundamental Theorem of Finitely Generated Abelian Groups) *Every finitely generated abelian group is isomorphic to a direct product of cyclic groups of the form*

$$C_{n_1} \times C_{n_2} \times ... \times C_{n_s} \times C_\infty \times ... \times C_\infty,$$

where each $n_i = p_i^{a_i}$ for some prime p_i and $a_i \in \mathbb{N}$. (The p_i need not be distinct.)

Note:

1. The torsion subgroup of G is $\mathrm{Tor}(G) = C_{n_1} \times C_{n_2} \times ... \times C_{n_s}$. Thus $|T| = n_1 n_2 ... n_s$.
2. The group $F = \underbrace{C_\infty \times ... \times C_\infty}_{f \text{ factors}}$ is torsion free. (It is called a free abelian group of rank f.) The number of factors f is the *(free) rank* or *Betti number* of G. G is finite if and only if $f = 0$.
3. Since $C_n \times C_m \simeq C_{nm}$ if m and n are coprime, we can also write
$$T \simeq C_{d_1} \times ... \times C_{d_t}$$
where $d_1 \mid d_2 \mid ... \mid d_t$ and $|T| = d_1 d_2 ... d_t$. The d_i, known as the *torsion invariants* of G, are unique.
4. Two finitely generated abelian groups are isomorphic if and only if they have the same free rank and the same torsion invariants.

Week 6 — Lecture 13 — Monday 19th April 2010.

Corollary 5.4. *The indecomposable finite abelian groups are precisely the cyclic groups of order p^a, where p is prime, $a \in \mathbb{N}$.*

Corollary 5.5. *If G is a finite abelian group and m divides $|G|$ then G has a subgroup of order m.*

5.2. Generators and relations for abelian groups.

Suppose that an abelian group is defined by generators $x_1, x_2, ..., x_m$ and a number of relations of the form

$$\begin{array}{rcl} x_1^{n_{11}} x_2^{n_{21}} \dots x_m^{n_{m1}} & = & e \\ x_1^{n_{12}} x_2^{n_{22}} \dots x_m^{n_{m2}} & = & e \\ \vdots & & \vdots \\ x_1^{n_{1n}} x_2^{n_{2n}} \dots x_m^{n_{mn}} & = & e. \end{array}$$

We also know that $[x_i, x_j] = e$ for all i, j as G is abelian.

Week 6 — Lecture 14 — Tuesday 20th April 2010.

To determine the rank and torsion invariants of G we use the following procedure.

Write the exponents n_{ij} in a matrix N, with the jth relation corresponding to the jth *column*. There must be at least as many columns as rows, so we have an $m \times n$ matrix with $n \geq m$. (If not, add columns of zeros to make $n \geq m$).

We then use certain row and column operations to reduce N to a diagonal matrix in which the diagonal entries are $d_1, ..., d_t, 0, ..., 0$ and the successive non-zero entries divide one another: $d_1 \mid d_2 \mid ... \mid d_t$. Then the entries $d_1, ...d_t$ are the torsion invariants of G and the number of zeros is the rank of G.

5.2.1. *Permissible row and column operations.*

(i) Interchange any two rows: $R_i,\ R_j \rightsquigarrow R_j,\ R_i$.
(ii) Multiply any row by -1: $R_i \rightsquigarrow -R_i$.
(iii) Add to any row an integer multiple of another row: $R_i \rightsquigarrow R_i + cR_j,\ c \in \mathbb{Z}$.

The corresponding column operations are also permitted.

It is not permissible to:
(i) Multiply a row by c, if $c \neq \pm 1$.
(ii) Replace R_i by $cR_i + dR_j$, if $c \neq \pm 1$.

5.2.2. *Why does it work?* Row operations correspond to changing the generators, column operations to manipulating the relations. Specifically, the row operation $R_i \rightsquigarrow R_i + cR_j$ corresponds to replacing generator x_j by $y_j = x_j x_i^{-c}$.

5.2.3. *Procedure.* The initial aim is to get the g.c.d. of all entries in the matrix to the $(1,1)$ position, and then use this entry as a pivot to eliminate all other entries in the first row and column. Then repeat this procedure on the $(m-1) \times (n-1)$ submatrix obtained by removing the first row and column. Continue.

