KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University Established Under Section 3 of UGC Act 1956)

Coimbatore – 641 021.

		Semester – I			
18MMP101	**ALGEBRA**	**L**	**T**	**P**	**C**
		4	**0**	**0**	**4**

Course Objectives

To learn the basic central ideas of linear algebra such as linear transformations, Eigen values, Eigen vectors, and, canonical forms.

Course Outcomes

After successful completion of this course the students will be able to:

- Understand the concept and the properties of finite abelian groups.
- Get pre-doctoral level knowledge in ring theory.
- Attain good knowledge in field theory.
- Define and study in details the properties of linear transformations.
- Analyze the concept of trace and transpose.

UNIT I

Another counting principle – application of theorems – Cauchy theorem – Sylow's theorem – Direct product – Finite Abelian groups.

UNIT II

Ring Theory- Basic definition- More ideals and quotient rings- Euclidean rings-A Particular Euclidean Rings –Polynomial Rings-Polynomial over the Rational Field.

UNIT III

Fields – Extension Fields-Finite Extension of F – Some basic Definitions and Theorem – Roots of a Polynomial – More about Roots – The elements of Galois Theory.

UNIT IV

Linear Transformations-The Algebra of Linear Transformation – Characteristic Root-Matrices-Canonical Forms –Triangular form-Nilpotent Transformations–Jordan form.

UNIT V

Trace and Transpose – Trace of T-Symmetric Matrix –Determinants–Hermitian Transformation, Unitary Transformation and Normal Transformation – Real quadratic forms.

SUGGESTED READINGS

TEXT BOOK

1. Herstein.I. N.,(2010). Topics in Algebra, Second edition, Wiley and sons Pvt Ltd, Singapore.

REFERENCES

1. Artin. M., (2009). Algebra, Pearson Prentice-Hall of India, New Delhi.
2. Fraleigh. J. B., (2008). A First Course in Abstract Algebra , Seventh edition , Pearson Education Ltd, New Delhi.
3. Kenneth Hoffman., Ray Kunze., (2003). Linear Algebra, Second edition, Prentice Hall of India Pvt Ltd, New Delhi.
4. Vashista.A.R., (2005). Modern Algebra, Krishna Prakashan Media Pvt Ltd, Meerut.

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)

(Established Under Section 3 of UGC Act 1956)

Coimbatore – 641 021.

LESSON PLAN
DEPARTMENT OF MATHEMATICS

Name of the faculty : Y.Sangeetha

Class : I M.Sc Mathematics

Subject : Algebra

Subject Code : 18MMP101

S. No	Lecture Duration Hour	Topics To Be Covered	Support Materials
		UNIT-I	
1	1	Another counting principle-Lemma and theorems	T1: chap-2 Pg.No:83-88
2	1	Definition and theorems for Conjugacy Relation	T1: chap-2 Pg.No:83-88
3	1	Cauchy's theorem	T1: chap-2 Pg.No:88-89
4	1	Sylow's theorem	R2: chap-7 Pg.No:321-326
5	1	Second proof of Sylow's theorem.	R2: chap-7 Pg.No:321-326
6	1	Third proof of Sylow's theorem	R2: chap-7 Pg.No:321-326
7	1	Corollary for Sylow's theorem.	R2: chap-7 Pg.No:327-332
8	1	Definition and theorems for Direct Product	T1: chap-2 Pg.No:104-107
9	1	Finite abelian group-theorem	T1: chap-2 Pg.No:109-114
10	1	Recapitulation and Discussion of possible questions	
Total No of Hours Planned For Unit I - 10 Hours			
		UNIT-II	
1	1	Ring Theory-Basic Definition and Examples	R2: chap-4 Pg.No:168-174
2	1	Theorems based on properties of ring	R2: chap-4 Pg.No:168-174
3	1	Ideal And Quotient Ring- Definition and	R4: chap-4 Pg.No:306-

		theorems	319
4	1	The Field of Quotient of an Integral Domain theorems	R4: chap-4 Pg.No:321-322
5	1	Euclidean Ring-Definition and theorems	T1: chap-2 Pg.No:143-149
6	1	Continuation of theorems for Euclidean ring	T1: chap-2 Pg.No:150-152
7	1	Polynomial Ring-Definition and Lemma	T1: chap-2 Pg.No:153-157
8	1	Theorems for Polynomial ring	T1: chap-2 Pg.No:153-157
9	1	Theorems for Polynomial ring	T1: chap-2 Pg.No:159-161
10	1	Recapitulation and Discussion of possible questions	
Total No of Hours Planned For Unit II - 10 Hours			
UNIT-III			
1	1	Field and Extension Field-Definition And theorem	R1: chap-13 Pg.No: 492-496
2	1	Continuation of theorem for Extension field	R1: chap-13 Pg.No: 492-496
3	1	Some Basic Definition and Examples For Extension Field	T1: chap-5 Pg.No: 212-214
4	1	Roots of Polynomial-Definition and theorems.	T1: chap-5 Pg.No: 219-226
5	1	More about Roots-Definition and Lemma and theorems	T1: chap-5 Pg.No: 232-236
6	1	The Elements of Galois theory-Definition and Lemma.	R1: chap-14 Pg.No: 537-543
7	1	Theorems on Elements of Galois Theory	R1: chap-14 Pg.No: 537-543
8	1	Continuation Of Theorems For Galois Theory	R1: chap-14 Pg.No: 537-543
9	1	Recapitulation and Discussion of possible questions	
Total No of Hours Planned For Unit III - 9 Hours			
UNIT-IV			
1	1	Linear Transformation-Definition and Lemma.	T1: chap-6 Pg.No: 262-263
2	1	Theorems on Linear Transformation.	T1: chap-6 Pg.No: 263-267
3	1	Characteristic Roots-theorems.	T1: chap-6 Pg.No: 270-272
4	1	Continuation of theorems for Characteristic roots	T1: chap-6 Pg.No: 272-275
5	1	Theorems for Triangular Form	T1: chap-6 Pg.No: 285-

			290
6	1	Theorems for Nilpotent Form	T1: chap-6 Pg.No: 292-298
7	1	Theorems for Jordon Form	R3: chap-7 Pg.No: 482-515
8	1	Recapitulation and Discussion of possible questions	
Total No of Hours Planned For Unit IV - 8 Hours			
UNIT-V			
1	1	Trace and Transpose-Definition and Concept	T1: chap-6 Pg.No: 313-319
2	1	Determinants	R3: chap-4 Pg.No: 209-238
3	1	Theorems for Determinants	R3: chap-4 Pg.No: 209-238
4	1	Unitary Transformation-Theorems	T1: chap-6 Pg.No: 337-341
5	1	Hermitian Transformation-Theorems	T1: chap-6 Pg.No: 341-342
6	1	Normal Transformation-Theorems	T1: chap-6 Pg.No: 342-348
7	1	Real Quadratic Form-Theorems	T1: chap-6 Pg.No: 350-354
8	1	Recapitulation and Discussion of possible questions	
9	1	Discussion on Previous ESE Question Papers	
10	1	Discussion on Previous ESE Question Papers	
11	1	Discussion on Previous ESE Question Papers	
Total No of Hours Planned For Unit V - 11 Hours			

SUGGESTED READINGS

TEXT BOOK

1. Herstein.I. N.,(2010). Topics in Algebra, Second edition, Wiley and sons Pvt Ltd, Singapore.

REFERENCES

1. Artin. M., (2008). Algebra, Prentice-Hall of India, New Delhi.
2. Fraleigh. J. B., (2004). A First Course in Abstract Algebra , Seventh edition , Pearson Education Ltd, Singapore.
3. Kenneth Hoffman., Ray Kunze., (2003). Linear Algebra, Second edition, Prentice Hall of India Pvt Ltd, New Delhi.
4. Vashista.A.R., (2005). Modern Algebra, Krishna Prakashan Media Pvt Ltd, Meerut.

