Department of Computer Science and Engineering, NIT Calicut

Lecture 1: Basic Algebraic Structures

Prepared by: K Murali Krishnan

These notes assume that the reader is not totally unfamiliar with the notions of groups, rings fields and vector spaces. The definitions are stated here only for fixing the notation. Exercises list out elementary facts which the reader is expected to know before proceeding further. Standard facts about matrices and determinants will be used without explanation.

Notation

Let $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ denote the set of integers, rationals, reals and complex numbers respectively. Let $\mathbf{N} = \{0, 1, 2, ..\}$. We will use the notation $\mathbf{M_n(R)}$, $\mathbf{M_n(Q)}$, $\mathbf{M_n(C)}$ to denote the set of $n \times n$ matrices with real, rational and complex entries.

Groups

Definition 1. *A* **monoid** $(G, .)$ *is a (non empty) set* G *together with an associative binary operator "." on* G *having an identity element (denoted by* 1 *or sometimes* e*). If "." is commutative,* G *will be called a* **commutative monoid**. *G is a* **group** *if in addition every element in* G *has an inverse. A commutative group is called an* **Abelian group**.

Exercise 1. *Find the category to which* $(\mathbf{Z}, +)$, $(\mathbf{Z}, .)$, $(\mathbf{Q}, +)$, $(\mathbf{Q}, .)$, $(\mathbf{N}, +)$, $(\mathbf{N}, .)$ *belong to where, "+" and "." represent standard addition and multiplication. What about* $(Q \setminus \{0\}, .)$*? and* $(N \setminus \{0\}, .)$*?*

Example 1. $(M_n(X), +)$ *for* $X \in \{\mathbf{Q}, \mathbf{R}$ *or* $\mathbf{C}\}$ *and "+" the standard matrix addition is an Abelian group with zero matrix* 0 *as identity.* $(M_n(X), .)$ *for* $X \in \{\mathbf{Q}, \mathbf{R}$ *and* $\mathbf{C}\}$ *and "." the standard matrix multiplication is a (non-commutative) monoid with the* $n \times n$ *identity matrix* I_n *as identity. The set* $GL_n(X)$ *consisting of* **non-singular** $n \times n$ *matrices over* X *forms a (non-Abelian) group with respect to multiplication.*

Example 2. *The set* $(X^n, +)$*, consisting of* $n-$*tuples where* $X \in \{\mathbf{Q}, \mathbf{R}$ *or* $\mathbf{C}\}$ *is an Abelian group with standard vector addition. Let* T *be any (non-empty) set. If we consider the set of functions from a set* T *to* X $(X^T, +)$ *with addition of functions as point-wise addition, then these functions form an Abelian group with* $(f + g)(t)$ *defined as* $f(t) + g(t)$ *for each* $t \in T$*. The identity is the function* 0 *(*$0(t) = 0$ *for all* $t \in T$*). Note that* X^n *is a special case of this example where* $T = \{1, 2, ..n\}$*. (why?).*

Example 3. *The set* Z_n *is used to denote the set* $\{0, 1, 2, .., n-1\}$ *with "+" denoting addition modulo* n*. We will see later that* $Z_n, +$ *is an Abelian group.*

Exercise 2. *If* $(G, .)$ *is a group with* $a, b \in G$*.*

1. *Show that a group can have at most one identity element.*
2. *Show that an element has at most one inverse in a group.*

Rings and Fields

Definition 2. *A set $(R, +, .)$ with two operators is a* **ring (with unity)** *if $(R, +)$ is an Abelian group, $(R, .)$ is a monoid and "." distributes over "+". A ring R is a* **commutative** *if $(R, .)$ is a commutative monoid. A commutative ring R is a* **field** *if $(R \setminus \{0\}, .)$ is an Abelian group. Normally 0 and 1 are used to represent the additive and multiplicative identities.*

Exercise 3. *Which among $(\mathbf{Z}, +, .)$, $(\mathbf{N}, +, .)$, $(\mathbf{Q}, +, .)$ are rings?. Which among them are fields?*

Example 4. *$(M_n(\mathcal{R}), +, .)$ is a non-commutative ring with unity (identity matrix I_n).*

Example 5. *The set $(Z_n, +, .)$ is used to denote the set $\{0, 1, 2, .., n-1\}$ with "+" denoting addition modulo n and "." denoting multiplication modulo n. We will see later that $Z_n, +$ is a commutative ring with unity.*

Example 6. *Let R be any commutative ring with unity. Let $R[x]$ denote the set of polynomials with coefficients in R. Then $R[x]$ forms a commutative ring with unity with standard polynomial addition and multiplication.*

Exercise 4. *Let $(R, +, .)$ be a ring. Let a, b, c be elements in R. Let $-a, -b, -c$ and a^{-1}, b^{-1}, c^{-1} respectively denote the additive and multiplicative inverses (whenever they exist) of a, b and c. Prove the following facts:*

1. *$a + 0 = a$ for all $a \in R$.*
2. *$-(ab) = (-a)b = a(-b)$.*
3. *0 does not have a multiplicative inverse.*
4. *If a has an inverse and $ab = ac$ then $b = c$. Show an example (in $M_2(\mathcal{R})$ to show that this fails if a is not invertible.) This property is called* cancellation law.
5. *Show that $ab = ac$ implies $b = c$ may hold for all $a, b, c \in R$, $a \neq 0$ even though R is not a field (Hint: consider integers). However, if R is finite, show that this condition will ensure that R is a field.*
6. *Show that invertible elements in R, called R^* forms a group (w.r.t multiplication). This group is called the* **unit group** *of R. Thus a field is a commutative ring with $R^* = R \setminus \{0\}$.*
7. *Show that if R is a field then $R[x]$ satisfies cancellation law.*

Vector Spaces

Definition 3. *An Abelian group $(V, +)$ is a vector space over a field F if there is* scalar multiplication *function "." from $F \times V$ to V satisfying $(a + b)v = av + bv$, $a(bv) = (ab)v$, $1v = v$, $a(v + w) = av + aw$ for all $a, b \in F$ and $v, w \in V$. Normally we write $V(F)$ to denote a vector space V over field F.*

Example 7. $\mathbf{R^n}$ *over* $\mathbf{R}$ *or* $\mathbf{Q}$ *(but not* $\mathbf{C}$ *– why?) is a vector space with addition and scalar multiplication defined in the standard way. So is* $\mathbf{C^n}$ *over* $\mathbf{R}$, $\mathbf{Q}$ *or* $\mathbf{C}$.

Example 8. *If* F *is any field, the set* F^n *consisting of* n *tuples over* F *is a vector space over* F *where multiplication of a vector with a scalar is defined (in the standard way) as component-wise multiplication.* $M_n(\mathbf{X})$ *is a vector space over* X *for* $X \in \{\mathbf{Q}, \mathbf{R}, \mathbf{C}\}$. *In general, if* T *is any set and* F *any field, then the set of functions from* T *to* X *(denoted by* X^T*) is a vector space over* F *with scalar multiplication defined in the standard way as* $(\alpha f)(x) = \alpha f(x)$. *The previous examples are special cases of this general case (how?).*

Example 9. *If* F *is a field, the set* $F[x]$ *of polynomials with coefficients in* F *is a vector space over* F.

Subgroups, Subrings and Subspaces

Definition 4. *A (non-empty) subset* S *or a group* $(G, .)$ *is called a* **subgroup** *if* $(S, .)$ *is a group. A subset* S *or a ring* $(R, .)$ *is called a* **subring** *if* $(R, +, .)$ *is a ring. A subset* V' *of a vector space* $V(F)$ *is called a* **subspace** *if* $V'(F)$ *is a vector space.*

Example 10. $(\mathbf{Q}, +)$ *is a group of* $(\mathbf{R}, +)$ *and the set of even numbers* $(2\mathbf{Z}, +)$ *is a subgroup of* $(\mathbf{Z}, +)$. *(In fact,* $k\mathbf{Z}$ *consisting of integer multiples of* k *is an additive subgroup of* Z *for any positive integer* k*.)* $(\mathbf{Q}, +, .)$ *is a subring (and a subfield) of* $(\mathbf{R}, +, .)$. $\mathbf{R}(\mathbf{R})$ *is a subspace of* $\mathbf{C}(\mathbf{R})$.

Example 11. *Consider* $F[x]$ *consisting of polynomials with coefficients in* F. *Consider* $xF[x]$ *which are polynomials with no constant term. It is easy to see that* $xF[x]$ *is a subring and a subspace of* $F[x]$ *over* F. *In general* x *may be replaced in this example with any* $g(x) \in F[x]$.

Example 12. *Consider* $\mathbf{R^2}$ *the two dimensional Cartesian place. Any line through the origin* $\{(x, y) \in \mathbf{R^2} : (ax + by = 0)\}$ *for any* $a, b \in \mathbf{R}$ *is a subspace. This subspace consists of the line through the origin perpendicular to the vector* (a, b). *The whole* R^2 *and the single point* $(0, 0)$ *are trivial subspaces. In general, in* R^n, *the (hyper) plane through the origin perpendicular to the vector* $(a_1, a_2, ...a_n)$ *will be the subspace defined by* $a_1x_1 + a_2x_2 + ... + a_nx_n = 0$.

Example 13. *The set of all* $n \times n$ *real matrices with determinant* ± 1 *denoted by* $SL_n(\mathbf{R})$ *(called* orthogonal matrices*) is a subgroup of* $GL_n(\mathbf{R})$ *with respect to multiplication.*

Exercise 5. *Suppose* $V(F)$ *is a vector space, show that* $V' \subseteq V$ *is a subspace if and only if for each* $v, w \in V'$, $av + bw \in V'$ *for any* $a, b \in F$.