To get the g.c.d. to the $(1,1)$ position, it will in general be necessary to use the Division Algorithm several times on the rows and/or columns, as in the following examples:

$$\begin{bmatrix} 7 & \cdots \\ 30 & \cdots \end{bmatrix} \sim \begin{bmatrix} 7 & \cdots \\ 2 & \cdots \end{bmatrix} (R_2 \rightsquigarrow R_2 - 4R_1) \sim \begin{bmatrix} 1 & \cdots \\ 2 & \cdots \end{bmatrix} (R_1 \rightsquigarrow R_1 - 3R_2).$$

$$\begin{bmatrix} 15 & 0 \\ 0 & 20 \end{bmatrix} \sim \begin{bmatrix} 15 & 0 \\ 20 & 20 \end{bmatrix} \sim \begin{bmatrix} 15 & 0 \\ 5 & 20 \end{bmatrix} \sim \begin{bmatrix} 5 & 20 \\ 15 & 0 \end{bmatrix} \sim \begin{bmatrix} 5 & 0 \\ 0 & -60 \end{bmatrix} \sim \begin{bmatrix} 5 & 0 \\ 0 & 60 \end{bmatrix}.$$

6. Groups Acting on Sets

6.1. **Introduction.**

Definition 6.1. Let G be a group and X a set. An *action of G on X* is a map $G \times X \to X$, $(g, x) \mapsto g * x$ such that

(i) for each $g_1, g_2 \in G$ and $x \in X$,
$$(g_1 g_2) * x = g_1 * (g_2 * x)$$
(ii) for each $x \in X$, $e * x = x$.

If there is no confusion, we may write gx for $g * x$.

Note:

(1) S_n acts on $X = \{1, 2, ..., n\}$.
(2) G acts on $X = G$ by
  (a) conjugation: $g * x = gxg^{-1}$
  (b) left multiplication: $g * x = gx$.
(3) If $H < G$, G acts on the left cosets of H by left multiplication: $g * xH = gxH$.
(4) If $G = GL(n, F)$ and V is a vector space of dimension n over F, then G acts on V by matrix multiplication.

Definition 6.2. If G acts on X then for any $x \in X$, $[x] = \{g * x \mid g \in G\}$ is called an *orbit* in X of the action.

If there is only one orbit then we say G is *transitive* on X.

Week 6 — Lecture 15 — Thursday 22nd April 2010.

Proposition 6.3. *The orbits of a group G acting on a set X are the equivalence classes under the equivalence relation on X:*

$$x \sim y \text{ if and only if } y = g * x \text{ for some } g \in G.$$

Hence X is the disjoint union of the distinct orbits.

Definition 6.4. If G acts on X then for any $x \in X$, the *stabilizer* of $x \in X$ is

$$S_G(x) = \{g \in G \mid g * x = x\}.$$

The stabilizer of x is a subgroup of G. It is sometimes called the *isotropy subgroup* of x, and sometimes denoted G_x.

6.2. The Orbit-Stabilizer Theorem.

Theorem 6.5. (Orbit-Stabilizer Theorem) *Let G act on X. Then for any $x \in X$,*

$$|[x]| = (G : S_G(x)).$$

Week 7 — Lecture 16 — Tuesday 27th April 2010.

6.3. Burnside's Theorem.

Theorem 6.6. (Burnside's Theorem) *Let G be a finite group and X a finite set such that G acts on X. Let r be the number of distinct orbits of G on X and for each $g \in G$ let*

$$X_g = \{x \in X \mid g * x = x\},$$

the set of all elements in X fixed by g. Then

$$r|G| = \sum_{g \in G} |X_g|.$$

6.3.1. *Application of Burnside's theorem to chemistry.*

Week 8 — Lecture 17 — Monday 3rd May 2010.

6.4. Cayley's Theorem.

Theorem 6.7. (Cayley's Theorem) *Every group is isomorphic to a group of permutations.*

7. The Sylow Theorems

7.1. **Sylow's first theorem.** The results of this chapter are due to the Norwegian mathematician Ludvig Sylow (1832 – 1918), though the proofs have been modernized. Along with Lagrange's theorem, they are the most important results of finite group theory – Lagrange's theorem gives a necessary condition for subgroups, and Sylow's theorems give sufficient conditions.