UNIT-I

Another counting principle – application of theorems – Cauchy theorem – Sylow's theorem – Direct products – Finite Abelian groups.

Another Counting Principle

DEFINITION If $a, b \in G$, then b is said to be a *conjugate* of a in G if there exists an element $c \in G$ such that $b = c^{-1}ac$.

We shall write, for this, $a \sim b$ and shall refer to this relation as *conjugacy*.

LEMMA

Conjugacy is an equivalence relation on G.

Proof. As usual, in order to establish this, we must prove that

1. $a \sim a$;
2. $a \sim b$ implies that $b \sim a$;
3. $a \sim b$, $b \sim c$ implies that $a \sim c$

for all a, b, c in G.

We prove each of these in turn.

1. Since $a = e^{-1}ae$, $a \sim a$, with $c = e$ serving as the c in the definition of conjugacy.
2. If $a \sim b$, then $b = x^{-1}ax$ for some $x \in G$, hence, $a = (x^{-1})^{-1}b(x^{-1})$, and since $y = x^{-1} \in G$ and $a = y^{-1}by$, $b \sim a$ follows.
3. Suppose that $a \sim b$ and $b \sim c$ where $a, b, c \in G$. Then $b = x^{-1}ax$, $c = y^{-1}by$ for some $x, y \in G$. Substituting for b in the expression for c we obtain $c = y^{-1}(x^{-1}ax)y = (xy)^{-1}a(xy)$; since $xy \in G$, $a \sim c$ is a consequence.

For $a \in G$ let $C(a) = \{x \in G \mid a \sim x\}$. $C(a)$, the equivalence class of a in G under our relation, is usually called the *conjugate class* of a in G; it consists of the set of all distinct elements of the form $y^{-1}ay$ as y ranges over G.

DEFINITION If $a \in G$, then $N(a)$, the *normalizer of a in G*, is the set $N(a) = \{x \in G \mid xa = ax\}$.

$N(a)$ consists of precisely those elements in G which commute with a.

LEMMA

$N(a)$ is a subgroup of G.

Proof. In this result the order of G, whether it be finite or infinite, is of no relevance, and so we put no restrictions on the order of G.

Suppose that $x, y \in N(a)$. Thus $xa = ax$ and $ya = ay$. Therefore, $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$, in consequence of which $xy \in N(a)$. From $ax = xa$ it follows that $x^{-1}a = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = ax^{-1}$, so that x^{-1} is also in $N(a)$. But then $N(a)$ has been demonstrated to be a subgroup of G.

THEOREM

If G is a finite group, then $c_a = o(G)/o(N(a))$; in other words, the number of elements conjugate to a in G is the index of the normalizer of a in G.

Proof. To begin with, the conjugate class of a in G, $C(a)$, consists exactly of all the elements $x^{-1}ax$ as x ranges over G. c_a measures the number of distinct $x^{-1}ax$'s. Our method of proof will be to show that two elements in the same right coset of $N(a)$ in G yield the same conjugate of a whereas two elements in different right cosets of $N(a)$ in G give rise to different conjugates of a. In this way we shall have a one-to-one correspondence between conjugates of a and right cosets of $N(a)$.

Suppose that $x, y \in G$ are in the same right coset of $N(a)$ in G. Thus $y = nx$, where $n \in N(a)$, and so $na = an$. Therefore, since $y^{-1} = (nx)^{-1} = x^{-1}n^{-1}$, $y^{-1}ay = x^{-1}n^{-1}anx = x^{-1}n^{-1}nax = x^{-1}ax$, whence x and y result in the same conjugate of a.

If, on the other hand, x and y are in different right cosets of $N(a)$ in G we claim that $x^{-1}ax \neq y^{-1}ay$. Were this not the case, from $x^{-1}ax = y^{-1}ay$ we would deduce that $yx^{-1}a = ayx^{-1}$; this in turn would imply that $yx^{-1} \in N(a)$. However, this declares x and y to be in the same right coset of $N(a)$ in G, contradicting the fact that they are in different cosets. The proof is now complete.

COROLLARY

$$o(G) = \sum \frac{o(G)}{o(N(a))}$$

where this sum runs over one element a in each conjugate class.

THEOREM

If $o(G) = p^n$ where p is a prime number, then $Z(G) \neq (e)$.

Proof. If $a \in G$, since $N(a)$ is a subgroup of G, $o(N(a))$, being a divisor of $o(G) = p^n$, must be of the form $o(N(a)) = p^{n_a}$; $a \in Z(G)$ if and only if $n_a = n$. Write out the class equation for this G, letting $z = o(Z(G))$. We get $p^n = o(G) = \sum(p^n/p^{n_a})$; however, since there are exactly z elements such that $n_a = n$, we find that

$$p^n = z + \sum_{n_a < n} \frac{p^n}{p^{n_a}}.$$

Now look at this! p is a divisor of the left-hand side; since $n_a < n$ for each term in the $\sum$ of the right side,

$$p \left| \frac{p^n}{p^{n_a}} = p^{n-n_a} \right.$$

so that p is a divisor of each term of this sum, hence a divisor of this sum. Therefore,

$$p \left| \left(p^n - \sum_{n_a < n} \frac{p^n}{p^{n_a}} \right) = z. \right.$$

Since $e \in Z(G)$, $z \neq 0$; thus z is a positive integer divisible by the prime p. Therefore, $z > 1$! But then there must be an element, besides e, in $Z(G)$! This is the contention of the theorem.

COROLLARY

If $o(G) = p^2$ where p is a prime number, then G is abelian.

Proof. Our aim is to show that $Z(G) = G$. At any rate, we already know that $Z(G) \neq (e)$ is a subgroup of G so that $o(Z(G)) = p$ or p^2. If $o(Z(G)) = p^2$, then $Z(G) = G$ and we are done. Suppose that $o(Z(G)) = p$; let $a \in G$, $a \notin Z(G)$. Thus $N(a)$ is a subgroup of G, $Z(G) \subset N(a)$, $a \in N(a)$, so that $o(N(a)) > p$, yet by Lagrange's theorem $o(N(a)) \mid o(G) = p^2$. The only way out is for $o(N(a)) = p^2$, implying that $a \in Z(G)$, a contradiction. Thus $o(Z(G)) = p$ is not an actual possibility.

THEOREM

(CAUCHY) *If p is a prime number and $p \mid o(G)$, then G has an element of order p.*

Proof. We seek an element $a \neq e \in G$ satisfying $a^p = e$. To prove its existence we proceed by induction on $o(G)$; that is, we assume the theorem to be true for all groups T such that $o(T) < o(G)$. We need not worry about starting the induction for the result is vacuously true for groups of order 1.