Exercise 6. *If* G *is a group, then* $S \subseteq G$ *is a subgroup if and only if for all* $a, b \in S$, $ab^{-1} \in S$. *Moreover, if* G *is finite, then if* $1 \in S$ *and for all* $a, b \in S$ $a, b \in S$, *then* S *is a subgroup.*

Exercise 7. *Let* $S = \{v_1, v_2, ..v_m\}$ *be vectors in a vector space* $V(F)$. *Define* $span(S) = \{a_1v_1 + a_2v_2 + ... + a_mv_m : a_1, a_2, ..a_m \in F\}$. *Show that* $span(S)$ *is a subspace of* V. *Show that a span of a non-zero vector* (x, y, z) *in* $\mathbf{R}^3(\mathbf{R})$ *is a line through the origin. Show that two points* (x, y, z) *and* (x', y', z') *spans a plane if and only if* $(0, 0, 0), (x, y, z)$ *and* (x', y', z') *are not on the same line.*

Department of Computer Science and Engineering, NIT Calicut

Lecture 2: Quotient Spaces

Prepared by: K Murali Krishnan

We focus on properties of cosets (to be defined below) defined by a subgroup of a group. Since (commutative) rings and vector spaces contain an Abelian group within, these properties hold for subrings and subspaces as well.

Definition 5. *Let H be a subgroup of a group G and let $a \in G$. Define the (left)* **coset** *of H, $aH = \{ax : x \in H\}$. (the notation $a + H$ will be used if the group operation is $+$).*

Example 14. *In the group $(\mathcal{Z}, +)$, consider the subgroup nZ consisting of all integer multiples of n. The cosets are $0 + Z = \mathcal{Z}$, $1 + \mathcal{Z} = \{1 \pm tn, t \in \mathcal{Z}\}$ etc. The coset defined by the number k, $k + \mathcal{Z} = \{k \pm tn, t \in \mathcal{Z}\}$. Show that if k and k' differ by a multiple of n, then $k + Z = k' + \mathcal{Z}$. Thus there are exactly n cosets, each one non-empty and disjoint. Moreover, every integer belongs to exactly one of the cosets. That is, the cosets partition the group.*

Example 15. *In $(\mathcal{C} \setminus 0, .)$, consider the (subgroup defined by) the unit circle $H = \{z \in \mathcal{C} : |z| = 1\}$. The cosets are rings of radius r for each positive real $r > 0$ around the origin in the Argand plane. Show that if a, b are complex numbers with $|a| = |b|$, then $aH = bH$. Note that here too, the cosets partition the group.*

Example 16. *In $\mathcal{R}^2$, the subspace defined by the line $ax+by = 0$ perpendicular to the point (a, b) through the origin. The coset defined by the point (p, q) is the line passing through (p, q) parallel to the line above. In this case as well, the cosets partition R^2. Generalize this example to R^n.*

Exercise 8. *Consider the subgroup $\mathcal{Z}$ of $\mathcal{Q}$. When are the cosets defined by rationals r and s the same? Can two different cosets have an non-empty intersection?*

We will now show that cosets equipartition the group.

Lagrange's Theorem

Let H be a subgroup of a group G.

Exercise 9. *If $a \in H$. Show that $aH = H$.*

Exercise 10. *Let $a, b \in G$. Define the map $f : aH \longrightarrow bH$ by $f(ah) = bh$ for each $h \in H$. Show that the map is bijective.*

The last two exercises show that every coset has the same size and H itself is one of the cosets. The following lemma show that cosets are disjoint.

Lemma 1. *if $aH \neq bH$ then $aH \cap bH = \emptyset$.*

Proof. Let $z \in aH \cap bH$. Then $\exists h_1, h_2 \in H$ such that $z = ah_1 = bh_2$. Multiplying on the right with h_1^{-1}, we have $a = bh_2h_1^{-1}$. Thus we see that $a \in bH$. If now $x \in aH$ – i.e., $x = ah_3$ for some $h_3 \in H$, then $x = bh_2h_1^{-1}h_3$ and thus $x \in bH$ as well. We have thus $aH \subseteq bH$. Similarly $bH \subseteq aH$. □

We that the cosets of H partition G into equal sized disjoint subsets, one of which is H itself. The following theorem is immediate:

Theorem 1 (Lagrange's Theorem)**.** *The size of any subgroup of a finite group G must divide the size of G.*

Corollary 1. *If G is a group with prime number of elements, then only $\{1\}$ and G are the subgroups of G.*

Quotient Groups

Let G be a group and H be a subgroup. Consider the collection of cosets of H denoted by G/H. That is $G/H = \{aH : a \in G\}$. Note that each element in G/H is a coset containing many elements in G. We will show that we can define a multiplication operation between elements in G/H if H satisfies certain *normality condition*. In this case, G/H will form a group with the multiplication operation essentially "inherited" from G.

Definition 6. *H is a normal subgroup of G if for any $a \in G$ and $h \in H$ $aha^{-1} \in H$.*

Example 17. *If G is Abelian, all subgroups and normal (why?).*

Exercise 11. *Show that $GL_n(\mathcal{R})$ and $SL_n(\mathcal{R})$ are normal subgroups of $M_n(\mathcal{R})$.*

These notes will be dealing with mostly Abelian groups and hence almost all examples in will involve only normal subgroups. In the following, assume that H is a **normal subgroup** of G.

Exercise 12. *Let $a \in G$ and $h \in H$. Show that there exists $h' \in H$ such that $ah = h'a$. This allows us to "shift a to the right" in a product when H is normal.*

Exercise 13. *Let $x \in aH$ and $y \in bH$. Show that $xy \in abH$. (Hint: Use previous exercise. Note that normality of H is crucial here).*

Lemma 2. *If $a'H = aH$ and $b'H = bH$, then $a'b'H = abH$.*

Proof. Since $a'H = aH$ and $b'H = bH$, we have $a' = ah_1$ and $b' = bh_2$ for for some $h_1, h_2 \in H$. Now, Let $z \in a'b'H$. Then $z = a'b'h_3$ for some $h_3 \in H$. Thus $z = ah_1bh_2h_3$. By normality of H, there is an $h_1' \in H$ such that $h_1b = bh_1'$. Hence $z = abh_1'h_2h_3$. Thus $a'b'H \subseteq abH$. Similary the reverse inequality may be proved. □

The lemma above allows us to define a multiplication between cosets. Simply define the product of aH and bH to be abH and the definition is consistent by the lemma. (Why do we need the lemma to make the definition consistent?).

Theorem 2. *$(G/H, .)$ where multiplication in G/H is defined by $aH.bH = abH$ is a group*

Proof. Show that $H = 1H$ is the identity and the inverse of aH is $a^{-1}H$. The rest follow from associativity of G and the previous lemma. □

Example 18. *If we consider group $(\mathcal{Z}, +)$ and the subgroup $3\mathcal{Z}$ of multiples of 3 in $\mathcal{Z}$, in the group $\mathcal{Z}/3\mathcal{Z}$ the inverse of $1 + \mathcal{Z}$ is $2 + \mathcal{Z}$ etc.*

The quotient group construction can be extended to rings and vector spaces as well. The analogue of normal subgroup in a ring is an *ideal*.

Definition 7. *A subset I of a ring R is an ideal if $(I, +)$ is a subgroup of $(R, +)$ and for all $a \in I$ and $x \in R$, $ax \in I$.*

Example 19. *$n\mathbf{Z}$ is an ideal in $\mathbf{Z}$. The set of all polynomials in $\mathbf{R}[x]$ which are multiples of $f(x) \in \mathbf{R}[x]$ is an ideal.*

Exercise 14. *If F is a field, show that the only ideals in F are $\{0\}$ and F itself.*

Exercise 15. *Let I be an ideal in a ring $(R, +, .)$. If $a' + I = a + I$ and $b' + I = b + I$, then $a'b' + I = ab + I$.*

Exercise 16. *Show that the set R/I with addition defined by $(a + I) + (b + I) = (a + b) + I$ and multiplication defined by $(a + I)(b + I) = ab + I$ for any $a, b \in R$. forms a ring This ring is called the* **quotient ring** *in R defined by the ideal I. (where did you use the fact that I is an ideal and not merely a subring?).*

Definition 8. *In the ring $(\mathcal{Z}, +, .)$, nZ is an ideal for any positive integer n. The ring $\mathcal{Z}/n\mathcal{Z}$ is a commutative ring with unity where the unity is $1 + n\mathcal{Z}$ and zero $0 + n\mathcal{Z} = n\mathcal{Z}$. Note that this is essentially the ring Z_n if we identify the coset $i + n\mathcal{Z}$ with the element i for $i \in \{0, 1, 2.., n\}$.*

Definition 9. *Let F be a field and let $f(x) \in F[x]$ of degree n. Consider the ideal I consisting of all polynomials that are multiples of $f(x)$. Then $F[x]/I$ is a commutative ring with unity with one coset per polynomial of degree at most $n - 1$ with addition and multiplication performed modulo $f(x)$. This ring is denoted by $F[x]/f(x)$ and can be identified with the ring of polynomials of degree atmost $n - 1$ with addition and multiplication performed modulo $f(x)$.*

Exercise 17. *Let $V(F)$ is a vector space and W a subspace of F. Let $u \in V$ and $\alpha \in F$. Show that $\alpha(u + W) = \alpha u + W$. Hence conclude the V/W is a vector space over F. This vector space is called the* **quotient space** *(in V) defined by W.*

Example 20. *Consider the subspace W defined by the line $x + y = 0$ in $V = \mathcal{R}^2$. For each real number r, the line parallel to $x + y = 0$ passing through $(r, 0)$ is an element (coset) in the quotient space.*

Department of Computer Science and Engineering, NIT Calicut

Lecture 3: Euclidian Domains

Prepared by: K Murali Krishnan

The primary object of study in this lecture are the rings $\mathbf{Z}$ and the ring of polynomials with coefficiants in a field F denoted by $F[x]$. Both these rings share the common *Euclidian* property that division with remainder is possible. We will show that the existance of unique factorization of elements in these rings into prime factors is a consequence of the Euclidian property of these rings.

