Modern Algebra (MA 521)
Synopsis of lectures
July-Nov 2015 semester, IIT Guwahati

Shyamashree Upadhyay

Contents

1 Lecture 1

1.1 Properties of Integers

Theorem 1.1.1. ***The well-ordering Principle****: Every non-empty set of positive (or non-negative) integers contains a smallest member.*

Definition 1.1.2. We say that a non-zero integer t is a **divisor** of an integer s if there exists an integer u such that $s = tu$. In this case, we write $t|s$ and read "t divides s.
When t is not a divisor of s, we write $t \nmid s$. $\square$

Definition 1.1.3. A **prime** is a positive integer > 1 whose only positive divisors are 1 and itself. $\square$

Definition 1.1.4. We say that an integer s is a **multiple** of an integer t if there exists an integer u such that $s = tu$. $\square$

Theorem 1.1.5. ***The division Algorithm****: Let a and b be integers with $b > 0$. Then $\exists$ unique integers q and r such that $a = bq + r$ where $0 \leq r < b$.*

Definition 1.1.6. The integer q in the division algorithm is called the **quotient** upon dividing a by b. The integer r is called the **remainder** upon dividing a by b. $\square$

Definition 1.1.7. The **greatest coomon divisor (gcd)** of two non-zero integers a and b is the largest among all common divisors of a and b. We denote this integer by $gcd(a, b)$. When $gcd(a, b) = 1$, we say that a and b are **relatively prime**. $\square$

Theorem 1.1.8. ***GCD is a linear combination****: For any two non-zero integres a and b, there exists integers s and t such that*

$$gcd(a, b) = as + bt.$$

Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Lemma 1.1.9. *If p is a prime that divides ab, then either p divides a or p divides b.*

Definition 1.1.10. The **least common multiple** of two integers a and b is the smallest positive integer that is a multiple of both a and b. We denote it by $lcm(a, b)$. $\square$

Theorem 1.1.11. ***The Prime factorization theorem***: *Every integer > 1 is either a prime or a product of primes. This product is unique, except for the order in which the factors appear. That is, if $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$, where the p_i s and the q_j s are primes. Then $r = s$ and after some rearrangement, $p_i = q_i$ $\forall i$ and $\alpha_i = \beta_i$ for all i.*

1.2 Sets, relations and functions

Definition 1.2.1. An **equivalence relation** on a set S is a set R of ordered pairs of elements of S such that
(i) $(a, a) \in R$ for all $a \in S$ (reflexive property).
(ii) $(a, b) \in R$ implies that $(b, a) \in R$ (symmetric property).
(iii) $(a, b) \in R$ and $(b, c) \in R$ together imply that $(a, c) \in R$ (transitive property). When R is an equivalence relation on a set S, it is customary to write aRb instead of $(a, b) \in R$. The symbol $\sim$ is usually used to denote an equivalence relation. If $\sim$ is an equivalence relation on a set S and $a \in S$, then the set $[a] := \{x \in S | x \sim a\}$ is called the **equivalence class of** S containing a. □

Example(s) 1.2.2. Let $S = \mathbb{Z}$ and let n be a positive integer. If $a, b \in S$, define $a \sim b$ if $a = b$ *mon* n, that is, if $a - b$ is divisible by n. Then $\sim$ is an equivalence relation on S and its distinct equivalence classes are $[0], [1], \ldots, [n-1]$. □

Definition 1.2.3. A **Partition** of a set S is a collection of non-empty disjoint subsets of S whose union is S. □

Proposition 1.2.4. *The equivalence classes of an equivalence relation on a set S constitute a partition of S.*

Remark 1.2.5. The converse of the above proposition is also true: For any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P.

Remark 1.2.6. Recall the definition of a **function** or a **mapping**. Recall the concept of **domain, codomain** and **range** or **image** of a function. Recall the definitions of **composition of functions**, **one-to-one function**, **onto function** and **bijections/one-to-one correspondence**.

1.3 Laws of modular arithmetic

Let n be a positive integer and a be an integer. We denote by $a \ mod \ n$ the remainder upon dividing a by n. We say that $a \equiv b \ mod \ n$ whenever $a - b$ is divisible by n. Recall that

$$(a+b) mod \ n = ((a \ mod \ n) + (b \ mod \ n)) mod \ n$$

and

$$(a.b) mod \ n = ((a \ mod \ n).(b \ mod \ n)) mod \ n.$$

2 Lecture 2

2.1 Groups

Definition 2.1.1. A non-empty set of elements G is said to be a **group** if in G, there is defined a binary operation, called the product, denoted by $\cdot$, such that
(i) $a, b \in G \Rightarrow a \cdot b \in G$. (Closure prperty)
(ii) $a, b, c \in G \Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$. (Associativity)
(iii) $\exists$ an element $e \in G$ such that $a \cdot e = e \cdot a = a$ $\forall a \in G$. (Existence of identity)
(iv) For every $a \in G$, $\exists$ an elementy a^{-1} in G such that $a \cdot a^{-1} = a^{-1} \cdot a = e$. (Existence of inverses) $\square$

Definition 2.1.2. A group G is called **abelian** or **commutative** if $a \cdot b = b \cdot a$ $\forall$ $a, b \in G$. A group which is not abelian is called **non-abelian**. $\square$

Definition 2.1.3. The number of elements in a group G is called the **order** of G. It is denoted by $o(G)$ or by $|G|$. When $o(G) < \infty$, we say that G is a **finite group**. $\square$

Example(s) 2.1.4. Let n be a fixed positive integer. Let $U(n)$ denote the set of all positive integers less than n and relatively prime to n.
Then $U(n)$ is a group under multiplication modulo n. $\square$

In the class, lots of other examples of groups were discussed.

Definition 2.1.5. Let n be a positive integer. Let G be the set consisting of all symbols a^i, where we insist that $a^0 = a^n = e$ and

$$a^i \cdot a^j = \begin{cases} a^{i+j} & \text{if } i + j \leq n \\ a^{i+j-n} & \text{otherwise} \end{cases}$$

It can be verified that G is a group. This G is called the **cyclic group of order n**. $\square$

2.2 Properties of a Group

Lemma 2.2.1. *If G is a group, then*
(a) The identity element of G is unique.
(b) Every $a \in G$ ahs a unique inverse in G.

(c) For every $a \in G$, $(a^{-1})^{-1} = a$.
(d) For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Theorem 2.2.2. *In a group G, the right and left cancellation laws hold, that is,*

$$ba = ca \Rightarrow b = c$$

and

$$ab = ac \Rightarrow b = c.$$

Lemma 2.2.3. *Given a, b in a group G, the equations $ax = b$ and $ya = b$ have unique solutions for x and y in G.*

2.3 Order

Definition 2.3.1. The number of elements of a group (finite or infinite) G is called the **order** of the group G. It is denoted by $|G|$ or $o(G)$. □

Definition 2.3.2. The **order of an element** g in a group G is the smallest positive integer n such that $g^n = e$. [In additive notation, this would be $ng = 0$.] If no such integer exists, we say that g has infinite order. The order of an element g is denoted by $|g|$ or $o(g)$. □

2.4 Subgroups

Definition 2.4.1. If a non-empty subset H of a group G is itself a group under the operation of G, we say that H is a **subgroup** of G. We denote this by $H \leq G$. □

Remark 2.4.2. If H is a subgroup of G that is not equal to G itself, then we say that H is a **proper subgroup** of G and denote it by $H < G$. The subgroup $\{e\}$ is called the **trivial subgroup** of G. A subgroup that is not equal to $\{e\}$ is called a **non-trivial subgroup** of G.

Theorem 2.4.3. ***One-step subgroup test***: *Let G be a group and H be a non-empty subset of G. Then $H \leq G$ if and only if $ab^{-1} \in H$ whenever $a, b \in H$.*

Theorem 2.4.4. ***Two-step subgroup test***: *Let G be a group and H be a non-empty subset of G. Then $H \leq G$ if and only if $ab \in H$ whenever $a, b \in H$ and $a^{-1} \in H$ whenever $a \in H$.*

Theorem 2.4.5. *Let H be a non-empty finite subset of a group G. Then H is a subgroup of G if H is closed under the operation of G.*

Theorem 2.4.6. *Let G be a group and let $a \in G$. Let $< a >:= \{a^n | n \in \mathbb{Z}\}$. Then $< a >$ is a subgroup of G.*

Remark 2.4.7. The subgroup $< a >$ is called the **cyclic subgroup** of G **generated by** a. In the case when $G =< a >$, we say that G is cyclic and a is **a generator** of G. Note that a cyclic group may have more than one generators.

Definition 2.4.8. The **center** $Z(G)$ of a group G is defined as

$$Z(G) := \{a \in G | ax = xa \ \forall x \in G\}.$$

□

Theorem 2.4.9. *The center $Z(G)$ of a group G is a subgroup of G.*

Definition 2.4.10. Let $a \in G$ be fixed. The **centralizer of** a in G, denoted by $C(a)$ is given by

$$C(a) := \{g \in G | ag = ga\}.$$

□

Theorem 2.4.11. *For each $a \in G$, $C(a)$ is a subgroup of G and $Z(G) = \cap_{a \in G} C(a)$.*

3 Lecture 3

3.1 Lagrange's theorem

Definition 3.1.1. Let G be a group, H a subgroup of G. For $a, b \in G$, we say that a is **congruent to** b *mod* H if $ab^{-1} \in H$. We denote this by $a \equiv b \ mod \ H$. □

Lemma 3.1.2. *The relation $a \equiv b \ mod \ H$ is an equivalence relation on G.*

Definition 3.1.3. If H is a subgroup of G and $a \in G$, then the set

$$Ha := \{ha | h \in H\}$$

is called a **right coset** of H in G. Similarly, the set $aH := \{ah | h \in H\}$ is called a **left coset** of H in G. □

Lemma 3.1.4. *For all $a \in G$,*

$$Ha = \{x \in G | a \equiv x \ mod \ H\}.$$

Remark 3.1.5. Since $a \equiv b \ mod \ H$ is an equivalence relation, it follows that Ha is the equivalence class of a in G. Proof: Follows from lemma 3.1.4.