Theorem 7.1. Sylow's First Theorem *Let G be a finite group of order $p^m r$, where p is a prime and r is coprime to p. Then G has a subgroup P of order p^m.*

Such a subgroup P, the existence of which is guaranteed by this theorem, is called a *Sylow p-subgroup* of G.

Lemma 7.2. *Let G be a finite p-group acting on the finite set X. Let*

$$F = \{x \in X \mid g * x = x \text{ for all } g \in G\}.$$

Then $|F| \equiv |X| \pmod p$.

Week 8 — Lecture 18 — Tuesday 4th May 2010.

7.2. **Sylow's second and third theorems.**

Theorem 7.3. (Sylow's Second Theorem) *Let P be a Sylow p-subgroup of the finite group G of order $p^m r$, where r is coprime to p. If Q is any p-subgroup of G (that is, $|Q|$ is a power of p) then $Q < gPg^{-1}$ for some $g \in G$.*

In particular, all Sylow p-subgroups are conjugate.

Lemma 7.4.
(i) *Let P be a Sylow p-subgroup of G and suppose $P \lhd G$. Then P is the* only *Sylow p-subgroup of G.*
(ii) *In any finite group G, P is the only Sylow p-subgroup of $N_G(P)$.*

Theorem 7.5. (Sylow's Third Theorem) *Let P be a Sylow p-subgroup of G. Then the number of Sylow p-subgroups of G is $(G : N_G(P))$. Further, $(G : N_G(P)) \equiv 1 \pmod p$.*

Theorem 7.6. (Cauchy's Theorem) *Let p divide $|G|$. Then G contains an element of order p.*

Corollary 7.7. *If p divides $|G|$ then G has a subgroup of order p.*

Week 8 — Lecture 19 — Thursday 6th May 2010.

7.3. **Examples.** We consider the structure of groups of order pq, where p and q are distinct odd primes, groups of order $2p$ where p is prime and groups of order less than or equal to 15.

8. Rings

8.1. **Definitions.**

Definition 8.1. A *ring* is a set R with two binary operations $+, \cdot$ such that

(i) $(R, +)$ is an abelian group
(ii) $a(bc) = (ab)c$ for all $a, b, c \in R$ *(Associative law for multiplication)*
(iii) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$ *(Distributive laws).*

Notes:
(1) As usual, we often omit $\cdot$ and write ab instead of $a \cdot b$.
(2) $(R, \cdot)$ is not necessarily a group – why?

(3) The additive identity of $(R,+)$ is denoted 0. Thus $a+0=0+a=a$ for all $a\in R$.
(4) The additive inverse of $(R,+)$ is denoted $-a$. Thus $a+(-a)=(-a)+a=0$ for all $a\in R$.
(5) R is called *a commutative ring* if $ab=ba$ for all $a,b\in R$.
(6) R is called *a ring with identity* if there is an element $1\neq 0$ in R such that $1.a=a.1=a$ for all $a\in R$.

8.2. **Examples of rings.**

(1) $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ are rings (commutative rings with identity).
(2) For any integer $n\geq 1$, $\mathbb{Z}_n$ is a ring under addition and multiplication $\pmod n$.
(3) For any integer $n\geq 1$, if R is a ring, then the set of $n\times n$ matrices $M_n(R)$ is a ring under the usual operations.
(4) The *Gaussian integers* $\mathbb{Z}(i)=\{a+bi\mid a,b\in\mathbb{Z}\}$.
(5) The set $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$.
(6) The ring of real quaternions

$$\mathbb{R}(\mathbb{H})=\{a+bi+cj+dk\mid a,b,c,d\in\mathbb{R},i^2=j^2=k^2=-1,ij=k,jk=i,ki=j\}.$$

Week 9 — Lecture 20 — Monday 10th May 2010.

8.3. **Properties of rings.**

(1) $0.a=a.0=0$ for all $a\in R$.
(2) $a(-b)=(-a)b=-ab$ for all $a,b\in R$.
(3) $(-a)(-b)=ab$ for all $a,b\in R$.