Definition 10. *A ring R is an* **integral domain** *if for any $a, b \in R$, whenever $ab = 0$, either $a = 0$ or $b = 0$.*

Exercise 18. *Show that a ring is an integral domain if and only if whenever $ab = ac$, $a \neq 0$ $b = c$ for all $a, b, c \in R$.*

Exercise 19. *Show that every field is an integral domain. If F is a field, show that $F[x]$, is an integral domain. Thus $\mathbf{R}[x]$, $\mathbf{Q}[x]$ etc. are integral domains.*

Example 21. *Note: $F[x]$ may* not *an integral domain when F is not a field. For instance, in $\mathbf{Z}_4[x]$ the product of $2x$ with itself is 0 though $2x \neq 0$.*

Exercise 20. *Is $\mathbf{Z}$ is an integral domain? Show that $Z_n[x]$ is not integral domain if n is composite. Later we will see that $\mathbf{Z}_n[x]$ is an integral domain if and only if n is prime.*

Recall that Exercise 4 asks you to show that the set of invertible elements in a ring R forms a group called the unit group R^* of R. We assume that $(R, +, .)$ is an integral domain in the rest of this lecture. The following definitions are fundamental.

Definition 11. *Let $(R, +, .)$ be an integral domain.*

1. *$u \in R$ is called a* **unit** *if $u \in R^*$.*
2. *$a \in R$ is said to* divide *$b \in R$ if there is a $c \in R$ such that $b = ac$. In this case we write $a|b$.*
3. *$a, b \in R$ are called* **associates** *if $b = au$ for some unit $u \in R$.*

Exercise 21. *Show that divisability is a reflexive, anti-symmetric and transitive relation in R.*

Exercise 22. *Suppose we define the following relation in R: $a \simeq b$ if a, b are associates. Show that $\simeq$ is an equivalance relation on R. Show that a, b are associates if and only if both $a|b$ and $b|a$.*

Exercise 23. *What is $\mathbf{Z}^*$? What are the associates of a number k in $\mathbf{Z}$? Show that a polynomial $a(x) \in F[x]$ is a unit if and only if $a \in F$. Hence units in $F[x]$ are precisely constant polynomials. What are the associates of $(x^2 + 1)$ in $\mathbf{R}[x]$?*

Definition 12. *A* **Euclidian function** *on an integral domain R is a map that assigns for each $a \in R \setminus \{0\}$ a positive integer $|a|$ satisfying the following property:*
Whenever $a, b \in R$ satisfying $|b| < |a|$ then there exists q, r in R such that $a = bq + r$ with either $r = 0$ or $|r| < |b|$. A Euclidian Domain *is a ring with a Euclidian function. Any q, r satisfying above are called a* quotient *and a* remainder *obtained by dividing a with b.*

Note that neither q nor r needs to be unique. If $r = 0$, clearly $a|b$.

Example 22. **Z** *is a Euclidan domain with Eucldian valuation of a number equal to its absolute value. In $F[x]$ the degree function is a Euclidian valuation. Note that $7 = 3.2+1 = 3.3-2$ in Z. Hence there are two possible q, r pairs $(2, 1)$ and $(3, -2)$ for $a = 7$ and $b = 3$.*

Exercise 24. *Suppose $a, b, d \in R$ such that $d|a$ and $d|b$, show that for any $x, y \in R$, $d|(ax + by)$. Hence a common divisor of a, b divides every linear combination of a and b in R. Hence if $d|a$, $d|b$ then if r is a remainder obtained by dividing a by b, then $d|r$ as well.*

Exercise 25. *Let $d \in R$. Denote by $< d >= \{x \in R : d|x\}$. Thus $< d >$ is the set of multiples of d. Show that $< d >$ is an ideal in R. Moreover if I' is any ideal in R with $d \in I'$ then show that $I \subseteq I'$. Thus $< d >$ is the* smallest *ideal in R containg d and is called the* ideal generated by *d.*

Exercise 26. *Suppose $a, b \in R$, show that the set $< a, b >= \{ax + by : x, y \in R\}$ is an ideal and is the smallest ideal containing a and b in R in the sense of exercise above.*

Definition 13. *An ideal I in a ring R is a* principal ideal *if there exists some $d \in R$ such that $I =< d >$. An integral domain R is* Principal Ideal Domain (PID) *if every ideal in R is principal.*

Theorem 3. *Every Euclidian domain R is a Principal Ideal domain.*

Proof. Let I be an ideal in R. Let $d \in I$ be a non-zero element of smallest valuation in I. (i.e., $|d| \leq |e|$ for every $e \in I \setminus \{0\}$). Let $a \in I \setminus \{0\}$. Then, $|a| \geq |d|$. Let q, r be such that $a = qd + r$. But as $d, a \in I$, $r \in I$. since $|r| < |d|$ cannot hold, $r = 0$. But then $a = qd$. Moreover, every mulitple of d must be in I. (why). Hence proved. □

Euclidian Algorithm

Throughout this section, R will be a Euclidian domain with valuaton $||$.

Definition 14. *$d \in R$ is a* greatest common divisor (GCD) *of $a, b \in R$ if $d|a, d|b$ and whenever $e|a$ and $e|b$ for some $e \in R$, then $e|d$. We denoted by $GCD(a, b) = \{d \in R$ such that d is a GCD of a and $b\}$.*

Exercise 27. *Find all $d \in$ **Z** that satisfies $d = GCD(4, 9)$.*

Exercise 28. *Suppose $d, d' \in GCD(a, b)$ then show that $d \simeq d'$. i.e., d, d' are associates. This shows that $GCD(a, b)$ is unique upto multiplication by units.*

Next we show that when R is a Euclidian domain then $GCD(a, b)$ exists for all $a, b \in R$. Moreover, we can express every $d \in GCD(a, b)$ in the form $ax + by$ for some $x, y \in R$. We begin with the following simple cases:

Exercise 29. *Show that $a \in GCD(a,0)$ if $a \neq 0$. Show that $b \in GCD(a,b)$ if $b|a$. In the above two cases, for each $d \in GCD(a,b)$, show that we can find Find $x, y \in R$ such that $d = xa + yb$.*

Exercise 30. *Let $a, b \in R$ such that $|a| \geq |b|$. Suppose $a = bq + r$ with $r \neq 0$. Show that if $d \in R$ satisfies $d \in GCD(a,b)$, then $d \in GCD(b,r)$ (Hint: Show that any divisor a, b must also be divsor or b, r and conversely. Hence if $d \in GCD(a,b)$ then $d \in GCD(b,r)$ and conversely).*

Theorem 4 (Euclidian Algorithm)**.** *Let $a \neq 0, b \in R$ where R is Euclidian domain with valuation $||$. Then there exists $d \in R$ such that $d \in GCD(a,b)$. Moreover, d is a linear combination of a and b. i.e., $d = xa + yb$ for some $x, y \in R$.*

Proof. Assume $a \neq 0$, $b \neq 0$ (see exercises above) Let $|a| \geq |b|$ and let $a = bq + r$. Assume $r \neq 0$ (see exercises above). Since $|r| < |b|$, using induction assume that there exists $x, y, d \in R$ such that $d \in GCD(b,r)$ and $d = xb + yr = xb + y(a - bq) = ya + (x = yq)b$. Now $d \in GCD(a,b)$ (see exercises above) and the theorem is proved. □

Exercise 31. *Show that if $d \in GCD(a,b)$ then $< a, b >=< d >$.*

Exercise 32. *In $\mathbf{Z}$ find $GCD(35,55)$ using Euclid's algorithm-. For each $d \in GCD(35,55)$ Find $x, y \in Z$ such that $d = 35x + 55y$.*

Exercise 33 (Modular Linear Equations)**.** *Let $R = \mathbf{Z_n}$. Let $a, b, n \in R$. Let $d \in GCD(a,n)$. Show that the equation $ax = b \mod n$ has a solution if and only if $d|b$. In paricular, $ax = 1 \mod n$ if and only if $GCD(a,n) = \{\pm 1\}$. Hence conclude that $a \in R^*$ if and only if $GCD(a,n) = \{\pm 1\}$.*

Exercise 34. *Use the previous exercise to show that for any positive integer n,* **$\mathbf{Z_n}$ is a field if and only if n is prime**.

Exercise 35. *Show that $\mathbf{Z_n}[x]$ is an integral domain if and only if n is prime.*

Definition 15 (**Euler's Tautient Function:**)**.** *For n positive intger, denote by $\phi(n)$ the number of elements in $\mathbf{Z_n^*}$. In particular if p is prime, $\phi(p) = p - 1$ (why?)*

Exercise 36. *Find $GCD(x^3 - 1, x^2 + x + 1)$ in $Q[x]$ using the Euclidian algorithm.*

Exercise 37. *Let G be a finite group. Let $a \in G$. Show that there is a positive integer k such that $a^k = 1$. Let k be the smallest such integer. Show that the set $\{a, a^2, a^3, ..., a^k\}$ is a subgroup of G. Use Lagrange's theorem to show that $k|n$. Hence conclude that $a^{|G|} = 1$*

Exercise 38 (**Euler and Fermat Theorems**)**.** *For n positive integer and $a \in Z$ such that $1 \in GCD(a,n)$ show that $a^{\phi(n)} = 1 \mod n$. This result is called* **Euler's theorem**. *In paricular, show that if p is prime and p does not divide a, then $a^{p-1} = 1 \mod p$ This result is called* **Fermat's little Theorem**.