Hence the right cosets Ha s yield a decomposition of G into disjoint subsets. And any two right cosets of H in G are either identical or disjoint.

Lemma 3.1.6. *There is a one-to-one correspondence between any two right cosets of H in G.*

Remark 3.1.7. Lemma 3.1.6 above is of most interest when G is a finite group because then it merely states that any two right cosets of H in G have the same number of elements. Since $H = He$ is also a right coset, it follows that any right coset of H in G has $o(H)$ many elements in it.

Now suppose G is a finite group and k is the number of distinct right cosets of H in G. Then it follows from the preceeding discussion that $ko(H) = o(G)$. Hence we have

Theorem 3.1.8. *If G is a finite group and H is a subgroup of G, then $o(H)$ divides $o(G)$.*

Definition 3.1.9. If H is a subgroup of G, then the **index** of H in G is the number of distinct right cosets of H in G. We denote this by $i_G(H)$. $\square$

If G is a finite group, then it follows from theorem 3.1.8 that $i_G(H) = \frac{o(G)}{o(H)}$.

Corollary 3.1.10. *If G is a finite group and $a \in G$, then $o(a)$ divides $o(G)$.*

Corollary 3.1.11. *If G is a finite group and $a \in G$, then $a^{o(G)} = e$.*

Corollary 3.1.12. *If G is a finite group whose order is a prime number, then G is a cyclic group.*

3.2 Applications to number theory

The **Euler-ϕ-function**, $\phi(n)$ is defined for all positive integers n by the following rule:

$$\phi(1) = 1 \ and \ for n > 1,$$

$$\phi(n) = the \ number \ of \ positive \ integers < n \ and \ coprime \ to \ n.$$

Clearly, order of $U(n) = \phi(n)$.

Lemma 3.2.1. *If n is a positive integer and a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \ mod \ n$.*

Corollary 3.2.2. *If p is a prime number and a is any integer. Then $a^p \equiv a \ mod \ p$.*

3.3 Properties of cosets

Theorem 3.3.1. *Let H be a subgroup of a group G. Let $a, b \in G$. Then*
(i) $a \in aH$.
(ii) $aH = H$ iff $a \in H$.
(iii) Either $aH = bH$ or $aH \cap bH = \emptyset$.
(iv) $aH = bH$ iff $a^{-1}b \in H$.
(v) $|aH| = |bH|$.
(vi) $aH = Ha$ iff $H = aHa^{-1}$.
(vii) aH is a subgroup of G iff $a \in H$.

An application of cosets to permutation groups

Definition 3.3.2. Let G be a group of permutations of a set S. For each $i \in S$, let

$$Stab_G(i) := \{\phi \in G | \phi(i) = i\}.$$

We call $Stab_G(i)$ the **stabilizer of** i in G. □

Exercise: Verify that $Stab_G(i)$ is a subgroup of G.

Definition 3.3.3. Let G be a group of permutations of a set S. For each $s \in S$, let

$$orb_G(s) := \{\phi(s) | \phi \in G\}.$$

The set $orb_G(s)$ is a subset of S and is called the **orbit of** s under G. □

Theorem 3.3.4. *Let G be a finite group of permutations of a set S. Then for any $i \in S$,*

$$|G| = |orb_G(i)||Stab_G(i)|.$$

3.4 Product of two Subgroups

Definition 3.4.1. If H and K are two subgroups of a group G, let

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

$\square$

Theorem 3.4.2. *HK is a subgroup of G if and only of $HK = KH$.*

Corollary 3.4.3. *If H and K are subgroups of an abelian group, then HK is a subgroup of G.*

Theorem 3.4.4. ***A counting principle**: If H and K are finite subgroups of a group G, then*

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)}.$$

4 Lecture 4

4.1 Normal subgroups, Quotient groups

Definition 4.1.1. A subgroup N of G is called a **normal subgroup** of G if, for every $g \in G$ and $n \in N$, we have $gng^{-1} \in N$. We denote this by $N \trianglelefteq G$. $\square$

Let $gNg^{-1} := \{gng^{-1} | n \in N\}$. Then N is a normal subgroup of G if and only if $gNg^{-1} \subseteq N$ for every $g \in G$.

Lemma 4.1.2. *N is a normal subgroup of G if and only if $gNg^{-1} = N$ for every $g \in G$.*

Remark 4.1.3. Lemma 4.1.2 DOES NOT say that for every $n \in N$ and for every $g \in G$, we should have $gng^{-1} = n$! It only says that the two sets N and gNg^{-1} should be the same.

Lemma 4.1.4. *The subgroup N of G is a normal subgroup of G if and only if every left coset of N in G is a right coset of N in G. In particular, $N \trianglelefteq G$ if and only if $Ng = gN$ for every $g \in G$.*

Theorem 4.1.5. *If G is a group and $N \trianglelefteq G$, let G/N denote the set of all right cosets of N in G. Then G/N forms a group under the binary operation $\circ$ given by*

$$Na \circ Nb := Nab.$$

Definition 4.1.6. The group G/N of theorem 4.1.5 above is called the **quotient group** or the **factor group** of G by N. □

Remark 4.1.7. The order of G/N equals the index $i_G(N)$.

Lemma 4.1.8. *If G is a finite group and $N \trianglelefteq G$. Then $o(G/N) = \frac{o(G)}{o(N)}$.*

Example(s) 4.1.9. 1) Every subgroup of an abelian group is normal.
2) The center of a group G is always normal in G.
3) $SL(2, \mathbb{C}) \trianglelefteq GL(2, \mathbb{C})$. □

Example(s) 4.1.10. For any positive integer n, the quotient $\mathbb{Z}/n\mathbb{Z}$ is an example of a Quotient group. □

4.2 Applications of Quotient groups

Theorem 4.2.1. *If $G/Z(G)$ is cyclic, then G is abelian.*

Definition 4.2.2. Let $(G, \circ)$ and $(G', \circ')$ be two groups. A map $f : G \to G'$ is called a **group homomorphism** if

$$f(a \circ b) = f(a) \circ' f(b)$$

for all $a, b \in G$. □

Definition 4.2.3. A group homomorphism $f : G \to G'$ is called an **isomorphism** (resp., **monomorphism**, **epimorphism**) if f is bijective (resp., injective, surjective). □

Definition 4.2.4. Let G be a group. The set of all isomorphisms from G onto itself is called the **automorphism group** of G, and is denoted by $Aut(G)$. □

Definition 4.2.5. Let

$$Inn(G) := \{\phi_g | g \in G\}$$

where $\phi_g : G \to G$ is given by

$$\phi_g(x) := gxg^{-1} \ \forall x \in G.$$

Then IT CAN BE PROVED (Exercise!) that $Inn(G)$ is a subgroup of $Aut(G)$, called the **inner automorphism group** of G. □

Theorem 4.2.6. *$G/Z(G)$ is isomorphic to $Inn(G)$.*

5 Lecture 5

5.1 Application of Quotient groups continued

Theorem 5.1.1. *Let G be a finite abelian group and let p be a prime that divides $o(G)$. Then G has an element of order p.*

5.2 Cyclic groups

Definition 5.2.1. A group G is called **cyclic** if there exists an element $a \in G$ such that $G = \{a^n | n \in \mathbb{Z}\}$. Such an element a is called a **generator** of G. We indicate that G is a cyclic group generated by a and denote it by $G =< a >$. □

Remark 5.2.2. A cyclic group can have more than one generators. For example, $\mathbb{Z}$ is a cyclic group under addition having two generators $+1$ and -1. Also $\mathbb{Z}_n$ is a cyclic group under addition mod n, having at least two generators $+1$ and $n-1$. Observe that $\mathbb{Z}_8$ has 4 generators: 1,3,5,7.

Example(s) 5.2.3. 1) $U(10)$ is cyclic having at least 2 generators, 3, 7.
2) $U(8)$ is NOT CYCLIC. □

Theorem 5.2.4. *Let G be a group and $a \in G$. If a has infinite order, then all distinct powers of a are distinct group elements. If a has finite order, say n, then $< a >= \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.*

Corollary 5.2.5. *$a^k = e \Rightarrow o(a)$ divides k.*

Theorem 5.2.6. *Let $G =< a >$ be a cyclic group of order n. Then $G =< a^k >$ if and only if $gcd(k, n) = 1$.*

Corollary 5.2.7. *An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $gcd(k, n) = 1$.*

6 Lecture 6

6.1 Fundamental theorem for cyclic groups

Theorem 6.1.1. *Every subgroup of a cyclic group is cyclic. Moreover, 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, $< a^{\frac{n}{k}} >$.*

Corollary 6.1.2. *For each positive divisor k of n, the set $< n/k >$ is the unique subgroup of $\mathbb{Z}_n$ or order k. Moreover, these are the only subgroups of $\mathbb{Z}_n$.*

Theorem 6.1.3. *If d is a positive divisor of n, then the number of elements of order d in a cyclic group of order n is $\phi(d)$, where ϕ is the Euler-phi function.*

6.2 Group Homomorphisms

Definition 6.2.1. A **Group Homomorphism** ϕ from a group $(G, \circ)$ to a group $(G', *)$ is a map from G into G' such that $\phi(a \circ b) = \phi(a) * \phi(b)$ for all $a, b \in G$. □

Definition 6.2.2. The **Kernel** of a group homomorphism $\phi : G \to G'$ is the set $\{x \in G | \phi(x) = e\}$. It is denoted by $Ker(\phi)$. □

Isomorphisms, monomorphisms and epimorphisms have been defined in definition 4.2.3.