If for any subgroup W of G, $W \neq G$, were it to happen that $p \mid o(W)$, then by our induction hypothesis there would exist an element of order p in W, and thus there would be such an element in G. Thus we may assume that p is not a divisor of the order of any proper subgroup of G. In particular, if $a \notin Z(G)$, since $N(a) \neq G$, $p \nmid o(N(a))$. Let us write down the class equation:

$$o(G) = o(Z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}.$$

Since $p \mid o(G)$, $p \nmid o(N(a))$ we have that

$$p \left| \frac{o(G)}{o(N(a))}, \right.$$

and so

$$p \left| \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}; \right.$$

since we also have that $p \mid o(G)$, we conclude that

$$p \left| \left(o(G) - \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))} \right) = o(Z(G)). \right.$$

$Z(G)$ is thus a subgroup of G whose order is divisible by p. But, after all, we have assumed that p is not a divisor of the order of any proper subgroup of G, so that $Z(G)$ cannot be a proper subgroup of G. We are forced to accept the only possibility left us, namely, that $Z(G) = G$. But then G is abelian; now we invoke the result already established for abelian groups to complete the induction. This proves the theorem.

Sylow's Theorem

THEOREM

(SYLOW) *If p is a prime number and $p^\alpha \mid o(G)$, then G has a subgroup of order p^α.*

Before entering the first proof of the theorem we digress slightly to a brief number-theoretic and combinatorial discussion.

The number of ways of picking a subset of k elements from a set of n elements can easily be shown to be

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

If $n = p^\alpha m$ where p is a prime number, and if $p^r \mid m$ but $p^{r+1} \nmid m$, consider

$$\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!}$$

$$= \frac{p^\alpha m(p^\alpha m - 1)\cdots(p^\alpha m - i)\cdots(p^\alpha m - p^\alpha + 1)}{p^\alpha(p^\alpha - 1)\cdots(p^\alpha - i)\cdots(p^\alpha - p^\alpha + 1)}.$$

The question is, What power of p divides $\binom{p^\alpha m}{p^\alpha}$? Looking at this number, written out as we have written it out, one can see that except for the term m in the numerator, the power of p dividing $(p^\alpha m - i)$ is the same as that dividing $p^\alpha - i$, so all powers of p cancel out except the power which divides m. Thus

$$p^r \mid \binom{p^\alpha m}{p^\alpha} \quad \text{but} \quad p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}.$$

First Proof of the Theorem. Let $\mathscr{M}$ be the set of all subsets of G which have p^α elements. Thus $\mathscr{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements. Given $M_1, M_2 \in \mathscr{M}$ (M is a subset of G having p^α elements, and likewise so is M_2) define $M_1 \sim M_2$ if there exists an element $g \in G$ such that $M_1 = M_2 g$. It is immediate to verify that this defines an equivalence relation on $\mathscr{M}$. We claim that there is at least one equivalence class of elements in $\mathscr{M}$ such that the number of elements in this class is not a multiple of p^{r+1}, for if p^{r+1} is a divisor of the size of each equivalence class, then p^{r+1} would be a divisor of the number of elements in $\mathscr{M}$. Since $\mathscr{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements and $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$, this cannot be the case. Let $\{M_1, \ldots, M_n\}$ be such an equivalence class in $\mathscr{M}$ where $p^{r+1} \nmid n$. By our very definition of equivalence in $\mathscr{M}$, if $g \in G$, for each $i = 1, \ldots, n$, $M_i g = M_j$ for some j, $1 \leq j \leq n$.

We let $H = \{g \in G \mid M_1 g = M_1\}$. Clearly H is a subgroup of G, for if $a, b \in H$, then $M_1 a = M_1$, $M_1 b = M_1$ whence $M_1 ab = (M_1 a)b = M_1 b = M_1$. We shall be vitally concerned with $o(H)$. We claim that $no(H) = o(G)$; we leave the proof to the reader, but suggest the argument used in the counting principle in Section 2.11. Now $no(H) = o(G) = p^\alpha m$; since $p^{r+1} \nmid n$ and $p^{\alpha+r} \mid p^\alpha m = no(H)$, it must follow that $p^\alpha \mid o(H)$, and so $o(H) \geq p^\alpha$. However, if $m_1 \in M_1$, then for all $h \in H$, $m_1 h \in M_1$. Thus M_1 has at least $o(H)$ distinct elements. However, M_1 was a subset of G containing p^α elements. Thus $p^\alpha \geq o(H)$. Combined with $o(H) \geq p^\alpha$ we have that $o(H) = p^\alpha$. *But then we have exhibited a subgroup of G having exactly p^α elements, namely H.* This proves the theorem; it actually has done more—

COROLLARY *If $p^m \mid o(G)$, $p^{m+1} \nmid o(G)$, then G has a subgroup of order p^m.*

Second Proof of Sylow's Theorem. We prove, by induction on the order of the group G, that for every prime p dividing the order of G, G has a p-Sylow subgroup.

If the order of the group is 2, the only relevant prime is 2 and the group certainly has a subgroup of order 2, namely itself.

So we suppose the result to be correct for all groups of order less than $o(G)$. From this we want to show that the result is valid for G. Suppose, then, that $p^m \mid o(G)$, $p^{m+1} \nmid o(G)$, where p is a prime, $m \geq 1$. If $p^m \mid o(H)$ for any subgroup H of G, where $H \neq G$, then by the induction hypothesis, H would have a subgroup T of order p^m. However, since T is a subgroup of H, and H is a subgroup of G, T too is a subgroup of G. But then T would be the sought-after subgroup of order p^m.

We therefore may assume that $p^m \nmid o(H)$ for *any* subgroup H of G, where $H \neq G$. We restrict our attention to a limited set of such subgroups. Recall that if $a \in G$ then $N(a) = \{x \in G \mid xa = ax\}$ is a subgroup of G; moreover, if $a \notin Z$, the center of G, then $N(a) \neq G$. Recall, too, that the class equation of G states that

$$o(G) = \sum \frac{o(G)}{o(N(a))},$$

where this sum runs over one element a from each conjugate class. We separate this sum into two pieces: those a which lie in Z, and those which don't. This gives

$$o(G) = z + \sum_{a \notin Z} \frac{o(G)}{o(N(a))},$$

where $z = o(Z)$. Now invoke the reduction we have made, namely, that $p^m \nmid o(H)$ for any subgroup $H \neq G$ of G, to those subgroups $N(a)$ for $a \notin Z$. Since in this case, $p^m \mid o(G)$ and $p^m \nmid o(N(a))$, we must have that

$$p \left| \frac{o(G)}{o(N(a))} \right.$$

Restating this result,

$$p \left| \frac{o(G)}{o(N(a))} \right.$$

for every $a \in G$ where $a \notin Z$. Look at the class equation with this information in hand. Since $p^m \mid o(G)$, we have that $p \mid o(G)$; also

$$p \left| \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \right..$$

Thus the class equation gives us that $p \mid z$. Since $p \mid z = o(Z)$, by Cauchy's theorem (Theorem 2.11.3), Z has an element $b \neq e$ of order p. Let $B = (b)$, the subgroup of G generated by b. B is of order p; moreover, *since* $b \in Z$, B *must be normal* in G. Hence we can form the quotient group $\bar{G} = G/B$. We look at $\bar{G}$. First of all, its order is $o(G)/o(B) = o(G)/p$, hence is certainly less than $o(G)$. Secondly, we have $p^{m-1} \mid o(\bar{G})$, but $p^m \nmid o(\bar{G})$. Thus, by the induction hypothesis, $\bar{G}$ has a subgroup $\bar{P}$ of order p^{m-1}. Let $P = \{x \in G \mid xB \in \bar{P}\}$; by Lemma 2.7.5, P is a subgroup of G. Moreover, $\bar{P} \approx P/B$ (Prove!); thus

$$p^{m-1} = o(\bar{P}) = \frac{o(P)}{o(B)} = \frac{o(P)}{p}.$$

This results in $o(P) = p^m$. Therefore P is the required p-Sylow subgroup of G. This completes the induction and so proves the theorem.