8.4. **Homomorphisms.**

Definition 8.2. Let R and R' be rings. A function $\phi:R\to R'$ is a *ring homomorphism* if

(i) $\phi(a+b)=\phi(a)+\phi(b)$
(ii) $\phi(ab)=\phi(a)\phi(b)$

for all $a,b\in R$.

The homomorphism ϕ is called an *isomorphism* if it is $1-1$ and onto.

The *kernel* of ϕ is *ker* $\phi=\{a\in R\mid \phi(a)=0\}$.

Note: The homomorphism ϕ is $1-1$ if and only if ker $\phi=\{0\}$.

8.5. **Subrings.**

Definition 8.3. A *subring* S of a ring R is a subset of R that is itself a ring.

Thus S is a subring of R if $(S,+)<(R,+)$ and if S is closed under multiplication.

In particular, if $\phi:R\to R'$ is a ring homomorphism then $\phi(R)$ and ker ϕ are subrings of R' and R respectively.

9. Integral Domains and Fields

9.1. **Definitions.**

Definition 9.1. Let R be a ring with identity 1. A *unit* of R is an element u that has a multiplicative inverse u^{-1}. So, $uu^{-1}=u^{-1}u=1$.

If every non-zero element of R is a unit then R is called a *field* when R is commutative, or a *skewfield* or *division ring* when R is not commutative.

Thus when R is a field, $(R,+)$ and $(R \setminus \{0\}, \cdot)$ are both abelian groups.

Definition 9.2. Let R be a ring. Non-zero elements a, b of R such that $ab = 0$ are called *zero-divisors.*

The ring $\mathbb{Z}_n$ $(n > 1)$ has no zero-divisors if and only if n is prime.

Definition 9.3. An *integral domain* is a commutative ring with identity which has no zero-divisors.

Examples:

(1) $\mathbb{Z}$ is an integral domain.
(2) If p is prime, $\mathbb{Z}_p$ is an integral domain.
(3) If n is composite, Z_n is not an integral domain.
(4) Every field is an integral domain.

Theorem 9.4. *Every finite integral domain is a field.*

Corollary 9.5. *If p is a prime, then $\mathbb{Z}_p$ is a field.*

Week 9 — Lecture 21 — Tuesday 11th May 2010.

9.2. **The field of quotients of an integral domain.** Let D be an integral domain. Then we can construct a field F containing D as follows:

Let
$$S = \{(a,b) \in D \times D \mid b \neq 0\}.$$

Define an equivalence relation on S by
$$(a,b) \sim (c,d) \text{ if } ad = bc.$$
Let F be the set of equivalence classes under this relation:
$$F = \{[(a,b)] \mid a, b \in D, b \neq 0\}.$$

Define operations of addition and multiplication on F by
$$[(a,b)] + [(c,d)] = [(ad + bc, bd)]$$
and
$$[(a,b)] \cdot [(c,d)] = [(ac, bd)].$$

Then F is a field under these operations and F contains an integral domain
$$\overline{D} = \{[(a,1)] \mid a \in D\}$$
which is isomorphic to D. We usually say that $D \subset F$.

The field F is called the *field of quotients* of D. This field is the smallest field containing D, and is unique up to isomorphism.

10. Polynomials

10.1. **Basic operations.** Let R be a ring. We denote by $R[x]$ the set of all *polynomials* in x with coefficients in R. Here x is an 'indeterminate', not a variable or element of R.

Thus
$$R[x] = \left\{ \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \dots \;\middle|\; a_i \in R, \text{ only a finite number of } a_i \text{ non-zero} \right\}.$$

The *degree* of the polynomial $f(x)$ is the largest i such that $a_i \neq 0$. It is conventional to say that the zero polynomial 0 has degree $-\infty$.