Example(s) 6.2.3. The map $det : GL(2, \mathbb{R}) \to \mathbb{R}^*$ which maps any matrix A to its determinant is a group homomorphism. Its kernel is $SL(2, \mathbb{R})$. □

Theorem 6.2.4. *Let $\phi : G \to G'$ be a group homomorphism. Let $g \in G$ be arbitrary. Then*
(i) ϕ carries the identity of G to the identity of G'.
(ii) $\phi(g^n) = [\phi(g)]^n$ for every integer n.
(iii) If $|g| = n$, then $|\phi(g)|$ divides n.
(iv) If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G | \phi(x) = g'\} = gKer\phi$.

7 Lecture 7

7.1 Properties of Homomorphisms

Theorem 7.1.1. *Let $\phi : G \to \overline{G}$ be a group homomorphism. Let H be a subgroup of G. Then*
(i) $\phi(H)$ is a subgroup of $\overline{G}$.
(ii) If H is cyclic, then so is $\phi(H)$.
(iii) If H is abelian, then so is $\phi(H)$.
(iv) If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.
(v) If $|Ker(\phi)| = n$, then ϕ is an n-to-1 map from G onto $\phi(G)$.
(vi) $|\phi(H)|$ divides $|H|$.
(vii) If $\overline{K} \leq \overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G | \phi(k) \in \overline{K}\}$ is a subgroup of G.
(viii) If $\overline{K} \trianglelefteq \overline{G}$, then $\phi^{-1}(\overline{K}) \trianglelefteq G$.
(ix) If ϕ is onto and $Ker(\phi) = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.

Corollary 7.1.2. *Let $\phi : G \to \overline{G}$ be a group homomorphism. Then $Ker(\phi)$ is a normal subgroup of G.*

Definition 7.1.3. Let $N \trianglelefteq G$. Then there is a natural group epimorphism $\pi_N : G \to G/N$ under which $a \mapsto aN$. This map π_N is called the **canonical projection** with respect to N. □

Theorem 7.1.4. *Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the map π_N.*

7.2 Isomorphism theorems

Theorem 7.2.1. *If $f : G \to H$ is a group homomorphism and $N \trianglelefteq G$ such that $N \subseteq Ker(f)$, then there exists a unique homomorphism $\overline{f} : G/N \to H$ such that $\overline{f}(aN) = f(a)$ for all $a \in G$. Moreover, $Im(f) = Im(\overline{f})$ and*

$Ker(\overline{f}) = \frac{Ker(f)}{N}$. *In particular,* $\overline{f}$ *is an isomorphism if and only if* f *is an epimorphism and* $N = Ker(f)$.

Corollary 7.2.2. ***1st isomorphism theorem***: *If* $f : G \to H$ *is a group homomorphism, then* $G/Ker(f)$ *is isomorphic to* $Im(f)$.

Corollary 7.2.3. ***2nd isomorphism theorem***: *If* K *and* N *are subgroups of a group* G *with* $N \trianglelefteq G$*, then*

$$K/N \cap K \backsimeq NK/N.$$

Corollary 7.2.4. ***3rd isomorphism theorem***: *If* K *and* H *are two normal subgroups of a group* G *and* $K \leq H$*, then* $H/K \trianglelefteq G/K$ *and*

$$(G/K)/(H/K) \backsimeq G/H.$$

Corollary 7.2.5. *If* $f : G \to H$ *is a group homomorphism,* $N \trianglelefteq G$*,* $M \trianglelefteq H$*, and* $f(N) \leq M$*, then* f *induces a homomorphism*

$$\overline{f} : G/N \to H/M$$

given by $\overline{f}(aN) = f(a)M$.

8 Lecture 8

8.1 A theorem on epimorphism of groups

Theorem 8.1.1. *Let* $f : G \to H$ *be an epimorphism of groups. Let* $S_f(G)$ *denote the collection of all subgroups of* G *which contain* $Ker(f)$ *and let* $S(H)$ *be the collection of all subgroups of* H*. Then the map* $T : S_f(G) \to S(H)$ *given by* $K \mapsto f(K)$ *is a one-to-one correspondence. Under this correspondence, normal subgroups correspond to normal subgroups.*

Corollary 8.1.2. *If* $N \trianglelefteq G$*, then every subgroup of* G/N *is of the form* K/N*, where* K *is a subgroup of* G *that contains* N*. Furthermore,* $K/N \trianglelefteq G/N \Leftrightarrow K \trianglelefteq G$.

8.2 Permutation Groups

Definition 8.2.1. A **permutation** of a set A is a function from A to A that is bijective. □

Definition 8.2.2. A permutation group of a set A is a set of permutations of A that forms a group under function composition. □

Definition 8.2.3. Let n be a fixed positive integer. Let $A = \{1, 2, \ldots, n\}$. The set of all permutations of the set A is called the **symmetric group** of degree n, and is denoted by S_n. □

Clearly, S_n has cardinality $n!$. The composition of any two permutations in S_n expressed in array notation is carried out from right to left, by going from top to bottom, then again from top to bottom.

Definition 8.2.4. An r-**cycle** $(a_1\ a_2\ \ldots\ a_r)$ is a permutation that maps a_1 to a_2, a_2 to a_3,..., a_r to a_1, and fixes all other elements. The **length** of an r-cycle is r. □

The identity permutation ϵ is the permutation that takes every element to itself. It is usually denoted by a one-cycle, (1) or (2) or ... or (n).

Definition 8.2.5. Two cycles $(a_1\ a_2\ \ldots\ a_r)$ and $(b_1\ b_2\ \ldots\ b_m)$ are called **disjoint** if the sets $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_m\}$ are disjoint. □

Theorem 8.2.6. *Every permutation in S_n can be expressed as a one-cycle or as a product ot disjoint cycles,*

Theorem 8.2.7. *If two cycles $\alpha = (a_1\ a_2\ \ldots\ a_r)$ and $\beta = (b_1\ b_2\ \ldots\ b_m)$ are disjoint, then they commute, that is, $\alpha\beta = \beta\alpha$.*

Theorem 8.2.8. *The order of a permutation of a finite set written in disjoint cycle form is the lcm of the lengths of the (disjoint) cycles.*

Definition 8.2.9. A 2-cycle is called a **transposition**. □

Example(s) 8.2.10. $(a\ b)$ is a transposition. The effect of $(a\ b)$ is to interchange a and b. A transposition is its own inverse since it has order 2. □

Theorem 8.2.11. *Every permutation in S_n, $n > 1$, is a product of (not necessarily disjoint) transpositions.*

Remark 8.2.12. 1) $(a_1\ a_2\ \dots\ a_r) = (a_1\ a_r)(a_1\ a_{r-1})\dots(a_1\ a_2)$.
2) The decomposition of a permutation into a product of transpositions is not unique.

Lemma 8.2.13. *If $\epsilon = \beta_1\beta_2\dots\beta_r$ where the β_i s are transpositions, then r must be even.*

Theorem 8.2.14. *If a permutation α can be expressed as a product of an even (resp. odd) number of transpositions, then every decomposition of α into a product of transpositions must have an even (resp. odd) number of transpositions in it.*

Definition 8.2.15. A permutation that can be expressed as a product of an even (resp. odd) number of transpositions is called an **even permutation** (resp. **odd permutation**). □

Theorem 8.2.16. *The set of all even permutations in S_n forms a subgroup of S_n.*

Definition 8.2.17. The group of all even permutations on n symbols is denoted by A_n and is called the **alternating group of degree** n. □

Theorem 8.2.18. *For $n > 1$, A_n has order $\frac{n!}{2}$.*

9 Lecture 9

9.1 Alternating group contd....

Lemma 9.1.1. *A subgroup of index 2 of S_n must contain all 3-cycles.*

Lemma 9.1.2. *For $n \geq 3$, A_n is generated by all 3-cycles.*

Theorem 9.1.3. *For each $n \geq 2$, A_n is normal in S_n and A_n has index 2 in S_n. Furthermore, A_n is the only subgroup of S_n of index 2.*

Definition 9.1.4. A group G is called **simple** if G has no proper normal subgroups other than the trivial subgroup. □

Lemma 9.1.5. *Ler r and s be two fixed arbitrary elements of $\{1, 2, \dots, n\}$. Then A_n $(n \geq 3)$ is generated by the 3-cycles $\{(r\ s\ k) | 1 \leq k \leq n, k \neq r, s\}$.*

Lemma 9.1.6. *If N is normal in A_n and N contains a 3-cycle, then $N = A_n$.*

Theorem 9.1.7. *A_n is simple if and only if $n \neq 4$.*

Another important subgroup of S_n $(n \geq 3)$ is the subgroup D_n generated by $a = (1\ 2\ 3\ \ldots\ n)$ and

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix} = \Pi_{2 \leq i < n+2-i}(i\ n{+}2{-}i).$$

This subgroup D_n is called the **dihedral group of degree** n. This group D_n is isomorphic to the group of all symmetries of a regular n-gon.
For $n \geq 3$, D_n is a group of order $2n$ whose generators a and b satisfy:
(i) $a^n = (1) = b^2$
(ii) $a^k \neq (1)$ if $0 < k < n$.
(iii) $ba = a^{-1}b$.