DEFINITION Let G be a group, A, B subgroups of G. If $x, y \in G$ define $x \sim y$ if $y = axb$ for some $a \in A$, $b \in B$.

LEMMA

The relation defined above is an equivalence relation on G.

The equivalence class of $x \in G$ is the set $AxB = \{axb \mid a \in A, b \in B\}$.

We call the set AxB a *double coset* of A, B in G.

If A, B are finite subgroups of G, how many elements are there in the double coset AxB? To begin with, the mapping $T: AxB \to AxBx^{-1}$ given by $(axb)T = axbx^{-1}$ is one-to-one and onto (verify). Thus $o(AxB) = o(AxBx^{-1})$. Since xBx^{-1} is a subgroup of G, of order $o(B)$, by Theorem 2.5.1,

$$o(AxB) = o(AxBx^{-1}) = \frac{o(A)o(xBx^{-1})}{o(A \cap xBx^{-1})} = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

LEMMA

If A, B are finite subgroups of G then

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

LEMMA

Let G be a finite group and suppose that G is a subgroup of the finite group M. Suppose further that M has a p-Sylow subgroup Q. Then G has a p-Sylow subgroup P. In fact, $P = G \cap xQx^{-1}$ for some $x \in M$.

Proof. Before starting the details of the proof, we translate the hypotheses somewhat. Suppose that $p^m \mid o(M)$, $p^{m+1} \nmid o(M)$, Q is a subgroup of M of order p^m. Let $o(G) = p^n t$ where $p \nmid t$. We want to produce a subgroup P in G of order p^n.

Consider the double coset decomposition of M given by G and Q; $M = \bigcup GxQ$. By Lemma 2.12.4,

$$o(GxQ) = \frac{o(G)o(Q)}{o(G \cap xQx^{-1})} = \frac{p^n t p^m}{o(G \cap xQx^{-1})}.$$

Since $G \cap xQx^{-1}$ is a subgroup of xQx^{-1}, its order is p^{m_x}. We claim that $m_x = n$ for some $x \in M$. If not, then

$$o(GxQ) = \frac{p^n t p^m}{p^{m_x}} = t p^{m+n-m_x},$$

so is divisible by p^{m+1}. Now, since $M = \bigcup GxQ$, and this is disjoint union, $o(M) = \sum o(GxQ)$, the sum running over one element from each double coset. But $p^{m+1} \mid o(GxQ)$; hence $p^{m+1} \mid o(M)$. This contradicts $p^{m+1} \nmid o(M)$. Thus $m_x = n$ for some $x \in M$. But then $o(G \cap xQx^{-1}) = p^n$. Since $G \cap xQx^{-1} = P$ is a subgroup of G and has order p^n, the lemma is proved.

THEOREM

(SECOND PART OF SYLOW'S THEOREM) *If G is a finite*

group, p a prime and $p^n \mid o(G)$ but $p^{n+1} \nmid o(G)$, then any two subgroups of G of order p^n are conjugate.

Proof. Let A, B be subgroups of G, each of order p^n. We want to show that $A = gBg^{-1}$ for some $g \in G$.

Decompose G into double cosets of A and B; $G = \bigcup AxB$. Now, by Lemma 2.12.4,

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}.$$

If $A \neq xBx^{-1}$ for every $x \in G$ then $o(A \cap xBx^{-1}) = p^m$ where $m < n$. Thus

$$o(AxB) = \frac{o(A)o(B)}{p^m} = \frac{p^{2n}}{p^m} = p^{2n-m}$$

and $2n - m \geq n + 1$. Since $p^{n+1} \mid o(AxB)$ for every x and since $o(G) = \sum o(AxB)$, we would get the contradiction $p^{n+1} \mid o(G)$. Thus $A = gBg^{-1}$ for some $g \in G$. This is the assertion of the theorem.

THEOREM

(THIRD PART OF SYLOW'S THEOREM) *The number of p-Sylow subgroups in G, for a given prime, is of the form $1 + kp$.*

Proof. Let P be a p-Sylow subgroup of G. We decompose G into double cosets of P and P. Thus $G = \bigcup PxP$.

$$o(PxP) = \frac{o(P)^2}{o(P \cap xPx^{-1})}.$$

Thus, if $P \cap xPx^{-1} \neq P$ then $p^{n+1} \mid o(PxP)$, where $p^n = o(P)$. Paraphrasing this: if $x \notin N(P)$ then $p^{n+1} \mid o(PxP)$. Also, if $x \in N(P)$, then $PxP = P(Px) = P^2x = Px$, so $o(PxP) = p^n$ in this case.

Now

$$o(G) = \sum_{x \in N(P)} o(PxP) + \sum_{x \notin N(P)} o(PxP),$$

where each sum runs over one element from each double coset. However, if $x \in N(P)$, since $PxP = Px$, the first sum is merely $\sum_{x \in N(P)} o(Px)$ over the *distinct cosets* of P in $N(P)$. Thus this first sum is just $o(N(P))$. What about the second sum? We saw that each of its constituent terms is divisible by p^{n+1}, hence

$$p^{n+1} \Big| \sum_{x \notin N(P)} o(PxP).$$

We can thus write this second sum as

$$\sum_{x \notin N(P)} o(PxP) = p^{n+1}u.$$

Therefore $o(G) = o(N(P)) + p^{n+1}u$, so

$$\frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}u}{o(N(P))}.$$

Now $o(N(P)) \mid o(G)$ since $N(P)$ is a subgroup of G, hence $p^{n+1}u/o(N(P))$ is an integer. Also, since $p^{n+1} \nmid o(G)$, p^{n+1} can't divide $o(N(P))$. But then $p^{n+1}u/o(N(P))$ *must be divisible by* p, so we can write $p^{n+1}u/o(N(P))$ as kp, where k is an integer. Feeding this information back into our equation above, we have

$$\frac{o(G)}{o(N(P))} = 1 + kp.$$

Recalling that $o(G)/o(N(P))$ is the number of p-Sylow subgroups in G, we have the theorem.

Direct Products

DEFINITION Let G be a group and $N_1, N_2, \ldots, N_n$ *normal* subgroups of G such that

1. $G = N_1 N_2 \cdots N_n$.
2. Given $g \in G$ then $g = m_1 m_2 \cdots m_n$, $m_i \in N_i$ in a unique way.

We then say that G is the *internal direct product* of $N_1, N_2, \ldots, N_n$.

THEOREM

Suppose that G is the internal direct product of $N_1, \ldots, N_n$.

Then for $i \neq j$, $N_i \cap N_j = (e)$, and if $a \in N_i$, $b \in N_j$ then $ab = ba$.

Proof. Suppose that $x \in N_i \cap N_j$. Then we can write x as

$$x = e_1 \cdots e_{i-1} x e_{i+1} \cdots e_j \cdots e_n,$$

where $e_t = e$, viewing x as an element of N_j. But every element—and so, in particular x—has a unique representation in the form $m_1 m_2 \cdots m_n$, where $m_i \in N_1, \ldots, m_n \in N_n$. Since the two decompositions in this form for x must coincide, the entry from N_i in each must be equal. In our first decomposition this entry is x, in the other it is e; hence $x = e$. Thus $N_i \cap N_j = (e)$ for $i \neq j$.

Suppose $a \in N_i$, $b \in N_j$, and $i \neq j$. Then $aba^{-1} \in N_j$ since N_j is normal; thus $aba^{-1}b^{-1} \in N_j$. Similarly, since $a^{-1} \in N_i$, $ba^{-1}b^{-1} \in N_i$, whence $aba^{-1}b^{-1} \in N_i$. But then $aba^{-1}b^{-1} \in N_i \cap N_j = (e)$. Thus $aba^{-1}b^{-1} = e$; this gives the desired result $ab = ba$.