Department of Computer Science and Engineering, NIT Calicut

Lecture 4: Factorization

Prepared by: K Murali Krishnan

Definition 16. *A non-zero, non-unit element a in an ring R is* **irreducible** *if whenever $a = bc$, either b or c must be a unit (and hence the other an associate of a).*

Definition 17. *A non-zero, non-unit element a in an ring R is* **prime** *if whenever $a|(bc)$ either $a|b$ or $a|c$.*

Note that elements in R^* are neither irreducible nor prime by definition.

Example 23. *In $Z_{12}[x]$ $(x-5)(x-7) = x^2 - 1 = (x-1)(x-11)$. Here all among $(x+5), (x+11), (x+7)$ and $(x+1)$ are irreducible as they cannot be split into non unit, non associate factors. However none among them is a prime (why?).*

The above example shows that an element $Z_{12}[x]$ can have multiple factorziation into irreducible elements and also a polynomial $(x^2 - 1)$ has more roots (here four) than his degree etc. Our objective in this lecture is to show that Euclidian domains are well behaved with respect to factorization into irreducibles.

In the rest of this lecture we assume R is a Euclidian domain with valuation $||$.

Exercise 39. *If $a \in R$ is prime, then a must be irreducible.*

Theorem 5. *$a \in R$ is irreducible if and only if a is prime.*

Proof. Let a be irreducible. Let $a|bc$. It is enough to show that either $a|b$ or $b|c$. Let $a \nmid b$. Hence $1 \in GCD(a, b)$ (why?). Thus, by the Euclidian algorithm there exists $x, y \in R$ such that $1 = ax + by$. Multiply by c to yield $c = acx + bcy$. Now a divides the LHS. Hence a must divide c. The converse follows from the previous exercise. □

We now show that every $a \in R$ can be written as a finite product of primes (equivalently irreducibles) essentially in a **unique** way (provided we treat associate elements equivalent). We first establish certain key properties of the Eucldian valuation before proving the Unique Factorizability Theorem.

Exercise 40. *Let I be any ideal in a Euclidian domain R. Show that $I =< d >$ for some $a \in R$ if and only if d is a non-zero element of smallest Euclidian valuation in R. Hence any two generators of the ideal must have the same Euclidian valuation.*

Exercise 41. *Let $a \simeq b$, then show that $|a| = |b|$.*

Lemma 3. *Let $a, b, c \in R$ be all non-zero. Let $a|bc$ then $|a| \leq |bc|$.*

Proof. Enough to show that $|a| \leq |ax|$ for any $x \in R$, $x \neq 0$. But since $ax \in < a >$, by the previous exercise, $|a| \leq |ax|$. □

Exercise 42. *Let $u \in R^*$, show that $|u| \leq |a|$ for all $a \in R$, $a \neq 0$. Moreover, show that if $u, w \in R^*$, $|u| = |w|$. Thus units have least Euclidian valuation among all non-zero elements in R.*

Lemma 4. *If a, b, c are non-zero non-unit elements in R with $a = bc$ then $|b| < |a|$ and $|c| < |b|$.*

Proof. By exercises above, $|b| \leq |a|$. Suppose $|b| = |a|$, then $< a >=< b >$ (why?). Hence a, b must be associates (why?) and $c \in R^*$, a contradiction. Similarly $|c| < |a|$. □

Corollary 2. *If $p|a$ for prime p and $a \neq 0$ then $|\frac{a}{p}| < |a|$.*

Theorem 6 (Factorizability)**.** *Every non-zero, non-unit $a \in R$ can be expressed as a finite product of (not necessarily distinct) primes (equivalently irreducibles).*

Proof. If a is irreducible, there is nothing to prove. Otherwise, let $a = bc$ with b, c non-unit, non-associates of a. By previous Lemma, $|b| < |a|$ and $|c| < |a|$. Inductively b,c have finite factorization into primes and the product of these factorizations yeild the required factorization of a. □

Example 24. *In Z, $6 = 3.2 = (-3)(-2)$. These are not "two different" prime factorizations because 2 and -2 are associates and so are 3 and -3. Similarly we can factorize $(x^2 - 1 = a(x+1).\frac{1}{a}(x-1)$ for any $a \in \mathbf{R} \setminus \{0\}$ in the Euclidian domain $\mathbf{R}[x]$. This shows that prime factorization need not be be unique in a Euclidian domain if we do not treat associates as equivalent.*

Theorem 7 (Unique Factorizability)**.** *Every non-zero, non-unit $a \in R$ has a unique factorization into a finite number of primes upto units and associates.*

Proof. Let k be the smallest number such that there is a non-zero, non-unit element $a \in R$ that has two factorizations with one of the factorizations containing k (not necessarily distinct) prime factors. Let $a = p_1 p_2 ... p_k = q_1 q_2 ... q_n$ be two prime factorizations of a with $n \geq k$. Since p_1 is prime and divides the RHS of the product, there must be some element in the product on the RHS (say q_1) which p_1 divides. Since q_1 is prime, p_1, q_1 must be associates. Let $q_1 = up_1$ for some $u \in R^*$. Cancelling p_1 we have $\frac{a}{p_1} = p_2 p_3 ... p_k = u q_2 q_3 .. q_n$. But this contradicts the minimality of k. □

An integral domain is called a **Unique Factorization Domain (UFD)** if every non-zero, non-unit element can be written uniquely (except for associates) as a product of irreducibles. The above theorem shows that Euclidian domains are UFDs.

Corollary 3 (Fundamental Theorem of Arithmetic)**.** **Z** *is a UFD.*

Exercise 43. *Show that $R[x]$ is a UFD if and only if R is an integral domain.*

Exercise 44. *Let $(R, +, .)$ be a UFD. show that for every $a, b \in R$, each $d \in GCD(a, b)$ is a product of irreducible common factors (not necessarily distinct) to both a and b*

Exercise 45 (Least Common Multiple (LCM))**.** *Let $(R, +, .)$ be a ring. Let $a, b \in R$. $d \in R$ is an $LCM(a, b)$ if $a|d$, $b|d$ and whenever $a|e$ and $b|e$ then $d|e$. Show that in a UFD, $d \in LCM(a, b)$ if and only if $d = ab/d'$ for some $d' \in GCD(a, b)$.*

Exercise 46. *Show that a PID must be a UFD.*

Exercise 47. *Show that an integral domain is a UFD if every non-zero, non-unit has a finite factorization into irreducibles and all irreducibles are primes. (Hint: The proof in the lecture required only that irreducibles are primes).*

The following exercises develop some group theoretic consequences of Euclidian algorithm. Here for any natural numbers a, b, $GCD(a, b)$ shall denote the positive GCD of a and b.

Definition 18. *Let group $(G, .)$ is* **cyclic** *if there is an $a \in G$ such that $G = \{a^i, i \in \mathbf{Z}\}$. Such an element a is called a* **generator** *for the group G. We use the notation $< a >$ to denote the fact that G is generated by a.*

Note: The same notation $< a >$ is used to denote the ideal generated by a in a ring and subgroup generated by a in a group.

Example 25. *$(\mathbf{Z}, +)$ is generated by 1. $(\mathbf{Z_n}, +)$ also has 1 as a generator.*

Example 26. *Let G be any group and $a \in G$. The set $\{a^i : i \in \mathbf{Z}\}$ is a cyclic subgroup called the* **cyclic subgroup generated by** *a. The size of the subgroup is called the* **order** *of a in G denoted by $o(a)$. Note that the order may be infinite.*

Example 27. *In $(\mathbf{Z_{10}}, +)$, $\{0, 2, 4, 6, 8\}$ is the cyclic subgroup generated by 2. In $\mathbf{Z}$, $\{0, \pm 2, \pm 4...\}$ is a cyclic subgroup generated by 2.*

Exercise 48. *If G is a finite group and $a \in G$, show that $o(a)$ is the least positive integer k such that $a^k = 1$ and $< a >= \{1, a, a^2, ..., a^k = 1\}$.*

For the rest of the lecture, assume G be a cyclic group n elements generated by a of order n. i.e., $G = \{a, a^2, a^3, ..., a^n = 1\}$ Let $b \in G$. Note that n must be a multiple of $o(b)$ by Lagrange's theorem (why?).

Exercise 49. *Let $a, b \in \mathbf{Z}^+$. Let $d = GCD(a, b)$. Show that $GCD(a/d, b/d) = 1$.*

Exercise 50. *Consider $b = a^i$, where $1 \leq i \leq n$. Let $t = n/GCD(n, i)$. Show that $a^t = 1$. Moreover, show that whenever $b^{t'} = 1$, $t|t'$. Thus $o(b) = t$.*

Exercise 51. *For each $d|n$, let $G_d = \{a^i : o(a^i) = d\}$. By the previous exercise, $|G_d| = |\{1 \leq i \leq n : n/(GCD(n, i) = d\}| = |\{1 \leq i \leq n : GCD(n, i) = n/d\}|$. Deduce that $|G_d| = |\{1 \leq j \leq d : GCD(d, j) = 1\}|$ (why?). Hence conclude that $|G_d| = \phi(d)$ (Definition 15).*

Exercise 52. *The above exercise show that there are exactly $\phi(d)$ elements of order d in a cyclic group of order n for each $d|n$. Hence conclude that $\sum_{d|n} \phi(d) = n$. Note that this formula is a number-theoretic result and does not depend on groups.*

The exercises above estabilish the following theorem:

Theorem 8 (Structure Theorem for Cyclic Groups)**.** *Let A cyclic group G of order n there are exactly $\phi(d)$ elements of order d for each $d|n$. Moreover, if $G =< a >$, then $o(a^i) = n/GCD(n, i)$.*

Corollary 4. *There are exactly $\phi(n)$ generators for a cyclic group of order n.*

Department of Computer Science and Engineering, NIT Calicut

Lecture 5: Finite Dimensional Vector Spaces

Prepared by: K Murali Krishnan

In this lecture we will develop some elementary theory about vector spaces. Let $V(F)$ be a vector space over field F.