10.1.1. *Addition and multiplication of polynomials.* If

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + \dots \\ g(x) &= b_0 + b_1x + b_2x^2 + \dots \end{aligned}$$

then

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots$$

and

$$f(x)g(x) = d_0 + d_1x + d_2x^2 + \dots$$

where $d_i = \sum_{j=0}^{i} a_j b_{i-j}$. Note that with these definitions,

$$\deg f(x)g(x) \le \deg f(x) + \deg g(x)$$

and

$$\deg(f(x) + g(x)) \le \max\{\deg f(x), \deg g(x)\}.$$

Under these operations, $R[x]$ is a ring.

If R is commutative, so is $R[x]$. If R has an identity 1, so has $R[x]$.

More generally, we can define the polynomial ring $R[x_1, x_2, \dots, x_n]$ in n indeterminates $x_1, x_2, \dots, x_n$ by

$$R[x_1, x_2, \dots, x_n] = (R[x_1, x_2, \dots, x_{n-1}])[x_n].$$

10.2. **Polynomials over an integral domain and field.** If D is an integral domain, so is $D[x]$ and hence so is $D[x_1, x_2, \dots, x_n]$. In this case

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

If F is a field, then $F[x]$ is an integral domain but *not* a field.

Week 10 — Lecture 22 — Monday 17th May 2010.

10.2.1. *The division algorithm.*

Lemma 10.1 (Division algorithm for $\mathbb{Z}$)**.** *Let m and n be integers with $m \neq 0$. Then there are unique integers q and r such that*

$$n = qm + r$$

and $0 \le r < m$.

Lemma 10.2 (Division algorithm for $F[x]$)**.** *Let F be a field and $f(x), g(x)$ be polynomials in $F[x]$ with $g(x) \neq 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that*

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

and $\deg r(x) < \deg g(x)$.

Note that $g(x) \mid f(x)$ if and only if $r(x) = 0$.

10.3. **Polynomial functions.** Let R be a ring and $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ a polynomial over R. Then the function $\overline{f} : R \to R$ given by $\overline{f}(r) = a_0 + a_1r + a_2r^2 + \cdots$ is called the *polynomial function* associated to f.

The set $\mathcal{P}(R)$ of all polynomial functions over R is a ring under the operations $(\overline{f} + \overline{g})(r) = \overline{f}(r) + \overline{g}(r)$ and $(\overline{f}\overline{g})(r) = \overline{f}(r).\overline{g}(r)$. It is then easy to show that

$$\overline{f} + \overline{g} = \overline{f + g}, \quad \overline{f}\,\overline{g} = \overline{fg}.$$

If R is a commutative ring with identity then so is $\mathcal{P}(R)$, but note that $\mathcal{P}(R)$ is not necessarily isomorphic to $R[x]$.

10.3.1. *Zeros of polynomials.* Let F be a field.

Definition 10.3. An element $a \in F$ is a *zero* of $f(x) \in F[x]$ if $\overline{f}(a) = 0$.

Theorem 10.4 (Factor Theorem)**.** *The element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a \mid f(x)$.*

Corollary 10.5. *A polynomial of degree n over a field F has at most n zeros in F.*

Week 10 — Lecture 23 — Tuesday 18th May 2010.

Definition 10.6. A non-constant polynomial $f(x) \in F[x]$ is *irreducible over F* if

$f(x) \neq g(x)h(x)$ for any polynomials $g(x), h(x)$ of degree less than $f(x)$.

11. Ideals

11.1. **Introduction.**

Definition 11.1. A subring I of a ring R is called an *ideal* of R if for all $r \in R$ and $i \in I$ we have $ir \in I$ and $ri \in I$.

11.2. **The Factor Ring.**

Theorem 11.2 (The Factor Ring)**.** *Let I be an ideal of the ring R. Then the set R/I of all cosets of I in R is a ring under the operations*

$$\begin{aligned} (r+I)+(s+I) &= (r+s)+I \\ (r+I).(s+I) &= rs+I. \end{aligned}$$

If R is a commutative ring, or a ring with identity, then so is R/I.

Lemma 11.3. *Let $\phi : R \to S$ be a ring homomorphism. Then* $\ker \phi$ *is an ideal of R.*

Theorem 11.4 (Homomorphism Theorem)**.** *If $\phi : R \to S$ is a ring homomorphism then*

$$R/ker\ \phi \simeq \phi(R).$$

Week 10 — Lecture 24 — Thursday 20th May 2010.