One should point out that if $K_1, \ldots, K_n$ are normal subgroups of G such that $G = K_1 K_2 \cdots K_n$ and $K_i \cap K_j = (e)$ for $i \neq j$ it *need not be true* that G is the internal direct product of $K_1, \ldots, K_n$.

THEOREM

Let G be a group and suppose that G is the internal direct product of $N_1, \ldots, N_n$. Let $T = N_1 \times N_2 \times \cdots \times N_n$. Then G and T are isomorphic.

Proof. Define the mapping $\psi: T \to G$ by

$$\psi((b_1, b_2, \ldots, b_n)) = b_1 b_2 \cdots b_n,$$

where each $b_i \in N_i$, $i = 1, \ldots, n$. We claim that ψ is an isomorphism of T onto G.

To begin with, ψ is certainly onto; for, since G is the internal direct product of $N_1, \ldots, N_n$, if $x \in G$ then $x = a_1 a_2 \cdots a_n$ for some $a_1 \in N_1, \ldots, a_n \in N_n$. But then $\psi((a_1, a_2, \ldots, a_n)) = a_1 a_2 \cdots a_n = x$. The mapping ψ is one-to-one by the *uniqueness* of the representation of every element as a product of elements from $N_1, \ldots, N_n$. For, if $\psi((a_1, \ldots, a_n)) = \psi((c_1, \ldots, c_n))$, where $a_i \in N_i$, $c_i \in N_i$, for $i = 1, 2, \ldots, n$, then, by the definition of ψ, $a_1 a_2 \cdots a_n = c_1 c_2 \cdots c_n$. The uniqueness in the definition of internal direct product forces $a_1 = c_1$, $a_2 = c_2, \ldots, a_n = c_n$. Thus ψ is one-to-one.

All that remains is to show that ψ is a homomorphism of T onto G. If $X = (a_1, \ldots, a_n)$, $Y = (b_1, \ldots, b_n)$ are elements of T then

$$\begin{aligned} \psi(XY) &= \psi((a_1, \ldots, a_n)(b_1, \ldots, b_n)) \\ &= \psi(a_1 b_1, a_2 b_2, \ldots, a_n b_n) \\ &= a_1 b_1 a_2 b_2 \cdots a_n b_n. \end{aligned}$$

However, by Lemma 2.13.1, $a_i b_j = b_j a_i$ if $i \neq j$. This tells us that $a_1 b_1 a_2 b_2 \cdots a_n b_n = a_1 a_2 \cdots a_n b_1 b_2 \cdots b_n$. Thus $\psi(XY) = a_1 a_2 \cdots a_n b_1 b_2 \cdots b_n$. But we can recognize $a_1 a_2 \cdots a_n$ as $\psi((a_1, a_2, \ldots, a_n)) = \psi(X)$ and $b_1 b_2 \cdots b_n$ as $\psi(Y)$. We therefore have $\psi(XY) = \psi(X)\psi(Y)$. In short, we have shown that ψ is an isomorphism of T onto G. This proves the theorem.

Finite Abelian Groups

THEOREM

Every finite abelian group is the direct product of cyclic groups.

So suppose that G is an abelian group of order p^n. Our objective is to find elements $a_1, \ldots, a_k$ in G such that every element $x \in G$ can be written in a unique fashion as $x = a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_k^{\alpha_k}$. Note that if this were true and $a_1, \ldots, a_k$ were of order $p^{n_1}, \ldots, p^{n_k}$, where $n_1 \geq n_2 \geq \cdots \geq n_k$, then the maximal order of any element in G would be p^{n_1} (Prove!). This gives us a cue of how to go about finding the elements $a_1, \ldots, a_k$ that we seek.

The procedure suggested by this is: let a_1 be an element of maximal order in G. How shall we pick a_2? Well, if $A_1 = (a_1)$ the subgroup generated by a_1, then a_2 maps into an element of highest order in G/A_1. If we can successfully exploit this to find an appropriate a_2, and if $A_2 = (a_2)$, then a_3 would map into an element of maximal order in G/A_1A_2, and so on. With this as guide we can now get down to the brass tacks of the proof.

Let a_1 be an element in G of highest possible order, p^{n_1}, and let $A_1 = (a_1)$. Pick b_2 in G such that $\bar{b}_2$, the image of b_2 in $\bar{G} = G/A_1$, has maximal order p^{n_2}. Since the order of $\bar{b}_2$ divides that of b_2, and since the order of a_1 is maximal, we must have that $n_1 \geq n_2$. In order to get a direct product of A_1 with (b_2) we would need $A_1 \cap (b_2) = (e)$; this might not be true for the initial choice of b_2, so we may have to adapt the element b_2. Suppose that $A_1 \cap (b_2) \neq (e)$; then, since $b_2^{p^{n_2}} \in A_1$ and is the first power of b_2 to fall in A_1 (by our mechanism of choosing b_2) we have that $b_2^{p^{n_2}} = a_1^{i}$. Therefore $(a_1^{i})^{p^{n_1-n_2}} = (b_2^{p^{n_2}})^{p^{n_1-n_2}} = b_2^{p^{n_1}} = e$, whence $a_1^{ip^{n_1-n_2}} = e$. Since a_1 is of order p^{n_1} we must have that $p^{n_1} \mid ip^{n_1-n_2}$, and so $p^{n_2} \mid i$. Thus, recalling what i is, we have $b_2^{p^{n_2}} = a_1^{i} = a_1^{jp^{n_2}}$. This tells us that if $a_2 = a_1^{-j}b_2$ then $a_2^{p^{n_2}} = e$. The element a_2 is indeed the element we seek. Let $A_2 = (a_2)$. We claim that $A_1 \cap A_2 = (e)$. For, suppose that $a_2^{t} \in A_1$; since $a_2 = a_1^{-j}b_2$, we get $(a_1^{-j}b_2)^t \in A_1$ and so $b_2^{t} \in A_1$. By choice of b_2, this last relation forces $p^{n_2} \mid t$, and since $a_2^{p^{n_2}} = e$ we must have that $a_2^{t} = e$. In short $A_1 \cap A_2 = (e)$.

We continue one more step in the program we have outlined. Let $b_3 \in G$ map into an element of maximal order in $G/(A_1A_2)$. If the order of the image of b_3 in $G/(A_1A_2)$ is p^{n_3}, we claim that $n_3 \leq n_2 \leq n_1$. Why? By the choice of n_2, $b_3^{p^{n_2}} \in A_1$ so is certainly in A_1A_2. Thus $n_3 \leq n_2$. Since

$b_3^{p^{n_3}} \in A_1A_2$, $b_3^{p^{n_3}} = a_1^{i_1}a_2^{i_2}$. We claim that $p^{n_3} \mid i_1$ and $p^{n_3} \mid i_2$. For, $b_3^{p^{n_2}} \in A_1$ hence $(a_1^{i_1}a_2^{i_2})^{p^{n_2-n_3}} = (b_3^{p^{n_3}})^{p^{n_2-n_3}} \equiv b_3^{p^{n_2}} \in A_1$. This tells us that $a_2^{i_2p^{n_2-n_3}} \in A_1$ and so $p^{n_2} \mid i_2p^{n_2-n_3}$, which is to say, $p^{n_3} \mid i_2$. Also $b_3^{p^{n_1}} = e$, hence $(a_1^{i_1}a_2^{i_2})^{p^{n_1-n_3}} = b_3^{p^{n_1}} = e$; this says that $a_1^{i_1p^{n_1-n_3}} \in A_2 \cap A_1 = (e)$, that is, $a_1^{i_1p^{n_1-n_3}} = e$. This yields that $p^{n_3} \mid i_1$. Let $i_1 = j_1p^{n_3}$, $i_2 = j_2p^{n_3}$; thus $b_3^{p^{n_3}} = a_1^{j_1p^{n_3}}a_2^{j_2p^{n_3}}$. Let $a_3 = a_1^{-j_1}a_2^{-j_2}b_3$, $A_3 = (a_3)$; note that $a_3^{p^{n_3}} = e$. We claim that $A_3 \cap (A_1A_2) = (e)$. For if $a_3^t \in A_1A_2$ then $(a_1^{-j_1}a_2^{-j_2}b_3)^t \in A_1A_2$, giving us $b_3^t \in A_1A_2$. But then $p^{n_3} \mid t$, whence, since $a_3^{p^{n_3}} = e$, we have $a_3^t = e$. In other words, $A_3 \cap (A_1A_2) = (e)$.