Definition 19. *A Set of vectors S is* linearly dependent *if there are distinct vectors $v_1, v_2..., v_n$ in S and scalars $a_1, a_2, ..., a_n$ in F, not all zero satisfying $a_1v_1+a_2v_2+...+a_nv_n = 0$. We follow the convention that $\emptyset$ is linearly independent and $\{0\}$ linearly dependent.*

A set of vectors S is linearly dependent if S is not linearly independent. That is, whenever $a_1v_1 + a_2v_2 + ... + a_nv_{=}0$ for distinct $v_1, v_2..., v_n \in S$ then $a_1 = a_2 = ... = a_n = 0$.

Example 28. *The vectors $v_1 \begin{bmatrix}1\\1\end{bmatrix}$ and $v_2 \begin{bmatrix}2\\2\end{bmatrix}$ are linearly dependent in $\mathcal{R}^2$ as $2v_1 - v_2 = 0$. The vectors $e_1 = \begin{bmatrix}1\\0\end{bmatrix}$ and $e_2 = \begin{bmatrix}0\\1\end{bmatrix}$ are linearly independent. In general*

Example 29. *In general, the vectors $e_1 = [1, 0, ..., 0]^T$, $e_2 = [0, 1, 0, ..., 0]^T$ $e_n[0, 0, ..., 1]^T$ are linearly independent in $\mathcal{R}^n$. Moreover, $span(\{e_1, e_2, ..., e_n\}) = \mathcal{R}^n$.*

Example 30. *$\{1, x, x^2, ..., x^n...\}$ forms a linearly independent set in vector space $F[x]$ for any field F. The span of the set is the whole $F[x]$.*

Let $S = \{v_1, v_2, ..v_m\}$ be vectors in a vector space $V(F)$. Recall from Lecture 1 (last exercise) that $span(S) = \{a_1v_1 + a_2v_2 + ... + a_mv_m : a_1, a_2, ..a_m \in F\}$ is a subspace of V. $Span(S)$ is essentially the set of vectors expressible as finite linear combinations of vectors in S. The following lemma says that a set of vectors in linearly dependent if and only if one of the vectors is the span of the remaining.

Lemma 5. *A set of vectors $v_1, v_2, ..., v_n$ in a vector space $V(F)$ is linearly dependent if and only if for some $k \leq n$, $v_k \in span(v_1, v_2, ..v_{k-1})$.*

Proof. Let k be the smallest index such that $v_1, v_2, ..v_k$ are linearly dependent (why should such k exist?). Then, there exist $a_1, a_2, ..., a_k$ such that $a_1v_1+a_2v_2+...+a_kv_k = 0$. Moreover, $a_k \neq 0$ (why?). Hence $v_k = -(a_1/a_k)v_1 - (a_2/a_k)v_2 + ... - (a_{k-1}/a_k)v_{k-1}$. Converse is easy (why?). □

The next definition is very central to the study of vector spaces.

Definition 20. *A set S of vectors in $V(F)$ forms a* **basis** *for V if S is linearly independent and $span(S) = V$.*

Example 31. *It is easy to see that $v_1 = [x, y]^T$ and $v_2 = [x', y']^T$ forms a basis of $\mathcal{R}^2$ whenever they do not fall on a line passing through the origin.*

Lemma 6. *If $\{x_1, x_2, ..., x_n\}$ spans V and $\{y_1, y_2, .., y_m\}$ is a linearly independent set, the $m \leq n$. That is, the size of the largest independent set cannot exceed the size of the smallest spanning set for V (whenever there exists a finite set of vectors that span V).*

Proof. Since $y_m \in span\{x_1, x_2, ..., x_n\}$, the set $\{y_m, x_1, x_2, ..., x_n\}$ is linearly dependent. By previous lemma, there must be some x_i such that $x_i \in span\{y_m, x_1, x_2, .., x_{i-1}\}$. Hence we can eliminate x_i from the set and $\{y_m, x_1, x_2, .., x_{i-1}, x_{i+1}, ...x_n\}$ will be a spanning set. Now we add y_{m-1} to this set and remove another $x_{i'}$ from the resultant set and still get a spanning set. If we continue this process, $x_i s$ cannot be finished before all $y_j s$ are added for otherwise we will have $y_k, y_{k+1}, ..., y_m$ will be a spanning set for some $k > 1$ and this will be contradiction as then y_1 will be in the span of $y_k, y_{k+1}, ..., y_m$. Hence $n \geq m$. □

We are ready to prove the main theorem:

Theorem 9. *If V has a finite basis, then any two basis of V the same number of elements. This number is called the* **dimension** *of V. V is said to be a finite*

Proof. Let S and T be two (finite) basis for V. Since S is spanning and T linearly independent, we have $|S| \geq |T|$ by lemma above. Since T is spanning and S linearly independent, $|T| \geq |S|$. Hence $|S| = |T|$. □

Theorem 10. *Let $\{v_1, v_2, ..., v_n\}$ be a basis for a FDVS $V(F)$. Then for each $v \in V$, there exists unique $a_1, a_2, ..., a_n \in F$ such that $v = a_1 v_1 + a_2 v_2 + ... + a_n v_n$. $a_1, a_2, ..., a_n$ are called the* **coordinates of v with respect to basis** *$v_1, v_2, ..., v_n$.*

Proof. Clearly $a_1, a_2, ..., a_n$ must exist as $\{v_1, v_2, ..., v_n\}$ spans V. Suppose $v = a_1 v_1 + a_2 v_2 + ... + a_n v_n = b_1 v_1 + b_2 v_2 + ... + b_n v_n$, then $(a_1 - b_1)v_1 + (a_2 - b_2)v_2 + ... + (a_n - b_n)v_n = 0$. It follows from linear independence of $\{v_1, v_2, ..., v_n\}$ that $a_i = b_i$ for each i. □

To construct a basis for a FDVS $V(F)$, we can start with any vector v_1, pick v_2 outside $span(v_1)$, pick v_3 outside $span(v_1, v_2)$ and so forth. The process must terminate in finite number of steps as otherwise $v_1, v_2, ...v_n$ will be an infinite linearly independent set contradicting the finite dimensionality of V. (why?). Similarly, if W is a subspace of V, we can extend a basis of W to a basis of V exactly as above. (how?). Essentially we have proved the following:

Theorem 11. *Every finite dimensional vector space $V(F)$ has a basis. Moreover, basis for a subspace may be extended to a basis for V.*

The facts that every vector space has a basis and that any two basis have the same cardinality hold for arbitrary vector spaces - finite or infinite dimensional. The proofs will involve Zorn's Lemma.

Quotient Space

Recall from the previous chapter that if W is a subspace of a finite dimensional vector space $V(F)$ then the quotient space V/W itself is a vector space over F. We will now establish the relation between $dim(V)$, $dim(W)$ and $dim(V/W)$.

Theorem 12. *Let $V(F)$ be of dimension n. Let W be a subspace with $dim(W) = k$. Then $dim(V/W) = n - k$.*

Proof. Let $w_1, w_2, ..., w_k$ be a basis of W. extend the set with $v_1, v_2, .., v_{n-k}$ to a basis of V. Consider the cosets $v_1 + W, v_2 + W, ..., v_{n-k} + W$ in V/W. It is enough to show a basis of V/W. Note that W is the zero element in V/W.

Suppose $a_1(v_1 + W) + a_2(v_2 + W) + ... + a_n(v_n + W) = 0$ in V/W for $a_i \in F$ for all i. This means $a_1v_1 + a_2v_2 + ... + a_{n-k}v_{n-k} + W = 0$ in V/W. (why?). In turn this implies, $a_1v_1 + a_2v_2 + ... + a_{n-k}v_{n-k} \in W$ and consequently there must elements $b_1, b_2, ..., b_k$ in F such that $a_1v_1 + a_2v_2 + ... + a_{n-k}v_{n-k} = b_1w_1 + b_2w_2 + ... + b_kw_k$. Now linear independence of $\{w_1, .., w_k, v_1, .., v_{n-k}\}$ ensures that all a_i^s and b_j^s are zero showing linear independence of $v_1 + W, v_2 + W, ..., v_{n-k} + W$. It remains now that they span V/W.