9.2 Group actions

Definition 9.2.1. A **group action** of a group G on a non-empty set A is a map : $G \times A \to A$ which takes (g, a) to $g.a$ and satisfies the following properties:
(i) $g_1.(g_2.a) = (g_1g_2).a$ for all $g_1, g_2 \in G$ and for all $a \in A$.
(ii) $1.a = a$ for all $a \in A$. □

Let a group G act on a set A. Let $S_A :=$ the group of all permutations of the set A. For each fixed $g \in G$, we get a map $\sigma_g : A \to A$ defined as $\sigma_g(a) = g.a$. It can be proved that
(i) For each fixed $g \in G$, σ_g is a permutation of A and
(ii) The map : $G \to S_A$ given by $g \mapsto \sigma_g$ is a group homomorphism.

Definition 9.2.2. The group homomorphism $\phi : G \to S_A$ given by $g \mapsto \sigma_g$ is called the **permutation representation associated to the given action** of Gon A. □

Definition 9.2.3. 1) **Kernel** of the action $= \{g \in G | g.a = a\ \forall a \in A\}$.
2) For each fixed $a \in A$, $Stab_G(a) = \{g \in G | g.a = a\}$ is called the **stabilizer** of a in G. It is also denoted by G_a.
3) An action is called **faithful** if its kernel is the identity. □

Remark 9.2.4. Kernel of the action $= \cap_{a \in A} G_a$.

Example(s) 9.2.5. Let n be a positive integer. The group $G = S_n$ acts on the set $A = \{1, 2, \ldots, n\}$ by $g.i = g(i)$ for all $i \in A$. Check that the permutation representation associated to this action is the identity map $Id : S_n \to S_n$. Check also that this action is afithful and for each $i \in A$, the stabilizer G_i is isomorphic to S_{n-1}. $\square$

10 Lecture 10

10.1 Group action continued...

Remark 10.1.1. Suppose a group G acts on a non-empty set A. Then two group elements g_1 and g_2 induce the same permutation of A if and only if g_1 and g_2 belong to the same coset of the Kernel of the action.

Given a group action on a non-empty set A. there exists a permutation representation associated to it, which is a group homomorphism! Conversely, given any non-empty set A and any group homomorphism $\phi : G \to S_A$, we can obtain an action of G on A by defining

$$g.a = \phi(g)(a) \ \forall a \in A, \ \forall g \in G.$$

The kernel of this action is the same as $Ker(\phi)$. And the permutation representation associated to this action is precisely the given homomorphism ϕ. Hence we have the following theorem:

Theorem 10.1.2. *For any group G and any non-empty set A, there is a bijection between the actions of G on A and the homomorphisms from G into S_A.*

Proposition 10.1.3. *Let $H \leq G$ and let G act on the set A of all left cosets of H in G by left multiplication. Then the kernel of the induced permutation representation $: G \to S_A$ is contained in H.*

Corollary 10.1.4. *If $H \leq G$ and $[G : H] = n$ and no nontrivial normal subgroup of G is contained in H, then G is isomorphic to a subgroup of S_n.*

Corollary 10.1.5. *If G is a finite group and $H \leq G$ be of index p, where p is the samllest prime dividing $o(G)$, then $H \trianglelefteq G$.*

10.2 Isomorphisms

Definition 10.2.1. An **isomorphism** ϕ from a group G to a group G' is a group homomorphism that is bijective. $\square$

If there is an isomorphism from G onto G', we say that G and G' are isomorphic and write $G \backsimeq G'$.

Example(s) 10.2.2. Let $G = (\mathbb{R}, +)$ and G' be the group of all positive real numbers under multiplication. Then G and G' are isomorphic under the map $\phi : G \to G'$ given by $\phi(x) = 2^x$. $\square$

Example(s) 10.2.3. Not an isomorphism: The mapping from $(\mathbb{R}, +)$ to itself given by $\phi(x) = x^3$ is not an isomorphism since $(x + y)^3 \neq x^3 + y^3$. $\square$

Example(s) 10.2.4. Any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$ and any infinite cyclic group is isomorphic to $\mathbb{Z}$. $\square$

Theorem 10.2.5. ***Cayley's theorem***: *Every group is isomorphic to a subgroup of the group of all permutations of a certain set.*

10.3 Properties of isomorphisms

Theorem 10.3.1. *Suppose that ϕ is an isomorphism from a group G onto a group G'. Then*
(i) ϕ carries identity of G to the identity of G'.
(ii) For every integer n and for every group element $a \in G$, we have $\phi(a^n) = [\phi(a)]^n$.
(iii) For any two elements $a, b \in G$, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
(iv) G is abelian if and only if G' is abelian.
(v) Isonorphisms preserve order, that is, $|a| = |\phi(a)|$ for all $a \in G$.
(vi) G is cyclic if and only if G' is cyclic.
(vii) If G is a finite group, then for a fixed integer k and a fixed group element $b \in G$, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in G'.
(viii) ϕ^{-1} is an isomorphism from G' to G.
(ix) If K is a subgroup of G, then $\phi(K) = \{\phi(k) | k \in K\}$ is a subgroup of G'.

11 Lecture 11

11.1 Automorphisms

Definition 11.1.1. An isomorphism from a group G to itself is called an *automorphism* of G. $\square$

Example(s) 11.1.2. Let $G = SL(2, \mathbb{R})$ and let $M \in G$. Define the map $\phi_M : G \to G$ by $\phi_M(A) = MAM^{-1}$. Then ϕ_M is an automorphism of G. $\square$

Let G be a group and $a \in G$. Let $\phi_a : G \to G$ be defined as $\phi_a(x) = axa^{-1}$. Then ϕ_a is an automorphism of G.

Definition 11.1.3. ϕ_a is called the *inner automorphism of G induced by a.* $\square$

When G is a group, we use $Aut(G)$ to denote the set of all automorphisms of G and $Inn(G)$ to denote the set of all inner automorphisms of G.

Theorem 11.1.4. *Given a group G, the sets $Aut(G)$ and $Inn(G)$ are both groups under the operation function composition.*

Theorem 11.1.5. *For every positive integer n, $Aut(\mathbb{Z}_n)$ is isomorphic to $U(n)$.*

Proposition 11.1.6. *Let $H \trianglelefteq G$. Then G acts on H by conjugation. The action of G on H by conjugation defined (for each $g \in G$) by $h \mapsto ghg^{-1}$ is an automorphism of H. The permutation representation associated to this action is a homomorphism of G into $Aut(H)$ with kernel $C_G(H) := \{g \in G | ghg^{-1} = h \; \forall h \in H\}$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.*

Corollary 11.1.7. *If $K \leq G$ and $g \in G$, then $K \backsimeq gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.*

Corollary 11.1.8. *For any subgroup H of G, let $N_G(H) := \{g \in G | gHg^{-1} = H\}$. Then $C_G(H)$ is normal in $N_G(H)$ and the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$. In particular, $G/Z(G) \backsimeq$ a subgroup of $Aut(G)$.*

Definition 11.1.9. A subgroup H of a group G is called *characteristic* in G if $\sigma(H) = H$ for all $\sigma \in Aut(G)$. It is denoted by H *char* G. $\square$

Characteristic subgroups are normal. If H is the unique subgroup of G of a given order, then H *char* G. A characteristic subgroup of a normal subgroup must be normal. We may think of characteristic subgroups as "strongly normal" subgroups.

11.2 Group action revisited

Theorem 11.2.1. *Let G be a group that acts on a set S.*
(i) The relation $\sim$ on S defined by

$$x \sim x' \Leftrightarrow gx = x' \text{ for some } g \in G$$

is an equaivalence relation.
(ii) For each $x \in S$, $G_x := \{g \in G | gx = x\}$ is a subgroup of G.

Remark 11.2.2. (i) The equivalence classes of the equivalence relation $\sim$ as in the previous theorem are called the **orbits** of G on S. The orbit if $x \in S$ is denoted by $\bar{x}$.
(ii) The subgroup G_x of G is called the **isotropy group** of x or the **stabilizer** of x.

Example(s) 11.2.3. If a group G acts on itself by conjugation, the the orbit $\{gxg^{-1} | g \in G\}$ of $x \in G$ is called the *conjugacy class* of x. □

Proposition 11.2.4. *Two elements in S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes in S_n equals the number of partitions of n.*

Theorem 11.2.5. ***Orbit-stabilizer theorem**: If a group G acts on a set S, then the cardinality of the orbit of $x \in S$ equals the index $[G : G_x]$.*

Corollary 11.2.6. *Let G be a finite group.*
(i) The number of elements in the conjugacy class of $x \in G$ is $[G : C_G(x)]$ where $C_G(x) := \{g \in G | gxg^{-1} = x\}$. This number divides $o(G)$.
(ii) If $\{\bar{x}_1, \ldots, \bar{x}_n\}$ ($x_i \in G$) is the list of all distinct conjugacy classes of G, then $o(G) = \Sigma_{i=1}^n [G : C_G(x_i)]$.