Continuing this way we get cyclic subgroups $A_1 = (a_1)$, $A_2 = (a_2), \ldots, A_k = (a_k)$ of order $p^{n_1}, p^{n_2}, \ldots, p^{n_k}$, respectively, with $n_1 \geq n_2 \geq \cdots \geq n_k$ such that $G = A_1A_2 \cdots A_k$ and such that, for each i, $A_i \cap (A_1A_2 \cdots A_{i-1}) = (e)$. This tells us that every $x \in G$ has a unique representation as $x = a_1'a_2' \cdots a_k'$ where $a_1' \in A_1, \ldots, a_k' \in A_k$. In other words, G is the direct product of the cyclic subgroups $A_1, A_2, \ldots, A_k$. The theorem is now proved.

DEFINITION If G is an abelian group of order p^n, p a prime, and $G = A_1 \times A_2 \times \cdots \times A_k$ where each A_i is cyclic of order p^{n_i} with $n_1 \geq n_2 \geq \cdots \geq n_k > 0$, then the integers $n_1, n_2, \ldots, n_k$ are called the *invariants* of G.

DEFINITION If G is an abelian group and s is any integer, then $G(s) = \{x \in G \mid x^s = e\}$.

LEMMA

If G and G' are isomorphic abelian groups, then for every integer s, $G(s)$, and $G'(s)$ are isomorphic.

Proof. Let ϕ be an isomorphism of G onto G'. We claim that ϕ maps $G(s)$ isomorphically onto $G'(s)$. First we show that $\phi(G(s)) \subset G'(s)$. For, if $x \in G(s)$ then $x^s = e$, hence $\phi(x^s) = \phi(e) = e'$. But $\phi(x^s) = \phi(x)^s$; hence $\phi(x)^s = e'$ and so $\phi(x)$ is in $G'(s)$. Thus $\phi(G(s)) \subset G'(s)$.

On the other hand, if $u' \in G'(s)$ then $(u')^s = e'$. But, since ϕ is onto, $u' = \phi(y)$ for some $y \in G$. Therefore $e' = (u')^s = \phi(y)^s = \phi(y^s)$. Because ϕ is one-to-one, we have $y^s = e$ and so $y \in G(s)$. Thus ϕ maps $G(s)$ *onto* $G'(s)$.

Therefore since ϕ is one-to-one, onto, and a homomorphism from $G(s)$ to $G'(s)$, we have that $G(s)$ and $G'(s)$ are isomorphic.

THEOREM

Two abelian groups of order p^n are isomorphic if and only if they have the same invariants.

In other words, if G and G' are abelian groups of order p^n and $G = A_1 \times \cdots \times A_k$, where each A_i is a cyclic group of order p^{n_i}, $n_1 \geq \cdots \geq n_k > 0$, and $G' = B_1' \times \cdots \times B_s'$, where each B_i' is a cyclic group of order p^{h_i}, $h_1 \geq \cdots \geq h_s > 0$, then G and G' are isomorphic if and only if $k = s$ and for each i, $n_i = h_i$.

Proof. One way is very easy, namely, if G and G' have the same invariants then they are isomorphic. For then $G = A_1 \times \cdots \times A_k$ where $A_i = (a_i)$ is cyclic of order p^{n_i}, and $G' = B_1' \times \cdots \times B_k'$ where $B_i' = (b_i')$ is cyclic of order p^{n_i}. Map G onto G' by the map $\phi(a_1^{\alpha_1} \cdots a_k^{\alpha_k}) = (b_1')^{\alpha_1} \cdots (b_k')^{\alpha_k}$. We leave it to the reader to verify that this defines an isomorphism of G onto G'.

Now for the other direction. Suppose that $G = A_1 \times \cdots \times A_k$, $G' = B_1' \times \cdots \times B_s'$, A_i, B_i' as described above, cyclic of orders p^{n_i}, p^{h_i}, respectively, where $n_1 \geq \cdots \geq n_k > 0$ and $h_1 \geq \cdots \geq h_s > 0$. We want to show that if G and G' are isomorphic then $k = s$ and each $n_i = h_i$.

If G and G' are isomorphic then, by Lemma 2.14.1, $G(p^m)$ and $G'(p^m)$ must be isomorphic for any integer $m \geq 0$, hence must have the same order. Let's see what this gives us in the special case $m = 1$; that is, what information can we garner from $o(G(p)) = o(G'(p))$. According to the corollary to Lemma 2.14.2, $o(G(p)) = p^k$ and $o(G'(p)) = p^s$. Hence $p^k = p^s$ and so $k = s$. At least we now know that the *number* of invariants for G and G' is the same.

If $n_i \neq h_i$ for some i, let t be the first i such that $n_t \neq h_t$; we may suppose that $n_t > h_t$. Let $m = h_t$. Consider the subgroups, $H = \{x^{p^m} \mid x \in G\}$ and $H' = \{(x')^{p^m} \mid x' \in G\}$, of G and G', respectively. Since G and G' are isomorphic, it follows easily that H and H' are isomorphic. We now examine the invariants of H and H'.

Because $G = A_1 \times \cdots \times A_k$, where $A_i = (a_i)$ is of order p^{n_i}, we get that

$$H = C_1 \times \cdots \times C_t \times \cdots \times C_r,$$

where $C_i = (a_i^{p^m})$ is of order $p^{n_i - m}$, and where r is such that $n_r > m = h_t \geq n_{r-1}$. Thus the invariants of H are $n_1 - m,\ n_2 - m, \ldots, n_r - m$ and the number of invariants of H is $r \geq t$.

Because $G' = B_1' \times \cdots \times B_k'$, where $B_i = (b_i')$ is cyclic of order p^{h_i}, we get that $H' = D_1' \times \cdots \times D_{t-1}'$, where $D_i' = ((b_i')^{p^m})$ is cyclic of order $p^{h_i - m}$. Thus the invariants of H' are $h_1 - m, \ldots, h_{t-1} - m$ and so the number of invariants of H' is $t - 1$.

But H and H' are isomorphic; as we saw above this forces them to have the same number of invariants. But we saw that assuming that $n_i \neq h_i$ for some i led to a discrepancy in the number of their invariants. In consequence each $n_i = h_i$, and the theorem is proved.