Consider any element $v + W$ in V/W. If $v \in W$, then $v + W = W$ and there is nothing to prove (why?). Otherwise, let $v = a_1v_1 + a_2v_2 + ... + a_{n-k}v_{n-k} + b_1w_1 + b_2w_2 + ... + b_kw_k$ (why must such expression exist?). Let $b_1w_1 + b_2w_2 + ... + b_kw_k = w$. Clearly $w \in W$. Hence $v+W = (a_1v_1+a_2v_2+...+a_{n-k}v_{n-k}+w)+W = (a_1v_1+a_2v_2+...+a_{n-k}v_{n-k}+W)+(w+W) = (a_1v_1 + a_2v_2 + ... + a_{n-k}v_{n-k} + W) = a_1(v_1 + W) + a_2(v_2 + W) + ... + a_{n-k}(v_{n-k} + W)$. □

Exercise 53. *Let U, W be subspaces of a space $V(F)$. Define $U + W = \{u + w : u \in U, w \in W\}$. Show that $U + W$ is a subspace of V. This is called the* sum *of U and W. Show that $U \cap W$ is a subspace of V.*

Exercise 54. *Show that every $v \in U + W$ expressible as $v = u + w$ for unique $u \in U$ and $w \in W$ if and only if $U \cap W = \emptyset$. In this case, we way the sum of U and W is a* **direct sum** *and write $U \oplus W$.*

Exercise 55. *Let $dim(U) = p$ and $dim(W) = q$. Let $u_1, w_2, .., w_k$ be a basis for $U \cap W$. Let $u_1, u_2, .., u_{p-k}$ extend this to a basis of U and $w_1, w_2, ..., w_{q-k}$ extend this set to a basis of W. Show that all these vectors together is a basis of $U + W$. Hence conclude that $dim(U + W) = dim(U) + dim(W) - dim(U \cap W)$. In particular, $U + W$ is a direct sum of U and W, then $dim(U \oplus W) = dim(U) + dim(W)$.*

Exercise 56. *Let W be a subspace of a vector space $V(F)$. Let $w_1, w_2, .., w_k$ be a basis of W and let $w_{k+1}, w_{k+2}, ..., w_n$ extend this to a basis of V. Let $U = span(w_{k+1}, w_{k+2}, ..., w_n)$. Show that $V = W \oplus U$.*

Definition 21. *Let W is a subspace of $V(F)$. We way U is a complement of W in V if $V = U \oplus W$.*

Exercise 57. *In $\mathcal{R}^2$ find two different complements to the subspace defined by $x + y = 0$.*

Exercise 58. *Consider the vector space $V = \mathcal{R}^{\mathcal{R}}$ over $\mathcal{R}$ consisting of all real functions over $\mathcal{R}$. Let $W = \{f : f(-x) = f(x)\}$ and $U = \{f : f(-x) = -f(x)\}$ consist of all even and odd functions. Show that $V = W \oplus U$.*

Department of Computer Science and Engineering, NIT Calicut

Lecture 6: Homomorphisms

Prepared by: K Murali Krishnan

A homomorphism is a map between two similar algebraic structures that preserve the structure. Two such structures can be identified (that is considered to be the same) there is an isomorphism between them. Rings will remain commutative unless stated otherwise.

Definition 22. *A map f between two groups $(G, .)$ and $(G', .)$ is a group homomorphism if for all $a, b \in G$, $f(ab) = f(a)f(b)$. Similarly a map g between two rings $(R, +, .)$ and $(R', +, .)$ is a ring homomorphism if $g(1) = 1, g(a + b) = g(a) + g(b)$ and $g(ab) = g(a)g(b)$ for all a, b in R. A map h from a vector space $V(F)$ to another $V'(F)$ (the field must be the same) is a homomorphism (or a* **linear transformation***) if $h(v + v') = h(v) + h(v')$ and $h(av) = ah(v)$ for all $v, v' \in V$ and $a \in F$. A bijective homomorphism is called an* **isomorphism**.

A isomorphism between two structures indicate that the two are identical except for a re-naming of elements (via the map).

Definition 23. *Let f be a homomorphism between two groups G and G'. The image of the map in G' is $f(G)$ is sometimes denoted by $img(f)$. The* **kernel** *of the map denoted by $ker(f)$ is the collection of elements in G that gets mapped to the identity element in G'. These definitions extend to rings and vector spaces with identify referring to the identify 0 of the respective additive group.*

Example 32. *The map from $\mathcal{R}^3$ to $\mathcal{R}$ defined by $f(x, y, z) = x+y+z$ is a linear transformation. The map from $\mathcal{R}^2$ to itself which rotates each vector by θ degrees is a homomorphism. The action of the map on the point $\begin{bmatrix} x \\ y \end{bmatrix}$ is left multiplication by the matrix $\begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix}$*

Exercise 59. *Find the kernel and image of the maps above. (The answer will depend on the value of θ.)*

Example 33. *The map from $\mathcal{Z}$ to$\mathcal{Z}_n$ sending number k to $k(\mod n)$ is a ring homomorphism (why?). What is the kernel and image?*

Exercise 60. *Let F be any field and let $\alpha \in F$. The map Φ from $F[x]$ to F defined by $\Phi(f) = f(\alpha)$ is a ring homomorphism and is called the "evaluation map at α". This map is a vector space homomorphism as well (prove). If $F = \mathcal{R}$ and $\alpha = 1$, what is the kernel and image? What if $\alpha = 0$? What if $\alpha = \pi$? (Hint: For the last part, you need to know the fact that there is no polynomial with real (in fact even complex) coefficients which has π as a root).*

Exercise 61. *Let G, H be cyclic groups of order n generated by a and b respectively. Show that the map $f : G \longrightarrow H$ defined by $f(a) = b$ is a group isomorphism. Hence there is only one cyclic group of order n upto isomorphism.*

Example 34. *The map from the group of positive reals, $(\mathcal{R}+,.)$ to $(\mathcal{R},+)$ sending x to $\log x$ (to any base) is a group homomorphism. In fact, this is an isomorphism and allows us to uniquely retrieve a positive real number from its logarithm. Note that the homomorphism property precisely ensures that addition of logarithms suffices to do multiplication on positive reals. Find the kernel and image of the map.*

Exercise 62. *Show that the kernel and image of a homomorphism between two groups (rings or vector spaces) must be a subgroups (subrings or subspaces) of the respective spaces.*

Exercise 63. *Let f be a homomorphism from group G to G'. Show that $ker(f)$ is a normal subgroup. If f is a homomorphism from a ring R to R', show that $ker(f)$ is an ideal.*

The exercise gives hints about the connection between homomorphism and normal subgroups/ideals.

Exercise 64. *Show that a homomorphism is injective if and only if $ker(f) = \{0\}$ (or identity element for group homomorphisms). This is important as proving injectivity at zero suffices to prove injectivity of the map.*

Exercise 65. *Let f be a ring homomorphism from a field F to a ring R. Show that either $ker(f) = 0$ in which case the map is injective or $ker(f) = F$ making the map trivial (zero map).*

Homomorphism Theorems

In this section we will prove the fundamental homomorphism theorem for groups. The result will be extended to ring and vector space homomorphism through exercises. The theorem show that the image of a homomorphism is isomorphic to the quotient group (ring or space) defined by the kernel.

In the following theorem, let f be an *surjective* homomorphism from a group G to G'. (If f is not surjective, take G' to be $img(f)$.). Let $H = ker(f)$. We have seen that G' is a subgroup and H is normal.

Theorem 13. *G' and G/H are isomorphic.*

Proof. First note that f maps every element in the coset aH gets to the same element $f(a)$. (why?). This allows us to define the map $\Phi : G/H \longrightarrow G'$ as $\Phi(aH) = f(a)$. To prove the theorem, it suffices to show that Φ is an isomorphism. Clearly $\Phi(abH) = f(ab) = f(a)f(b) = \Phi(aH).\Phi(bH)$. This shows that Φ is structure preserving. Suppose $\Phi(aH) = 1$. Then $f(aH) = 1$ or $aH = H$. This proves injectivity (why?). Finally, since f is surjective, for any $y \in G'$, $y = f(a)$ for some $a \in G$. Hence $\Phi(aH) = y$ and this proves surjectivity. □

The following exercises develop the corresponding isomorphism theorems for rings and vector spaces.

Exercise 66. *Let f be an surjective homomorphism between rings R and R'. Let $ker(f) = I$. We have seen I is an ideal in R. Define the map $\Phi : R/I \longrightarrow R'$ as $\Phi(a + I) = f(a)$ for each $a \in R$. The map is well defined (why?). Show that $\Phi((a+I)(b+I)) = \Phi(a+I)\Phi(b+I)$. Show that Φ is an isomorphism between R/I and R'.*

Exercise 67. *Let T be a surjective linear transformation between vector spaces $V(F)$ and $V'(F)$. Let $W = ker(T)$. Define the map $\Phi : V/W \longrightarrow V'$ as $\Phi(u + W) = T(u)$ for each $u \in V$. Show that Φ is an isomorphism between spaces V/W to V'.*

Exercise 68. *Let T be a bijective linear transformation (isomorphism) between vector spaces $V(F)$ and $W(F)$. Let $b_1, b_2, ..., b_n$ be a basis of V. Show that $T(b_1), T(b_2), ..., T(b_n)$ is a basis of W. In particular, $dim(V) = dim(W)$.*

Let T be a linear transformation from vector space $V(F)$ to $W(F)$. define $Rank(T)$ to be $dim(Img(T))$ and $Nullity(T)$ to be $dim(ker(T))$. In view of the two previous exercises, $dim(V/ker(T)) = dim(V) - Nullity(T) = dim(Img(T)) = Rank(T)$ or We have thus the following **Rank-Nullity Theorem**:

Theorem 14. *$Rank(T) + Nullity(T) = dim(V)$ for any linear transformation T.*

Exercise 69. *Let α be a real number. Consider the map Φ_α defined from $\mathcal{R}[x]$ to $\mathcal{R}$ defined by $\Phi_\alpha(f) = f(\alpha)$. For various values of α, what can you say about $\ker(\Phi_\alpha)$ and $img(\Phi_\alpha)$? What can you say about $Rank(\Phi_\alpha)$ and $Nullity(\Phi_\alpha)$ for various values of Φ?*

Exercise 70. *Let $b_1, b_2, .., b_n$ be a basis for $V(F)$. Suppose T is a linear map from V to $W(F)$ of dimension m.. Show that for each choice of (not necessarily distinct vectors) $w_1, w_2, ..., w_n$ in W and setting $T(b_1) = w_1, T(b_2) = w_2, ..., T(b_n) = w_n$ we get a distinct linear transformation from V to W. Show that each linear transformation from V to W corresponds to a unique assignment of values for $T(b_1), t(b_2), ..., T(b_n)$ in W. This result is often stated as "fixing the image of the basis fixes the linear map".*

Exercise 71. *Let $V(F)$ be a vector space of dimension. Let $e_1 = [1, 0, .., 0]^T$, $e_2 = [0, 1, ..., 0]^T$, $e_n = [0, 0, ..., 1]^T$ be the standard basis of the vector space F^n. Let $b_1, b_2, .., b_n$ be any basis for $V(F)$. Define the map $T(b_1) = e_1$, $T(b_2) = e_2$,...,$T(b_n) = e_n$. Show that T is an isomorphism. It follows that every vector space of dimension n over F is isomorphic to F^n.*

A linear transformation from a space $V(F)$ to itself is called a projection if $P^2 = P$. That is, $P(P(v)) = P(v)$ for each $v \in V$.