Lemma 11.5. *If I and J are ideals of R then so are $I + J$ and $I \cap J$.*

Theorem 11.6 (Isomorphism Theorem)**.**

(i) *Let I be an ideal of R. Then there is a $1-1$ correspondence between subrings S of R containing I and subrings S/I of R/I. Here S is an ideal of R if and only if S/I is an ideal of R/I.*

(ii) *Let $I \subset J \subset R$ with I and J ideals of R. Then*

$$R/J \simeq (R/I)/(J/I).$$

(iii) *Let I and J be ideals of R. Then*

$$(I+J)/J \simeq I/(I \cap J).$$

11.3. **Ideals in commutative rings with identity.** Let R be a commutative ring with identity.

Definition 11.7. An ideal of the form $\langle a \rangle = \{ar \mid r \in R\}$ is called a *principal* ideal of R.

An ideal M of R is called a *maximal* ideal if there is no ideal I of R such that $M \subset I \subset R$.

Theorem 11.8. *Let R be a commutative ring with identity. Then M is a maximal ideal of R if and only if R/M is a field.*

12. Factorization in Integral Domains

12.1. Irreducibles and associates.

Definition 12.1. An element c of an integral domain, not zero or a unit, is called *irreducible* if, whenever $c = df$, one of d or f is a unit.

Elements c and d are called *associates* if $c = du$ for a unit u.

12.2. Euclidean domains.

Definition 12.2. A *Euclidean domain* is an integral domain D together with a function $\delta : D^* \to \mathbb{N}$ satisfying

(i) $\delta(a) \leq \delta(ab)$ for all non-zero $a, b \in D$
(ii) for all $a, b \in D$, $b \neq 0$ there exist $q, r \in D$ such that

$$a = bq + r$$

with either $r = 0$ or $\delta(r) < \delta(b)$.

The function δ is called a *Euclidean valuation*.

Examples:

(1) $\mathbb{Z}$ with $\delta(n) = |n|$.
(2) $F[x]$ with $\delta(f(x)) = \deg f(x)$, where F is a field.

Week 11 — Lecture 25 — Monday 24th May 2010.

Note 12.1. (a) If $a \in D^*$ then $\delta(1) \leq \delta(a)$.
(b) If $u \in D^*$ then $\delta(u) = \delta(1)$ if and only if u is a unit.

12.3. The integral domains $\mathbb{Z}(\sqrt{d})$.

12.3.1. *The Gaussian integers.*

This is the integral domain

$$\mathbb{Z}(i) = \{m + ni \mid m, n \in \mathbb{Z}\}$$

with $\delta(m + ni) = m^2 + n^2$ and $i = -1$ as usual. Then δ is a Euclidean valuation.

12.3.2. *The general case.*

If $d \in \mathbb{Z}$ we define

$$\mathbb{Z}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

This is an integral domain, a subdomain of $\mathbb{C}$. We normally take $d \neq 0, 1$ and d squarefree.

The *norm* in $\mathbb{Z}(\sqrt{d})$ is the function $N : \mathbb{Z}(\sqrt{d}) \to \mathbb{N}$ given by

$$N(a + b\sqrt{d}) = |a^2 - db^2|.$$

Theorem 12.3. *In $\mathbb{Z}(\sqrt{d})$,*

(i) $N(x) = 0$ *if and only if* $x = 0$
(ii) *for all* $x, y \in \mathbb{Z}(\sqrt{d})$, $N(xy) = N(x)N(y)$
(iii) x *is a unit if and only if* $N(x) = 1$
(iv) *if* $N(x)$ *is prime, then* x *is irreducible in* $\mathbb{Z}(\sqrt{d})$.

Note that N is in some cases, but not in all cases, a Euclidean valuation, so for some d, $\mathbb{Z}(\sqrt{d})$ is a Euclidean domain with valuation N. There are also cases where $\mathbb{Z}(\sqrt{d})$ is a Euclidean domain with a different valuation.

12.4. Principal ideal domains.

Definition 12.4. An integral domain D is a *principal ideal domain (PID)* if every ideal of D is principal.