Possible Questions

PART-B (6 Mark)

1. Prove that if G is a finite group, then prove that c_a=O(G)/O(N(a))
2. Suppose G is a finite abelian group and p|o(G), where p is prime numberthen prove there is an element $a \neq e \in G$ such that a^p=e.
3. State and prove second part of the Sylow's Theorem.
4. Let G be a group and suppose that G is the internal direct product of N_1, N_2, ….., N_n. Let N_1 X N_2 X……X N_n. Then G and T are isomorphic.
5. Show that the number of elements conjugate to a in G is the index of the normalizer of a in G.
6. State and prove Cauchy's theorem.
7. If G is a finite group, p a prime and $p^n \mid O(G)$ but $p^n \nmid O(G)$, then any two subgroups of G of order p^n are conjugate.
8. Prove that if p is a prime number and p| O(G),then prove that G has an element of order p.
9. State and prove first part of the Sylow's Theorem.
10. If p is a prime number and p| O(G),then prove that G has an element of order p.

PART-C (10 Mark)

1. State and prove third part of the Sylow's Theorem.
2. Prove that if G is a finite group, then prove that c_a=O(G)/O(N(a))
3. If G is a finite group, p a prime and $p^n \mid O(G)$ but $p^n \nmid O(G)$, then any two subgroups of G of order p^n are conjugate.

KARPAGAM ACADEMY OF HIGHER EDUCATION
DEPARTMENT OF MATHEMATICS
ALGEBRA (I8MMP101)
UNIT-I

Question	Option-1	Option-2	Option-3	Option-4	Answer
A group is said to be _____,if for every a,b in group then a*b=b*a	Abelian group	normal	sub group	order	Abelian group
If the number of element is finite then the group is called _____	Abelian group	finite group	infinite group	group	finite group
If the number of element is infinite then the group is called _____	Abelian group	finite group	infinite group	group	infinite group
An infinite group is said to be ----------order	identity	finite	infinite	symmetric	infinite
For every $a \in G, (a^{-1})^{-1}$ = -------	a^{-1}	1	a	0	a
If G is a group, then every $a \in G$ has a --------- inverse in G	zero	two	unique	three	unique
For all $a,b \in G$ $(a.b)^{-1}$ = ------	ab	$b.a^{-1}$	$(a.b)^{-1}$	$b^{-1}.a^{-1}$	$b^{-1}.a^{-1}$
The number of elements in a finite group is called ---------- of the group	order	Non-abelian	infinite	abeliean	order
If G is a group, then the identity element of G is ----------	zero	two	unique	three	unique
A nonempty subset H of a group G is said to be -------- of G H itself forms a group	coset	subset	normal-subgroup	subgroup	subgroup
If G is a finite group and H is a subgroup of G then -------- divisor of o(G)	o(G)	o(S)	o(H)	o(A)	o(H)
If H is a subgroup of G,$a \in G$ then aH is called----------	coset	left- coset	right- coset	ideal	left- coset
If H is a subgroup of G,$a \in G$ then Ha is called----------	coset	left- coset	right- coset	ideal	right- coset
If G is a finite group and H is a subgroup of G then -------- divisor of o(G)	o(G)	o(S)	o(H)	o(A)	o(H)
An isomorphic mapping Φ of a group G onto itself is called automorphism If Φ is _____	one-to-one	onto	into	one to one & onto	onto
An isomorphic mapping of a group G onto itself is called ----------	automorphism	isomorphism	homomorphism	monomorphism	automorphism
A homomorphism F from G into $\bar{G}$ is said to be ---------- ifF is one-to-one	automorphism	isomorphism	homomorphism	monomorphism	isomorphism
A homomorphism Φ from G into $\bar{G}$ is said to be isomorphism if Φ is	one-to-one	onto	into	one to one & onto	one-to-one
If G is a group, N normal subgroup of G then G/N is called -------	quotient group	ring	subgroup	c)normal-subgroup	quotient group
A subgroup N of a group G is said to be normal subgroup of G H if--------	$gng^{-1} \in G$	$gng^{-1} \in N$	$gn \in N$	$ng^{-1} \in N$	$gng^{-1} \in N$
A subgroup N of a group G is said to be ---------- of G H if $gng^{-1} \in N$	coset	subset	normal-subgroup	subgroup	normal-subgroup
If G is a finite group and $a \in G$ the --------- of 'a' is least positive integer m such that $a^m = e$	coset	subset	order	infinite order	order
If G is a finite group and $a \in G$ the order of a is least positive integer m such that a^m =_____	1	e	0	p	e
N(a) is a ---------- of G	coset	subset	normal-subgroup	subgroup	normal-subgroup
Conjugacy is ---------- on G	reflexive	symmetric	transitive	equivalence relation	equivalence relation
If $o(G) = p^2$ where p is a prime number, then G is ----------	Non-abeliean	abeliean	unity	inverse	abeliean
If p is a prime number, and p/o(G) then G has an element of --------	order 1	order p	order e	order 0	order p
If p is a prime number, and p^{α}/o(G) then G has a subgroup of --------	order p^{α}	order p	order 0	order e	order p^{α}
Let Φ be a homomorphism of G onto G with kernal K. Then ----------	G\K ~G	G\K =G	G\K =1	G\K =K	G\K ~G
By an automorphism of a group G we shall mean an ---------- of G onto itself	automorphism	isomorphism	homomorphism	monomorphism	isomorphism
The sub group N of G is a normal sub group of G if and only if every--------- of N in G is a right coset of N in G	coset	left- coset	right- coset	ideal	left- coset
The sub group N of G is a normal sub group of G if and only if every left coset of N in G is a ----- of N in G	coset	left- coset	right- coset	ideal	right- coset
If N and M are sub groups of G then ------ is also a normal sub group	mN	Nm	N/M	M/N	N/M

The center of a group is always a normal sub group	normal-subgroup	subgroup	group	Abelian group	normal-subgroup
If G is a group then A(G) the set of automorphism of G is a ----------	normal-subgroup	subgroup	group	Abelian group	group
Every group is ----------to a sub group of A(S) for some appropriate S	automorphism	isomorphism	homomorphism	monomorphism	isomorphism
Every permutation is the product of its ----------	cycles	2-cycles	group	subgroup	cycles
Every permutation is the --------- of its cycles	sum	division	product	difference	product
Every ---------- is the product of its cycles	normal-subgroup	subgroup	group	permutation	permutation
If o(G)=p2 where p is a prime number then is ----------	non-Abelian	subgroup	group	Abelian	Abelian
If ---------- where p is a prime number then is abelian	o(G)=p2	o(G)=p	o(G)=1	o(G)=n	o(G)=p2
Let G be a -------- then the identity element is unique	normal-subgroup	subgroup	group	permutation	group
The product of even permutation is an -------- permutation	even	even & odd	odd	prime	even
The product of two odd permutation is an --------- permutation	even	even & odd	odd	prime	even
Conjugacy is an ---------- relation on G	reflexive	symmetric	transitive	equivalence	equivalence
If G is a group of order231then the 11- sylow subgroup is in the center of G	sylow subgroup	subgroup	11sylow subgroup	normal subgroup	11sylow subgroup
If G is a group of order231then the 11- sylow subgroup is in the ---------- of G	sylow subgroup	subgroup	normal subgroup	center	center
If o(G)=pq ,p and q are distinct primes p<q then p/(q-1) there exists a unique _____ group of order pq	non abelian	abelian	cyclic	non cyclic	non abelian
If o(G)=_____ ,p and q are distinct primes p<q then p/(q-1) there exists a unique non abelian group of order pq	p	q	pq	p/q	pq
If o(G)=pq ,p and q are distinct primes p<q then _____ there exists a unique non abelian group of order pq	p/(q-1)	p-1/q-1	p/q	pq	p/(q-1)
S_{pk} has -------subgroup	sylow	k-sylow	p-sylow	11sylow subgroup	p-sylow
Every finite ----------group is the direct product of cyclic groups	abeliean	Non-abeliean	cyclic	permutation	abeliean

UNIT-II

Ring Theory- Basic definition- More ideals and quotient rings- Euclidean rings-A Particular Euclidean Rings –Polynomial Rings-Polynomial over the Rational Field.