Exercise 72. *If P is a projection, show that $I - P$ defined by $(I - P)(v) = v - P(v)$ for all $v \in V$ is a projection.*

Exercise 73. *If P is a projection, show that $V = ker(P) \oplus Img(P)$.*

Exercise 74. *If $V = U \oplus W$. Then, for each vector $v \in V$ can be written uniquely as $u + w$ with $u \in U$ and $w \in W$. Show that the map $P(u + w) = u$ is a projection. Show that the map $P'(u + w) = w$ is also a projection and satisfies $P' = I - P$.*

Exercise 75. *For what values of t can we say that $\mathcal{R}^2$ is a direct sum of points on the line $x + y = 0$ and $x - ty = 0$? Define the corresponding projection maps.*

Department of Computer Science and Engineering, NIT Calicut

Lecture 7: Finite Fields

Prepared by: K Murali Krishnan

Recall from Exercise 34 than Z_p is a field (precisely) for prime p and thus forms example for finite fields. In this lecture we ask the question what other finite fields are possible. In what follows, $(R, +, .)$ will be a commutative with unity.

Definition 24. *Let $(R, +, .)$ be a commutative ring with unity. The* **characteristic** *of R (denoted by $ch(R)$) is defined as the least positive integer n such that $(1+1+..ntimes..+1) = 0$ in R when such number exists. $ch(R)$ is defined to be 0 otherwise.*

Exercise 76. *The characteristic of $\mathbf{Q}, \mathbf{R}$ are zero. The characteristic of $\mathbf{Z_n}$ is n.*

Exercise 77. *Let $(R, +, .)$ be a (commutative) ring (with unity). Show that there is a unique homomorphism from Z to R. (Hint: $1 \in \mathbf{Z}$ maps to 1 in R.) Denote by $img(\mathbf{Z})$ the image of $\mathbf{Z}$ under the unique map. $img(\mathbf{Z})$ is a subring of R and must be isomorphic to either $\mathbf{Z}$ itself or $\mathbf{Z_n}$ for some $n \in \mathbf{N}$. In the former case, show that $ch(R) = 0$ and in the later case $ch(R) = n$. We may assume that R contains a "copy" of either $\mathbf{Z_n}$ or $\mathbf{Z}$ (viz. $Img(\mathbf{Z})$) within. This ring is called the* base ring *of R denoted by $base(R)$.*

Now we turn our attention to finite fields. Note that the simplest finite fields are $\mathbf{Z_p}$ for prime p.

Exercise 78. *Let R be a finite field. Then $base(R) = Z_p$ for some prime p. Thus $ch(R)$ must be prime.*

Definition 25. *Let F, E be fields such that $F \subseteq E$. We say E is an* **extension field** *of F and F a* **subfield** *of E.*

Corollary 5. *Every finite field is an extension field of Z_p for some prime p.*

Exercise 79. *Show that E is an extension field of F, then $E(F)$ is a vector space. $dim(E)$ as an F vector space is called the* **degree of the extension** *(field E over F).*

Exercise 80. *Let F be a finite field. Show that F must be a finite extension of some $\mathbf{Z_p}$. Use Exercise 71 to conclude that every finite field must have p^n elements for some prime p and positive integer n.*

To understand finite fields better, we need to develop properties of polynomials. In the following, F will be assumed to be an arbitrary field. Recall $F[x]$ is a Euclidian domain (and hence a UFD). Note that $(x - \alpha)$ is a prime (irreducible polynomial) for each $\alpha \in F$. The following is a central theorem about the complex field whose proof is beyond the scope of these lectures.

Theorem 15 (Fundamental Theorem of Algebra)**.** *Prime polynomials in $\mathbf{C}[x]$ are precisely polynomials of the form $(x - \alpha)$ for each alpha $\in \mathbf{C}$.*

Corollary 6. *Every $f(x) \in \mathbf{C}[x]$ factorizes (uniquely) into the form $(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ where $\alpha_1, ..., \alpha_n \in \mathbf{C}$, not necessarily distinct.*

Definition 26. *Let F be a field and $f(x) \in F[x]$. $\alpha \in F$ is called a root of $f(x)$ if $f(\alpha) = 0$.*

Lemma 7 (Remainder Theorem)**.** *The reminder of dividing $f(x) \in F[x]$ with $(x-\alpha)$ for any $\alpha \in F$ is $f(\alpha)$, the evaluation of f at α.*

Proof. Let $f(x) = q(x)(x-\alpha) + r$ by Euclidian algorithm, with $r \in F$. evaluating the LHS and RHS at $x = \alpha$ yields the desired result. □

Corollary 7 (Factor thereom)**.** *α is a root of $f(x)$ if and only if $(x-\alpha)|f(\alpha) = 0$*

Exercise 81. *Show that if $\alpha_1 \neq \alpha_2$, then $GCD(x-\alpha_1), (x-\alpha_2)) = 1$ in $F[x]$ for $\alpha_1, \alpha_2 \in F$.*

Exercise 82. *If $\alpha_1, \alpha_2....\alpha_n$ are roots of $f(x)$, then show that $(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)|f(x)$. Hence conclude that a if $f(x)$ has degree n then $f(x)$ has at most n roots in F.*

Note that the result in the above exercise may fail to hold if F is not a field. For instance in $Z_{12}[x]$, $x^2 - 1$ has four roots, $\{1, 5, 7, 11\}$.

We shall now prove the fact that if F is a finite field, then $F^* = F \setminus 0$ is a cyclic group.

Theorem 16 (Gauss Theorem)**.** *If F is a finite field, then F^* is cyclic.*

Proof. Let F be a finite field of field of p^n elements. Let $m = |F^*| = p^n - 1$. Let $d|m$. Suppose $a \in F^*$ has $o(a) = d$. By Corollary 4, there are exactly $\phi(d)$ elements of order d in the set $< a >= \{a, a^2, a^3, .., a^d\}$. Note that all d elements in $< a >$ satisfies the polynomial $x^d - 1$. Since a polynomial of degree d can have atmost d roots in F, no element in F other than those in $< a >$ satisfies this polynomial.

Suppose now $o(b) = d$ in F^*, then b must satisfy $x^d - 1 = 0$. Hence $b = a^i$ for some i. It follows that there are no more than $\phi(d)$ elements of order d in F^*. But by Exercise 52, $\sum_{d|m} \phi(d) = m$. Hence the number of elements of order d must be exactly $\phi(d)$ for each $d|m$ (why?). In particular, there must be $\phi(m) = \phi(p^n - 1)$ elements of order m and F^* must be cyclic. □

Department of Computer Science and Engineering, NIT Calicut

Lecture 8: Linear Transformations

Prepared by: K Murali Krishnan

Matrices

Let $V(F)$ have basis $b_1, b_2, ..., b_n$ and $W(F)$ have basis $c_1, c_2, ..., c_m$. Let T be a linear transformation from V to W. Let $T(b_1) = a_{11}c_1 + a_{12}c_2 + ... + a_{1m}c_m$. In dot product notation we write $T(b_1) = [c_1, c_2, ..., c_m][a_{11}, a_{12}, ..., a_{1m}]^T$. Similarly, let $T(b_2) = [c_1, c_2, ..., c_m][a_{21}, a_{22}, ..., a_{2m}]^T$,....., $T(b_n) = [c_1, c_2, ..., c_m][a_{n1}, a_{n2}, ..., a_{nm}]^T$.

Let $v = x_1, b_1 + x_2b_2 + ... + x_nb_n$. for some scalars $x_1, x_2, .., x_n$. By linearity of T,, $T(v) = x_1T(b_1) + x_2T(b_2) + ... + x_nT(b_n) = [T(b_1), T(b_2), ..., T(b_n)][x_1, x_2, ..., x_n]^T$ in dot product notation.