Remark 11.2.7. The equation $o(G) = \Sigma_{i=1}^n [G : C_G(x_i)]$ as in the above corollary is known as the **class equation** of the finite group G.

12 Lecture 12

12.1 The class equation

Observe that an element $x \in G$ is in $Z(G)$ if and only if the conjugacy class of x consists of x alone. Thus if G is finite and $x \in Z(G)$, then $|\bar{\mathrm{x}}|$=1 where $\bar{\mathrm{x}}$ denotes the conjugacy class of x. Consequently the calss equation of G may be written as

$$o(G) = |Z(G)| + \Sigma_{i=1}^{m}[G : C_G(x_i)]$$

where $\bar{\mathrm{x}}_i$ ($1 \leq i \leq m$, $x_i \in G \setminus Z(G)$) are distinct conjugacy classes of G and each $[G : C_G(x_i)] > 1$.

Theorem 12.1.1. *Let G be a finite group whose order is a power of a prime p. Then $Z(G)$ has more than one element in it.*

Corollary 12.1.2. *If $|G| = p^2$, where p is a prime, then G is abelian.*

12.2 Sylow theorems

Theorem 12.2.1. ***Sylow's first theorem**: Let G be a finite group and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k.*

Definition 12.2.2. Let G be a finite group and let p be a prime divisor of $|G|$. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of G of order p^k is called a **Sylow p-subgroup** of G. □

Corollary 12.2.3. ***Cauchy's theorem**: Let G be a finite group and p a prime that divides $|G|$. Then G has an element of order p.*

Definition 12.2.4. A group in which every element has order a power (≥ 0) of some fixed prime p is called a **p-group**. □

Definition 12.2.5. If $H \leq G$ and H is a p-group, then H is called a **p-subgroup** of G. □

Theorem 12.2.6. *A finite group G is a p-group if and only if $|G|$ is a power of p.*

Lemma 12.2.7. *If a group H of order p^n (p a prime) acts on a finite set S and if $S_0 := \{x \in S | hx = x \ \forall h \in H\}$, then $|S| \equiv |S_0|$ mod p.*

Lemma 12.2.8. *If H is a p-subgroup of a finite group G, then $[G : H] \equiv [N_G(H) : H]$ mod p.*

Corollary 12.2.9. *If H is a p-subgroup of a finite group G such that $p \mid [G : H]$, then $N_G(H) \neq H$.*

Theorem 12.2.10. *Let G be a group of order $p^n m$, with $n \geq 1$, p prime, and $(p, m) = 1$. Then every subgroup of G of order $p^i (1 \leq i < n)$ is normal in some subgroup of order p^{i+1}.*

13 Lecture 13

13.1 Sylow theorems continued

Theorem 13.1.1. ***Sylow's 2nd theorem****: If H is a subgroup of a finite group G and $|H|$ is a power of a prime p, then H is contained in some Sylow p-subgroup of G.*

Theorem 13.1.2. ***Sylow's 3rd theorem****: The number of Sylow p-subgroups of G is equal to 1 modulo p and this number divides $|G|$. Furthermore, any two sylow p-subgroups of G are conjugate.*

13.2 External Direct Products

Definition 13.2.1. Let $(G_1, \circ_1), \ldots, (G_n, \circ_n)$ be a finite collection of groups. The **external direct product** of $G_1, \ldots, G_n$ written as $G_1 \oplus \cdots \oplus G_n$ is the set of all n-tuples for which the i-th component is an element of G_i, and the operation is componentwise. In symbols,

$$G_1 \oplus \cdots \oplus G_n = \{(g_1, \ldots, g_n) | g_i \in G_i\}$$

where $(g_1, \ldots, g_n) \circ (g'_1, \ldots, g'_n)$ is defined to be $(g_1 \circ_1 g'_1, \ldots, g_n \circ_n g'_n)$. □

The external direct product of groups is itself a group.

Example(s) 13.2.2. $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$, the operation being componentwise addition. □

Theorem 13.2.3. *The order of an element of an external direct product of finite number of groups is the least common multiple of the orders of the components of the element. In symbols,*

$$|(g_1, \ldots, g_n)| = l.c.m(|g_1|, \ldots, |g_n|).$$

Theorem 13.2.4. *Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.*

Corollary 13.2.5. *An external direct product $G_1 \oplus \cdots \oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime whenever $i \neq j$.*

Corollary 13.2.6. *Let $m = n_1 n_2 \ldots n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ if and only if n_i and n_j are relatively prime whenever $i \neq j$.*

14 Lecture 14

14.1 Internal Direct Products

Definition 14.1.1. Let $H_1, \ldots, H_n$ be a finite collection of normal subgroups of a group G. We say that G is the **internal direct product** of $H_1, \ldots, H_n$ and write $G = H_1 \times \cdots \times H_n$ if
(i) $G = H_1 H_2 \ldots H_n = \{h_1 h_2 \ldots h_n | h_i \in H_i\}$ and
(ii) $(H_1 H_2 \ldots H_i) \cap H_{i+1} = e$ for all $i = 1, 2, \ldots, n-1$. $\square$

Exercise: Show that if G is the internal direct product of $H_1, \ldots, H_n$ and $i \neq j$ with $i, j \in \{1, 2, \ldots, n\}$, then $H_i \cap H_j = \{e\}$.

Theorem 14.1.2. $H_1 \times H_2 \times \cdots \times H_n \backsimeq H_1 \oplus H_2 \oplus \cdots \oplus H_n$.

14.2 Solvable groups

Definition 14.2.1. A group G is called **Solvable** if there exists a decreasing sequence of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = \{e\}$$

such that
(i) $G_{i+1} \trianglelefteq G_i$ for all $0 \leq i \leq n-1$ and
(ii) G_i / G_{i+1} is abelian for all $0 \leq i \leq n-1$. $\square$

Example(s) 14.2.2. 1) Any abelian group is solvable.
2) A solvable group need not be abelian: $G = S_3$ is not abelian but solvable because $S_3 = G_0 \supset G_1 = A_3 \supset G_2 = \{e\}$. $\square$

Definition 14.2.3. For any group G, let $G^{(1)}$:= the commutator subgroup of $G =< xyx^{-1}y^{-1} | x, y \in G >$. For $i \geq 2$, let $G^{(i+1)}$ denote the commutator of $G^{(i)}$. $\square$

Theorem 14.2.4. *A group G is solvable if and only if $G^{(n)} = \{e\}$ for some $n \geq 1$.*

Theorem 14.2.5. *(i) Any subgroup of a solvable group is solvable.*
(ii) Any quotient of a solvable group is solvable.

Proposition 14.2.6. *Let G be a group, K a normal subgroup such that both K and G/K are solvable. Then G is solvable.*

Proposition 14.2.7. *A group of prime power order is solvable.*

Proposition 14.2.8. *S_n is not solvable for $n \geq 5$.*

Proposition 14.2.9. *Any group of order pq, p and q being distinct primes, is solvable.*

Theorem 14.2.10. ***Burnside s theorem**: Any group of order $p^n q^m$, p, q primes, $n, m \geq 1$ is solvable.*

Theorem 14.2.11. ***Feit, Thompson**: Every group of odd order is solvable.*

Corollary 14.2.12. *Any finite non-abelian simple group is of even order.*

15 Lecture 15

15.1 Nilpotent groups

Definition 15.1.1. Let G be a group. The *upper central series* of G is the sequence of subgroups $\{C_n\}$ such that
(i) $\{e\} = C_0 \subset C_1 \subset \ldots \subset C_n \subset \ldots$
(ii) $\frac{C_i}{C_{i-1}} = Z(\frac{G}{C_{i-1}})$ for all $i \geq 1$. $\square$

Definition 15.1.2. A group G is called **nilpotent** if there exists some n such that $C_n = G$. $\square$

For subgroups H and K of G, we denote by $[H, K]$ the subgroup generated by all the commutators $aba^{-1}b^{-1}$, $a \in H$, $b \in K$.

Definition 15.1.3. The *lower central series* of G is the sequence of subgroups $\{Z^n\}$ such that
(i) $G = Z^0 \supset Z^1 \supset \ldots \supset Z^i \supset Z^{i+1} \ldots$
(ii) $Z^{i+1} = [G, Z^i]$ for all $i \geq 0$. □

Proposition 15.1.4. *G is nilpotent if and only of $Z^n = \{e\}$ for some n.*

Example(s) 15.1.5. 1) Any abelian group is nilpotent.
2) S_3 is not nilpotent.
3) Any nilpotent group is solvable. □

Proposition 15.1.6. *Any subgroup of a nilpotent group is nilpotent. Any homomorphic image of a nilpotenet group is nilpotent.*

Example(s) 15.1.7. It is NOT TRUE that if H and G/H are nilpotent, then G is nilpotent. For example: Take $G = S_3$ and $H = A_3$. □

Proposition 15.1.8. *Let G be a group, $H \neq \{e\}$ a subgroup contained in the center $Z(G)$ such that G/H is nilpotent. Then G is nilpotent.*

Proposition 15.1.9. *Any group of prime power order is nilpotent.*

Proposition 15.1.10. *Any proper subgroup H of a nilpotent group is properly contained in its normalizer.*

Theorem 15.1.11. *Let G be a finite group. The following conditions are equivalent:*
(i) G is nilpotent.
(ii) G is a direct product of its sylow subgroups.