Theorem 12.5. *Every Euclidean domain is a PID.*

Examples:

(1) $\mathbb{Z}$ is an ED and hence a PID.
(2) If F is a field, $F[x]$ is an ED, and hence a PID.
(3) The Gaussian integers $\mathbb{Z}(i)$ is a PID.
(4) The domain $\mathbb{Z}[x]$ is *not* a PID. (Consider the ideal $\langle 2, x\rangle = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$.)

Week 11 — Lecture 26 — Tuesday 25th May 2010.

---

13. Unique Factorization Domains

13.1. Definitions.

Definition 13.1. An integral domain D is called a *unique factorization domain (UFD)* if for every $a \in D$, not zero or a unit,

(i) $a = c_1 c_2 \dots c_n$ for irreducibles c_i
(ii) if $a = c_1 c_2 \dots c_n = d_1 d_2 \dots d_m$ with c_i, d_j all irreducible then $n = m$ and the d_i can be renumbered such that each c_i is an associate of d_i.

13.2. Irreducibility tests for polynomials.

Lemma 13.2. *Let F be a field. If $f(x) \in F[x]$ has degree 2 or 3 then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.*

Theorem 13.3 (Eisenstein's criterion). *Let $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$.*
Suppose that there is a prime p such that

(i) $p \nmid a_n$
(ii) $p | a_i$ *for* $i = 0, 1, \dots, n-1$
(iii) $p^2 \nmid a_0$.

Then apart from a constant factor $f(x)$ is irreducible over $\mathbb{Z}$.

13.3. Irreducibles and primes.

Definition 13.4. Let a, b elements of an integral domain D. If $a \neq 0$ we say that a *divides* b ($a \mid b$) if $b = ac$ for some $c \in D$.

Lemma 13.5. *Let D be an integral domain. Then*

(a) $a \mid b$ *if and only if* $\langle a\rangle \supseteq \langle b\rangle$.
(b) $\langle a\rangle = D$ *if and only if a is a unit.*
(c) $\langle a\rangle = \langle b\rangle$ *if and only if a and b are associates.*

Definition 13.6. An element p of an integral domain D, not zero or a unit, is called *prime* if whenever $p|ab$ for $a, b \in D$, either $p|a$ or $p|b$.

Week 12 — Lecture 27 — Monday 31st May 2010.

Lemma 13.7. *Every prime in an integral domain is irreducible.*

Theorem 13.8. *Let D be an integral domain. Then D is a UFD if and only if*

(i) *for every* $a \in D$*, not zero or a unit,* $a = c_1 c_2 \dots c_n$ *for irreducibles* c_i
(ii) *every irreducible in* D *is prime.*

Theorem 13.9. *Every PID is a UFD.*

Week 12 — Lecture 28 — Tuesday 1st June 2010.

Lemma 13.10. *Let* D *be a PID and let* $a_1, a_2, a_3, \dots$ *be a sequence of elements of* D *such that for each* i, $a_{i+1} | a_i$*. Then for some* N*,* a_n *is an associate of* a_N *for all* $n > N$*.*

13.4. **Polynomial rings as UFDs.**

Theorem 13.11. *If* D *is a UFD then so is* $D[x]$*.*

Corollary 13.12. *If* D *is a UFD so also is* $D[x_1, \dots, x_n]$*.*

Hence, in particular, $\mathbb{Z}[x], F[x,y], F[x,y,z]$ are UFDs.

13.5. **Relationships between classes of rings.**

$$ED \subset PID \subset UFD \subset ID \subset \text{ Commutative rings with identity.}$$

Examples:

EDs	$\mathbb{Z}, F[x], \mathbb{Z}(i), \mathbb{Z}(\sqrt{2})$
PIDs which are not EDs	$\{\frac{m}{2} + \frac{n}{2}\sqrt{-19} \mid m, n \in \mathbb{Z}\}$
UFDs which are not PIDs	$\mathbb{Z}[x], \mathbb{Z}[x,y], F[x,y]$
IDs which are not UFDs	$\mathbb{Z}(\sqrt{-5}), \mathbb{Z}(\sqrt{10})$
Commutative rings with 1 which are not IDs	$\mathbb{Z}_m$, m composite.