Noting that in dot product notation $T(b_i) = [c_1, c_2, ..., c_m][a_{i1}, a_{i2}, ..., a_{im}]^T$, we have in matrix notation:

$$\begin{bmatrix} T(b_1) & ... & T(b_n) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ .. \\ x_n \end{bmatrix} = \begin{bmatrix} c_1 & ... & c_m \end{bmatrix} \begin{bmatrix} a_{11} & a_{21} & ... & a_{n1} \\ a_{12} & a_{22} & ... & a_{n2} \\ .. & .. & ... & .. \\ a_{1m} & a_{2m} & ... & a_{nm} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ .. \\ x_n \end{bmatrix}.$$

Suppose $[y_1, y_2, ..., y_m]$ are the coordinates of $T(v)$ with respect to basis $c_1, c_2, ..., c_m$, then we have the relation:

$$\begin{bmatrix} y_1 \\ y_2 \\ .. \\ y_m \end{bmatrix} = \begin{bmatrix} a_{11} & a_{21} & ... & a_{n1} \\ a_{12} & a_{22} & ... & a_{n2} \\ .. & .. & ... & .. \\ a_{1m} & a_{2m} & ... & a_{nm} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ .. \\ x_n \end{bmatrix}.$$ Thus the matrix $A = \begin{bmatrix} a_{11} & a_{21} & ... & a_{n1} \\ a_{12} & a_{22} & ... & a_{n2} \\ .. & .. & ... & .. \\ a_{1m} & a_{2m} & ... & a_{nm} \end{bmatrix}$ is called the matrix of the linear transformation with respect to basis $b_1, b_2, ..., b_n$ and $c_1, c_2, .., c_m$. Conversely, it is easy to see that any $m \times n$ matrix will define a linear transformation for the basis of particular choice. Thus we see a correspondence between $m \times n$ matrices over the field F and linear transformations from V to W.

We have already seen that any n dimensional vector space over F is isomorphic to F^n. Hence, *once we fix a basis for V and W*, vectors from V correspond to elements in F^n, vectors in W correspond to elements in F^m and linear transformation from V to W correspond to $m \times n$ matrices over F. This correspondence draws matrices into the study of linear transformations.

In these lectures, we will be specific to the following special class of linear transformations.

Definition 27. *A* **(linear) operator** *on a vector space $V(F)$ is a linear transformation from V to itself.*

Once a(ny) basis for an n dimensional vector space V is fixed, each linear operator on V corresponds to a $n \times n$ square matrix. Thus, the set of operators on an n dimensional space V corresponds precisely to $M_n(F)$.

Exercise 83. *Let $b_1, b_2, ..., b_n$ be a basis for $V(F)$. Show that an operator T on V is bijective if and only if T is injective if and only if $T(b_1), T(b_2), ..., T(b_n)$ are linearly independent. Note that a linear transformation T is* **invertible** *if and only if T is bijective. Show that T^{-1} is also a linear operator from V to V. (why?).*

Let $b_1, b_2, ..., b_n$ be a basis of $V(F)$. We have already seen that the map $f : V \longrightarrow F^n$ defined by $f(b_1) = e_1, ..., f(b_n) = e_n$ is an isomorphism. With this identification, a vector $v = x_1b_1 + x_2b_2 + ... + x_nb_n$ may be identified with $[x_1, x_2, ..., x_n]^T \in F^n$ Now, let T be an operator in V. Then the matrix A of the map has coordinate vectors corresponding to $T(e_1), T(e_2), ...T(e_1)$ as columns (with our identification of e_i with b_i). In view of the above exercise, we see that T is invertible if and only if the columns of T are linearly independent. This in turn happens if and only if the space spanned by the columns of T is the whole of V (why?). This observation motivates the following definition:

Definition 28. *Let $A \in F^{n\times n}$ be an $n \times n$ matrix. $ColumnSpan(A)$ is defined as the subsace spanned by the columns of A. $RowSpan(A)$ is defined as the subspace spanned by the rows of A. The dimensions of the column and row space are called $RowRank(A)$ and $ColumnRank(A)$ of A.*

It follows from the previous discussion that an $n \times n$ matrix A over a field F is invertible if and only if $ColumnSpan(A) = F^n$. Since we A is invertible if and only if $det(A) \neq 0$, we have a correspondance between bijective linear operators and matrices in $GL_n(F)$.

Corollary 8. *$T : V \longrightarrow V$ is bijective (invertible) if and only if the matrix of T (with respect to any basis $b_1, b_2, .., b_n$) is non-singular.*

Basis Transformations

We study the effect of basis change on the coordinates of a vector. The matrix of an operator also changes when basis changes.

Let $B = b_1, b_2, ..., b_n$ and $C = c_1, c_2, ..., c_n$ be two basis for $V(F)$. Suppose we know the coordinates of vectors in S' wrt. those in S. i.e., let $c_1 = \alpha_{11}b_1 + \alpha_{12}b_2 + ... + \alpha_{1n}b_n$, $c_2 = \alpha_{21}b_1 + \alpha_{22}b_2 + ... + \alpha_{2n}b_n$,..., $c_n = \alpha_{n1}b_1 + \alpha_{n2}b_2 + ... + \alpha_{nn}b_n$. In matrix notation, $[c_1, c_2, ..., c_n] = [b_1, b_2, ..., b_n]Q$ where, $Q = \begin{bmatrix} \alpha_{11} & \alpha_{21} & ... & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & ... & \alpha_{n2} \\ .. & .. & ... & .. \\ \alpha_{1n} & \alpha_{2n} & ... & \alpha_{nn} \end{bmatrix}$

Since basis transformation is an isomorphism, Q must be invertible (why?). Thus we have $[b_1, b_2, .., b_n] = Q^{-1}[c_1, c_2, ..., c_n]$. Suppose now $v = x_1b_1 + x_2b_2 + ... + x_nb_n$ be a vector with coordinates $[x_1, x_2, ..., x_n]^T$ with respect to basis B. What will be the coordinates of v with respect to basis C? That is, we want to find out $[y_1, y_2, ..., y_n] \in F^n$ such that $v = [c_1, c_2, ..., c_n][y_1, y_2, ..., y_n]^T$. But $v = [b_1, b_2, ..., b_n][x_1, x_2, ..., x_n]^T = [c_1, c_2, ..., c_n]Q^{-1}[x_1, x_2, ..., x_n]^T$. Hence we have $[y_1, y_2, ..., y_n]^T = Q^{-1}[x_1, x_2, ..., x_n]^T$ giving the required relation between coordinate vectors. Q is called the matrix of basis change from B to C.

Example 35. *In $\mathcal{R}^2$, let v have coordinates $[1,1]^T$ w.r.t. the standard basis. To find its coordinates w.r.t. basis $c_1 = [1,1]^T$ and $c_2 = [1,0]^T$, we can see that $[c_1, c_2] = [e_1, e_2]Q$ where $Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. Thus the new coordinates will be $Q^{-1}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$.*

Now we take up the effect of basis change on the matrix of a linear operator on a FDVS. Let $B = \{b_1, b_2, ..., b_n\}$ and $C = \{c_1, c_2, ..., c_n\}$ be two basis for an FDVS $V(F)$. Let $[c_1, c_2, ..., c_n] = [b_1, b_2, ..., b_n]Q$. Let A be the matrix of a linear operator with respect to basis B. Let v be a vector in V whose coordinate vector w.r.t. basis B is $x = [x_1, x_2, .., x_n]^T$. It follows that the coordinates of v w.r.t. basis C will be $Q^{-1}x$.

Since A is the matrix of T w.r.t. basis B, coordinate vector of $T(v)$ w.r.t. basis B will be Ax. Hence the coordinate vector for $T(v)$ w.r.t. basis C will be $Q^{-1}Ax$.

Let A' be the matrix of T w.r.t. basis C. As v has coordinates $Q^{-1}x$ w.r.t. C and $T(v)$ has coordinates $Q^{-1}Ax$ w.r.t. C, action of A' on $Q^{-1}x$ must give $Q^{-1}Ax$. That is, we must have $A'Q^{-1}x = Q^{-1}Ax$. Hence we have $A'x = Q^{-1}AQx$. Since this must hold for all $x \in F^n$ as v was chosen arbitrary, we have $A' = Q^{-1}AQ$ as the matrix of T for the basis C.

Example 36. *T be the linear operator in $\mathcal{R}^2$ such that $T(\begin{bmatrix} 1 \\ 0 \end{bmatrix}) = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$ $T(\begin{bmatrix} 0 \\ 1 \end{bmatrix}) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ The matrix of T w.r.t. the standard basis is $\begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix}$. If we change the basis to $\{\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\}$ then the matrix of basis change $Q = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Hence the matrix of T w.r.t this basis will be $Q^{-1}AQ = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$*

Exercise 84. *Consider the operator T in $\mathcal{R}^3$ given by $T(e_1) = e_1$, $T(e_2) = e_1 + e_2$, $T(e_3) = e_1 + e_2 + e_3$. What is the matrix of this map w.r.t. the basis $b_1 = e_1 + e_2$, $b_2 = e_2 + e_3$ and $b_3 = e_1 + e_3$. (Hint, work with the relationship between the basis vectors directly instead of going for matrix manipulation and note that coordinate vectors of $T(b_1)$, $T(b_2)$ and $T(b_3)$ in the basis $\{b_1, b_2, b_3\}$ forms the columns of the matrix to be computed).*

Exercise 85. *Consider the set $F_n[x]$ consisting of all polynomials of degree less than n over a field F. Let $\alpha_1, \alpha_2, ..., \alpha_n$ be elements in F. Consider the map $T(p(x)) = p(\alpha_1) + p(\alpha_2)x + ..., +p(\alpha_n)x^n$ in $F_n[x]$. What is the matrix of the map with respect to the basis $\{1, x, x^2, ..., x^n\}$? This matrix is called a Vandermone's matrix. Find the expression for the determinant of the matrix and show that the map is invertible if and only if $\alpha_1, \alpha_2, ..., \alpha_n$ are distinct elements in F. This means that interpolation of a degree $n-1$ polynomial is possible only if evaluation at n distinct points are given. Moreover interpolation problem reduces to matrix inversion.*

References