Corollary 15.1.12. *Let G be a finite nilpotent group. Then for every divisor m of $o(G)$, there exists a subgroup of G of order m.*

16 Lecture 16

16.1 Rings, subrings and Ideals

Definition 16.1.1. A non-empty set R is called a **ring** if in R, there are defined two binary operations $+$ and . respectively such that

(i) $(R,+)$ is an abelian group.
(ii) $a.b \in R$ for all $a,b \in R$.
(iii) $a.(b.c) = (a.b).c = a.b.c$ for all $a,b,c \in R$.
(iv) $a.(b+c) = a.b + a.c$ and $(b+c).a = b.a + c.a$ for all $a,b,c \in R$. $\square$

Definition 16.1.2. If the multiplication . ina ring R is commutative, that is, $a.b = b.a$ for all $a,b \in R$, we say that R is a *commutative ring.* Also, a ring R need not always contain a multiplicative identity. When it contains, we say that R is a ring with *unity.* We denote the unity of R by 1. A non-zero element of a ring with 1 need not have a multiplicative inverse always. When it does, we say that the non-zero element is a *unit* of the ring. Thus $a(\neq 0)$ is a unit in R if a^{-1} exists. If a and b belong to a commutative ring R and a is non-zero, we say that a divides b and write $a|b$ if there exists an element $c \in R$ auch that $b = ac$. If a does not divide b, we write $a \nmid b$. $\square$

Example(s) 16.1.3. 1) The set $\mathbb{Z}$ of integers under ordinary addition and multiplication is a commutative ring with unity 1. The units of this ring are 1 and -1.
2) The set $\mathbb{Z}_n$ of integers modulo n is a ring under addition and multiplication modulo n. It is a commutative ring with unity 1. The set of all units of this ring is $U(n)$ (PROVE!). $\square$

Notation: We use $b - c$ to denote $b + (-c)$.

Theorem 16.1.4. *Let a,b,c belong to a ring R. Then*
(i) $a.0 = 0.a = 0$.
(ii) $a.(-b) = (-a).b = -(ab)$.
(iii) $(-a).(-b) = ab$.
(iv) $a.(b-c) = ab - ac$ *and* $(b-c).a = ba - ca$.
Furthermore, if R has a unity element 1, then
(v) $(-1).a = -a$.
(vi) $(-1)(-1) = 1$.

Theorem 16.1.5. *If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, then it is unique.*

Definition 16.1.6. A subset S of a ring R is called a **subring** of R if S is itself a ring with the operations of R. $\square$

Theorem 16.1.7. ***Subring test***: *A non-empty subset S of a ring R is a subring of R if both $a-b$ and $a.b$ belong to S whenever $a,b \in S$.*

Example(s) 16.1.8. For each positive integer n, the set $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$ is a subring of $\mathbb{Z}$. $\square$

Definition 16.1.9. A non-zero element a in a commmutative ring R is called a *zero-divisor* if there is a non-zero element b in R such that $ab = 0$. $\square$

Definition 16.1.10. A commutative ring with unity is called an *Integral domain* if it has no zero-divisors. $\square$

Thus in an integral domain, $ab = 0$ implies that either $a = 0$ or $b = 0$.

Example(s) 16.1.11. 1) The ring of integers $\mathbb{Z}$ is an integral domain.
2) The ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ is an integral domain.(PROVE!)
3) $\mathbb{Z}_n$ is an integral domain if and only if n is a prime. $\square$

Theorem 16.1.12. ***Cancellation law**: Let a, b, c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.*

Definition 16.1.13. A commutative ring with unity is called a *field* if every non-zero element in it is a unit. $\square$

Remark 16.1.14. Every field is an integral domain.

Theorem 16.1.15. *A finite integral domain is a field.*

Corollary 16.1.16. $\mathbb{Z}_p$ *is a field.*

Remark 16.1.17. $\mathbb{Z}_n$ is a field if and only if n is a prime.

Definition 16.1.18. The *Characteristic* of a ring R is the least positive integer n such that $n.x = 0$ for all $x \in R$. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $char(R)$. $\square$

Example(s) 16.1.19. $\mathbb{Z}$ has characteristic 0, but $\mathbb{Z}_n$ has Characteristic n. $\square$

Theorem 16.1.20. *Let R be a ring with unity 1. If 1 has infinite order under addition, then $char(R) = 0$. If 1 has order n under addition, then $char(R) = n$.*

Theorem 16.1.21. *The Characteristic of an integral domain is either* 0 *or a prime.*

Definition 16.1.22. A subring A of a ring R is called an **ideal** of R if for every $r \in R$ and every $a \in A$, both ra and ar belong to A. $\square$

Theorem 16.1.23. ***Ideal test**: A non-empty subset A of a ring R is an ideal of R if*
(i) $a - b \in A$ whenever $a, b \in A$. (ii) ra and ar both $\in A$ whenever $a \in A$ and $r \in R$.

Example(s) 16.1.24. 1) For any ring R, $\{0\}$ and R are ideals of R. The ideal $\{0\}$ is called the trivial ideal.
2) Let R be a commutative ring with unity. Let $a \in R$. The set $< a >:= \{ra | r \in R\}$ is an ideal of R, called the principal ideal generated by a. $\square$

16.2 Factor rings

Theorem 16.2.1. *Let R be a ring and A be a subring of R. The set of cosets $\{r + A | r \in R\}$ is a ring under the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R.*

Definition 16.2.2. IF R is a ring and A is an ideal of R, then the set of cosets $\{r + A | r \in R\}$ is a ring under the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$. This ring is called the **factor ring** or the **quotient ring** of R by A and denoted by R/A. $\square$

If R is commutative, so is R/A. If R has a unity 1, then R/A has unity $1 + A$.

16.3 Ring Homomorphisms

Definition 16.3.1. Let R and R' be two rings. A map $\phi : R \to R'$ is aclled a **ring homomorphism** if
(i) $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$ and
(ii) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$. $\square$

Lemma 16.3.2. *If $\phi : R \to R'$ is a ring homomorphism, then*
(i) $\phi(0) = 0$ and
(ii) $\phi(-a) = -\phi(a)$ for all $a \in R$.

Definition 16.3.3. If $\phi : R \to R'$ is a ring homomorphism, then the set $\{a \in R | \phi(a) = 0\}$ is called the *kernel* of ϕ and is denoted by $Ker(\phi)$. □

Lemma 16.3.4. *If $\phi : R \to R'$ is a ring homomorphism, then $Ker(\phi)$ is an ideal of R.*

Definition 16.3.5. A ring homomorphism $\phi : R \to R'$ is called an *isomorphism* if ϕ is both one-to-one and onto. □

Lemma 16.3.6. *If $\phi : R \to R'$ is an onto ring homomorphism, then ϕ is an isomorphism if and only if $Ker(\phi) = \{0\}$.*

Lemma 16.3.7. *Let R be a ring and A be an ideal in R. There always exists an onto ring homomorphism $\pi : R \to R/A$ given by $r \mapsto r + A$ whose kernel is A.*

Theorem 16.3.8. ***First isomorphism theorem****: Let R, R' be rings and $\phi : R \to R'$ be an onto ring homomorphism with kernel U. Then $R' \simeq R/U$. Moerover, there exists a one-to-one correspondence between the set of all ideals of R' and the set of all ideals of R which contain U. This correspondence can be achieved by associating with an ideal W' in R' the ideal W in R defined by $W = \{x \in R | \phi(x) \in W'\}$.*

16.4 The field of fractions of an integral domain

Given a commutative integral domain R with unity 1, consider the set $X = R \times R^*$ where $R^* = R - \{0\}$. Define a binary relation $\sim$ on X by saying that $(a, x) \sim (b, y)$ if $ay = bx$. It is easy to check that $\sim$ is an equivalence relation on X. Let $Q(R)$ denote the set of all equivalence classes in X. For $(a, x) \in X$, we denote by $\frac{a}{x}$ the equivalence class through (a, x) and call it the fraction associated to (a, x).
We make $Q(R)$ into a ring by defining addition as : $\frac{a}{x} + \frac{b}{y} = \frac{ay+bx}{xy}$ and defining multiplication as $\frac{a}{x} . \frac{b}{y} = \frac{ab}{xy}$.

Theorem 16.4.1. *$Q(R)$ with respect to the above two operations $+$ and $.$ forms a field and it contains R as a subring.*

Definition 16.4.2. $(Q(R), +, .)$ is called the *field of fractions* of R. □

Theorem 16.4.3. *For any commutative integral domain R with 1, $Q(R)$ is the smallest field containing R as a subring, smallest in the sense that if K is a field containing R as a subring, then $K \supseteq Q(R)$ as a subfield.*

16.5 Prime ideals and maximal ideals

Definition 16.5.1. A proper ideal A of a ring R is called a **prime ideal** of R if $a, b \in R$ and $ab \in A$ implies either $a \in A$ or $b \in A$. $\square$

Definition 16.5.2. A proper ideal A of a ring R is caled a **maximal ideal** of R if, whenever B is an ideal of R such that $A \subseteq B \subseteq R$, then either $B = A$ or $B = R$. $\square$

Theorem 16.5.3. *Let R be a ring with 1 and I be an ideal of R. Then*
(i) R/I is an integral domain if and only if I is a prime ideal of R.
(ii) R/I is a field if and only if I is a maximal ideal of R.

Corollary 16.5.4. *Every maximal ideal is a prime ideal.*

Corollary 16.5.5. *If R is a finite ring, then every prime ideal of R is a maximal ideal.*

Theorem 16.5.6. *Every proper ideal of a ring R is contained in a maximal ideal.*

17 Lecture 17

17.1 Factorization in domains

Let R be a commutative integral domain with 1. Let $R^* = R \setminus \{0\}$.

Definition 17.1.1. Let a and b be in R with $a \neq 0$. We say that *a divides b* if there exists a $c \in R$ such that $b = ac$ We denote it by $a|b$. $\square$

Remark 17.1.2. $a|b$ if and only if $(b) \subseteq (a)$.

Definition 17.1.3. Two elements a and b in R^* are called **associates** of each other if $a|b$ and $b|a$. $\square$

Proposition 17.1.4. *Let $a, b \in R^*$. Then the following are equivalent:*
(i) a and b are associates of each other.
(ii) $a = ub$ for some unit $u \in R$.
(iii) $(a) = (b)$.

Definition 17.1.5. A non-zero, non-unit element $a \in R$ is called **irreducible** if $a = bc$, then either b or c is a unit. That is, a cannot be written as a product of two non-units. $\square$

Definition 17.1.6. A non-zero, non-unit element $a \in R$ is called **prime** if $a|bc$ implies that either $a|b$ or $a|c$. $\square$

Proposition 17.1.7. *A prime element is always irreducible, but not conversely in general.*

Example(s) 17.1.8. Let $R = \mathbb{Z}[i\sqrt{3}] = \{a + bi\sqrt{3}|a, b \in \mathbb{Z}\}$. The element $1 + i\sqrt{3}$ is irreducible in R but not a prime. $\square$

Theorem 17.1.9. *Let a be a non-zero, non-unit in a commutative integral domain R. Then*
(i) a is irreducible if and only if the ideal (a) is maximal among all principal ideals other than R.
(ii) a is prime if and only if the ideal (a) is a non-zero prime ideal in R.

17.2 Euclidean domains

Definition 17.2.1. A commutative integral domain R (with or without unity) is called a **Euclidean domain** if there exists a map $d : R^* \to \mathbb{Z}^+$ such that
(i) $d(x) \leq d(xy)$ for all $x, y \in R^*$.
(ii) For all $a \in R$ and $b \in R^*$, there exists q and r (depending upon a and b) such that $a = bq + r$ with either $r = 0$ or $d(r) < d(b)$. $\square$

The map d is called the *algorithm map* and property (ii) is called the *division algorithm.*

Proposition 17.2.2. *A non zero Euclidean domain R has unity and the group of all units of R is given by $U(R) = \{a \in R^*|d(a) = d(1)\}$.*

Example(s) 17.2.3. 1) Any field K is a euclidean domain.(WHY?)
2) $\mathbb{Z}$ is euclidean, with the modulus as the algorithm map.
3) The ring of gaussian integers $\mathbb{Z}[i]$ is euclidean with square of modulus as the algorithm map.
4) The polynomial ring $K[X]$ in one variable X over a field K is euclidean with degree of the polynomial as the algorithm map. $\square$

17.3 Principal ideal domains

Definition 17.3.1. A commutative integral domain R is called a **principal ideal domain** or a PID if every ideal of R is principal, that is, generated by one element. $\square$

Theorem 17.3.2. *Every euclidean domain is a PID.*

Example(s) 17.3.3. Every PID need not be a euclidean domain. For instance, $\mathbb{Z}[\theta] := \{a + b\theta | a, b \in \mathbb{Z}\}$ where θ is the complex number $\frac{1+\sqrt{-19}}{2}$, is a PID but not a ED. $\square$

Theorem 17.3.4. *Let R be a PID (with 1). Then*
(i) Every irreducible element is a prime in R.
(ii) Every non-zero prime ideal is maximal in R.

Theorem 17.3.5. *For a commutative integral domain R with 1, the following are equivalent:*
(i) R is a field.
(ii) $R[X]$ is a euclidean domain.
(iii) $R[X]$ is a PID.

17.4 Factorization Domains

Definition 17.4.1. A commutative integral domain R (with 1) is called a **factorization domain** or a FD if every non-zero element $x \in R$ can be written as a unit times a finite product of irreducible elements. $\square$

Theorem 17.4.2. *Every PID is a FD.*

Proposition 17.4.3. *If d is a positive integer, then the ring $\mathbb{Z}[i\sqrt{d}]$ is a FD.*

17.5 Unique Factorization Domains

Definition 17.5.1. A commutative integral domain R (with 1) is called a **unique factorization domain** or a UFD if
(i) R is a FD and
(ii) The factorization into irreducibles is unique upto order and associates. That is, if $x \in R^*$ is factored as

$$x = ua_1a_2 \cdots a_r = vb_1b_2 \cdots b_s$$

where u, v are units and a_i, b_j are irreducibles,then $r = s$ and after some rearrangement, every a_i is an associate of b_i. $\square$

Theorem 17.5.2. *In a UFD, every irreducible element is a prime.*

Theorem 17.5.3. *An integral domain R is a UFD if and only if R is a FD in which every irreducible element is a prime.*

Corollary 17.5.4. *Every PID is a UFD.*

18 Lecture 18

18.1 Reducibility tests

Definition 18.1.1. Let D be an integral domain. A polynomial $f(x) \in D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be *irreducible over D* if whenever $f(x)$ is expressed as a product

$$f(x) = g(x)h(x)$$

with $g(x), h(x) \in D[x]$, then either $g(x)$ or $h(x)$ is a unit in $D[x]$. $\square$

Definition 18.1.2. A non zero non-unit element of $D[x]$ that is NOT irreducible over D is called *reducible over D*. $\square$

Remark 18.1.3. If D equals a field F, then a non constant $f(x) \in F[x]$ is said to be irreducible over F, if $f(x)$ cannot be expressed as a product of two non-constant polynomials of strictly lower degree.

Example(s) 18.1.4. The polynomial $f(x) = 2x^2 + 4$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{Z}$. $\square$

Theorem 18.1.5. *Let F be a field. If $f(x) \in F[x]$ and degree of $f(x)$ equals 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.*

Remark 18.1.6. Note that polynomials of degree > 3 may be reducible over a field, even though they do not have zeros in the field. For example, in $\mathbb{Q}[x]$, the polynomial $x^4 + 2x^2 + 1 = (x^2 + 1)^2$, but has no zeros in $\mathbb{Q}$.

Definition 18.1.7. The **content** of a non-zero polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where the $a_i \in \mathbb{Z}$, is the gcd of the integers $a_n, \ldots, a_1, a_0$. $\square$

Definition 18.1.8. A **primitive polynomial** is an element of $\mathbb{Z}[x]$ having content 1. $\square$

Lemma 18.1.9. ***Gauss's lemma***: *The product of two primitive polynomials in $\mathbb{Z}[x]$ is primitive.*

Theorem 18.1.10. *Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.*

Notation: Let $f(x) \in \mathbb{Z}[x]$ and let p be a prime. Let $\bar{f}^p(x)$ denote the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p.

Theorem 18.1.11. *Let $f(x) \in \mathbb{Z}[x]$ with degree of $f(x) \geq 1$. If there exists some prime p for which $\bar{f}^p(x)$ is irreducible over $\mathbb{Z}_p$ and $deg(\bar{f}^p(x)) = deg(f(x))$, then $f(x)$ is irreducible over $\mathbb{Q}$.*

Theorem 18.1.12. ***Eisenstein's criterion***: *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there exists a prime p such that $p \nmid a_n$, $p \mid a_{n-1}$,......., $p \mid a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.*

Corollary 18.1.13. *For any prime p, the p th cyclotomic polynomial*

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

18.2 Gauss's theorem for UFD s

Definition 18.2.1. Let X be a non-empty subset of a commutative ring R. An element $d \in R$ is called **a gcd** of X if
(i) $d \mid a$ for all $a \in X$ and
(ii) $c \mid a$ for all $a \in X$ implies that $c \mid d$. $\square$

Let D be a UFD. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ be a non-zero polynomial.

Definition 18.2.2. A gcd of the coefficients $a_0, a_1, \ldots, a_n$ is called a **content** of f and is denoted by $c(f)$. $\square$

Remark 18.2.3. $c(f)$ is unique upto multiplication by units.

Notation: We shall write $b \approx c$ whenever b and c are associates in D. Observe that $\approx$ is an equivalence relation on D.

Remark 18.2.4. If $a \in D$ and $f \in D[x]$, then $c(af) \approx ac(f)$.

Definition 18.2.5. If $f \in D[x]$ and $c(f)$ is a unit in D, then f is said to be **primitive**. $\square$

Remark 18.2.6. 1) For any polynomial $g \in D[x]$, we have $g = c(g)g_1$ with g_1 primitive.
2) Any non-constant irreducible polynomial in $D[x]$ is primitive.

Lemma 18.2.7. ***Gauss's lemma***: *Let D be a UFD and let $f, g \in D[x]$. Then $c(fg) \approx c(f)c(g)$.In particular, the product of two primitive polynomials is primitive.*

Lemma 18.2.8. *Let D be a UFD with field of fractions F. Let f and g be primitive polynomials in $D[x]$. Then f and g are associates in $D[x]$ if and only if they are associates in $F[x]$.*

Lemma 18.2.9. *Let D be a UFD with field of fractions F. Let f be a primitive polynomial of positive degree in $D[x]$. Then f is irreducible in $D[x]$ if and only if f is irreducible in $F[x]$.*

Theorem 18.2.10. ***Gauss's theorem***: *D is a UFD if and only if $D[x]$ is a UFD.*

Corollary 18.2.11. *The polynomial ring over a UFD is a UFD. (The number of variables may be finite or infinite.)*

Theorem 18.2.12. ***Eisenstein's criterion***: *Let D be a UFD with field of fractions F. If $f = \Sigma_{i=0}^{n} a_i x^i \in D[x]$, $deg(f) \geq 1$ and p is an irreducible element of D such that $p \nmid a_n$, $p \mid a_{n-1}, \ldots\ldots, p \mid a_0$ and $p^2 \nmid a_0$, then f is irreducible in $F[x]$.*

19 Lecture 19

19.1 Extension fields

Definition 19.1.1. Let F be a field. A field E is said to be an **extension** of F if $F \subseteq E$. $\square$

If E is an extension of F, then under the ordinary field operations in E, E is a vector space over F.

Definition 19.1.2. The **degree** of E over F is the dimension of E as a vector space over F. It is denoted by $[E : F]$. $\square$

Theorem 19.1.3. *Let F be a field and let $f(x)$ be a non-constant polynomial in F[x]. Then there exists an extension filed E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.*

Definition 19.1.4. An element α of an extension field E of a field F is called **algebraic** over F if $f(\alpha) = 0$ for some non-zero $f(x) \in F[x]$. If α is NOT algebraic over F, we say that α is **transcendental** over F. $\square$

Theorem 19.1.5. *Let E be an extension field of F, let $\alpha \in E$ be such that α is algebraic over F. Then there exists an irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. This irreducible polynomial $p(x)$ is uniquely determined upto a constant factor in F and it is a polynomial of minimal degree ≥ 1 in $F[x]$ having α as a zero. Moreover, if $f(\alpha) = 0$ for $f(x) \in F[x]$ with $f(x) \neq 0$, then $p(x)$ divides $f(x)$.*

Remark 19.1.6. By multiplying by a suitable constant in F, we can assume that $p(x)$ (in the theorem above) is a monic polynomial, that is, the coefficient of the highest power of x appearing in $p(x)$ is 1.

Definition 19.1.7. Let E be an extension field of a filed F. Let $\alpha \in E$ be algebraic over F. The unique monic polynomial $p(x)$ having the properties described in the preceeding theorem is called the **irreducible polynomial of α over F**, denoted by $irr(\alpha, F)$. The degree of the polynomial $irr(\alpha, F)$ is called the **degree of α over F**, denoted by $deg(\alpha, F)$. $\square$

Notation: Let F be a field and let $a_1, a_2, \ldots, a_n$ be elements of some extension E of F. Then $F(a_1, \ldots, a_n)$ denotes the smallest subfield of E that contains F and the set $\{a_1, a_2, \ldots, a_n\}$.

Theorem 19.1.8. *Let E be an extension field of F. Let $\alpha \in E$ be algebraic over F. Then $F(\alpha) \backsimeq F[x]/ < irr(\alpha, F) >$.*

Definition 19.1.9. An extension field E of a field F is called a **simple extension** of F if $E = F(\alpha)$ for some $\alpha \in E$. $\square$

Theorem 19.1.10. *Let E be an extension field of F. Let $\alpha \in E$ be algebaric over F. Let the degree of $irr(alpha, F)$ be $n \geq 1$. Then every element β of $F(\alpha)$ can be uniquely expressed in the form $\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$ where $b_i \in F$.*

Definition 19.1.11. If an extension field E of a field F is of finite dimension as a vectore space over F, we say that E is a **finite extension** of F. $\square$

Remark 19.1.12. Let E be an extension field of F and let $\alpha \in E$ be algebraic over F. Then the previous theorem says that $F(\alpha)$ is a finite extension of F and $[F(\alpha) : F] = deg(\alpha, F)$.

Theorem 19.1.13. *Let E be an extension field of F and let $\alpha \in E$ be algebraic over F. If $deg(\alpha, F) = n$, then $F(\alpha)$ is an n-dimensional vector space over F with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Furthermore, every element β of $F(\alpha)$ is algebraic over F, and $deg(\beta, F) \leq deg(\alpha, F)$.*

19.2 Algebraic extensions

Definition 19.2.1. An extension field E of a field F is called an **algebraic extension** of F is every element in E is algebraic over F. $\square$

Theorem 19.2.2. *A finite extension is always algebraic.*

Theorem 19.2.3. *If E is a finite extension field of a field F, and K is a finite extension field of E, then K is a finite extension field of F and $[K : F] = [K\text{‘} : E][E : F]$.*

Corollary 19.2.4. *If F_i is a field for $i = 1, \ldots, r$ and F_{i+1} is a finite extension of F_i, then F_r is a finite extension of $F - 1$ and*

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1].$$

Corollary 19.2.5. *If E is an extension field of F, $\alpha \in E$ is algebraic over F and $\beta \in F(\alpha)$. Then $deg(\beta, F)$ divides $deg(\alpha, F)$.*

Theorem 19.2.6. *Let E be an algebraic extension of a field F. Then there exists a finite number of elements $\alpha_1, \ldots, \alpha_n$ in E such that $E = F(\alpha_1, \ldots, \alpha_n)$ if and only if $[E : F] < \infty$.*

19.3 Splitting fields

Definition 19.3.1. Let E be an extension field of F and let $f(x) \in F[x]$. We say that $f(x)$ **splits** in E if $f(x)$ can be factored as a product of linear factors in $E[x]$. □

Definition 19.3.2. We call E a **splitting field** for $f(x)$ over F if $f(x)$ splits in E but in no proper subfield of E. □

Remark 19.3.3. If $f(x) \in F[x]$ and $f(x)$ factors as

$$b(x - a_1)(x - a_2) \cdots (x - a_n)$$

over some extension E of F, then $F(a_1, \ldots, a_n)$ is a splitting field for $f(x)$ over F.

Theorem 19.3.4. *Let F be a field and let $f(x)$ be a non-constant element of $F[x]$. Then there exists a splitting field E of $f(x)$ over F.*

Theorem 19.3.5. *Let ϕ be an isomorphism from a field F to a field F'. Let $f(x) \in F[x]$. If E is a spiltting field for $f(x)$ over F and E' is a splitting field for $\phi(f(x))$ over F', then there exists an isomorphism from E to E' that agrees with ϕ on f.*

Corollary 19.3.6. ***Splitting fields are unique upto iso****: Let F be a field and let $f(x) \in F[x]$. Then any two splitting fields of $f(x)$ over F are isomorphic.*

19.4 Algebraic extensions revisited

Let E be an extension field of a field K. Let $S \subseteq E$ be any subset (finite or infinite).

Definition 19.4.1. $K(S) :=$ the samllest subfield of E containing K ans S. □

Theorem 19.4.2. *The subfield $K(S)$ consists of all elements of the form $f(u_1, \ldots, u_n)g(u_1, \ldots, u_n)^{-1}$ where n is a positive integer, $f, g \in K[x_1, \ldots, x_n]$, $u_1, \ldots, u_n \in S$ and $g(u_1, \ldots, u_n) \neq 0$.*

Theorem 19.4.3. *If K is an algebraic extension of E and E is an algebraic extension of F, then K is an algebraic extension of F.*

Corollary 19.4.4. *Let E be an extension field of F. Then the set of all elements of E that are algebraic oer F, is a subfield of E.*

Definition 19.4.5. For any extension E of a field F, the subfield of E consisting of all the elements of E that are algebraic over F, is called the **algebraic closure** of F in E. □

Remark 19.4.6. Finite extensions are always algebraic, but algebraic extension need not always be finite. For example, $\mathbb{Q}(2^{1/2}, 2^{1/3}, 2^{1/4}, \ldots)$ is an algebraic extension of $\mathbb{Q}$ that is not finite.

19.5 Characteristic of a field

The characteristic of a field is defined as the characteristic of the underlying ring.

Theorem 19.5.1. *The characteristic of a field os either 0 or a prime p.*

Theorem 19.5.2. *If F is a field of characteristic p (p a prime), then F contains a subfield isomorphic to $\mathbb{Z}_p$.If F is a field of characteristic 0, then F contains a subfield isomorphic to $\mathbb{Q}$.*

Remark 19.5.3. Every field has a smallest subfield, that is, a subfield which is contained in every subfield. Such a smallest subfield is equal to the intersection of all subfields of a field, hence is unique.

Definition 19.5.4. This SMALLEST subfield is called the **prime subfield** of the given field. □

Theorem 19.5.5. *The prime subfield of a field of characteristic p is isomorphic to $\mathbb{Z}_p$, whereas the prime subfield of a field of characteristic 0 is isomorphic to $\mathbb{Q}$.*

19.6 Finite fields

Theorem 19.6.1. *For each prime p and each positive integer n, there exists, upto isomorphism, a unique finite field of order p^n.*

Definition 19.6.2. Since there is only one field (upto isomorphism) for each prime power p^n, we may unambiguously denote it by $GF(p^n)$, in honor of Galois, and call it **the Galois field of order** p^n. □

Theorem 19.6.3. *As a group under addition, $GF(p^n)$ is isomorphic to*

$$\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p \ (n \text{ times}).$$

As a group under multiplication, the set of all non-zero elements of $GF(p^n)$ is isomorphic to $\mathbb{Z}_{p^n-1}$ (and, is therefore, cyclic).

Corollary 19.6.4. $[GF(p^n) : GF(p)] = n$.

19.7 Subfields of a finite field

Theorem 19.7.1. *For each divisor m of n, $GF(p^n)$ has a unique subfield of order p^m. Moreover, these are the only subfields of $GF(p^n)$.*