Ring Theory

DEFINITION A nonempty set R is said to be an *associative ring* if in R there are defined two operations, denoted by $+$ and $\cdot$ respectively, such that for all a, b, c in R:

1. $a + b$ is in R.
2. $a + b = b + a$.
3. $(a + b) + c = a + (b + c)$.
4. There is an element 0 in R such that $a + 0 = a$ (for every a in R).
5. There exists an element $-a$ in R such that $a + (-a) = 0$.
6. $a \cdot b$ is in R.
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ (the two distributive laws).

DEFINITION If R is a commutative ring, then $a \neq 0 \in R$ is said to be a *zero-divisor* if there exists a $b \in R$, $b \neq 0$, such that $ab = 0$.

DEFINITION A commutative ring is an *integral domain* if it has no zero-divisors.

DEFINITION A ring is said to be a *division ring* if its nonzero elements form a group under multiplication.

DEFINITION A *field* is a commutative division ring.

DEFINITION An integral domain D is said to be of *characteristic* 0 if the relation $ma = 0$, where $a \neq 0$ is in D, and where m is an integer, can hold only if $m = 0$.

DEFINITION An integral domain D is said to be of *finite characteristic* if there exists a *positive* integer m such that $ma = 0$ for all $a \in D$.

DEFINITION A mapping ϕ from the ring R into the ring R' is said to be a *homomorphism* if

1. $\phi(a + b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$,

for all $a, b \in R$.

DEFINITION A homomorphism of R into R' is said to be an *isomorphism* if it is a one-to-one mapping.

DEFINITION Two rings are said to be *isomorphic* if there is an isomorphism of one *onto* the other.

Ideals and Quotient Rings

DEFINITION A nonempty subset U of R is said to be a (two-sided) *ideal* of R if

1. U is a subgroup of R under addition.
2. For every $u \in U$ and $r \in R$, both ur and ru are in U.

LEMMA 3.4.1 *If U is an ideal of the ring R, then R/U is a ring and is a homomorphic image of R.*

More Ideals and Quotient Rings

LEMMA

Let R be a commutative ring with unit element whose only ideals are (0) and R itself. Then R is a field.

Proof. In order to effect a proof of this lemma for any $a \neq 0 \in R$ we must produce an element $b \neq 0 \in R$ such that $ab = 1$.

So, suppose that $a \neq 0$ is in R. Consider the set $Ra = \{xa \mid x \in R\}$. We claim that Ra is an ideal of R. In order to establish this as fact we must show that it is a subgroup of R under addition and that if $u \in Ra$ and $r \in R$ then ru is also in Ra. (We only need to check that ru is in Ra for then ur also is since $ru = ur$.)

Now, if $u, v \in Ra$, then $u = r_1a$, $v = r_2a$ for some $r_1, r_2 \in R$. Thus $u + v = r_1a + r_2a = (r_1 + r_2)a \in Ra$; similarly $-u = -r_1a = (-r_1)a \in Ra$. Hence Ra is an additive subgroup of R. Moreover, if $r \in R$, $ru = r(r_1a) = (rr_1)a \in Ra$. Ra therefore satisfies all the defining conditions for an ideal of R, hence is an ideal of R. (Notice that both the distributive law and associative law of multiplication were used in the proof of this fact.)

By our assumptions on R, $Ra = (0)$ or $Ra = R$. Since $0 \neq a = 1a \in Ra$, $Ra \neq (0)$; thus we are left with the only other possibility, namely that $Ra = R$. This last equation states that every element in R is a multiple of a by some element of R. In particular, $1 \in R$ and so it can be realized as a multiple of a; that is, there exists an element $b \in R$ such that $ba = 1$. This completes the proof of the lemma.

DEFINITION An ideal $M \neq R$ in a ring R is said to be a *maximal ideal* of R if whenever U is an ideal of R such that $M \subset U \subset R$, then either $R = U$ or $M = U$.

THEOREM

If R is a commutative ring with unit element and M is an ideal of R, then M is a maximal ideal of R if and only if R/M is a field.

Proof. Suppose, first, that M is an ideal of R such that R/M is a field. Since R/M is a field its only ideals are (0) and R/M itself. But by Theorem 3.4.1 there is a one-to-one correspondence between the set of ideals of R/M and the set of ideals of R which contain M. The ideal M of R corresponds to the ideal (0) of R/M whereas the ideal R of R corresponds to the ideal R/M of R/M in this one-to-one mapping. Thus there is no ideal between M and R other than these two, whence M is a maximal ideal.

On the other hand, if M is a maximal ideal of R, by the correspondence mentioned above R/M has only (0) and itself as ideals. Furthermore R/M is commutative and has a unit element since R enjoys both these properties. All the conditions of Lemma 3.5.1 are fulfilled for R/M so we can conclude, by the result of that lemma, that R/M is a field.

The Field of Quotients of an Integral Domain

DEFINITION A ring R *can be imbedded* in a ring R' if there is an isomorphism of R into R'. (If R and R' have unit elements 1 and 1′ we insist, in addition, that this isomorphism takes 1 onto 1′.)

THEOREM

Every integral domain can be imbedded in a field.

define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

In fact in what is to follow we make these considerations our guide. So let us leave the heuristics and enter the domain of mathematics, with precise definitions and rigorous deductions.

Let $\mathscr{M}$ be the set of all ordered pairs (a, b) where $a, b \in D$ and $b \neq 0$. (Think of (a, b) as a/b.) In $\mathscr{M}$ we now define a relation as follows:

$$(a, b) \sim (c, d) \text{ if and only if } ad = bc.$$

We claim that this defines an equivalence relation on $\mathscr{M}$. To establish this we check the three defining conditions for an equivalence relation for this particular relation.

1. If $(a, b) \in \mathscr{M}$, then $(a, b) \sim (a, b)$ since $ab = ba$.
2. If $(a, b), (c, d) \in \mathscr{M}$ and $(a, b) \sim (c, d)$, then $ad = bc$, hence $cb = da$, and so $(c, d) \sim (a, b)$.
3. If $(a, b), (c, d), (e, f)$ are all in $\mathscr{M}$ and $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $ad = bc$ and $cf = de$. Thus $bcf = bde$, and since $bc = ad$, it follows that $adf = bde$. Since D is commutative, this relation becomes $afd = bed$; since, moreover, D is an integral domain and $d \neq 0$, this relation further implies that $af = be$. But then $(a, b) \sim (e, f)$ and our relation is transitive.

Let $[a, b]$ be the equivalence class in $\mathscr{M}$ of (a, b), and let F be the set of all such equivalence classes $[a, b]$ where $a, b \in D$ and $b \neq 0$. F is the candidate for the field we are seeking. In order to create out of F a field we must introduce an addition and a multiplication for its elements and then show that under these operations F forms a field.

We first dispose of the addition. Motivated by our heuristic discussion at the beginning of the proof we define

$$[a, b] + [c, d] = [ad + bc, bd].$$

Since D is an integral domain and both $b \neq 0$ and $d \neq 0$ we have that $bd \neq 0$; this, at least, tells us that $[ad + bc, bd] \in F$. We now assert that this addition is well defined, that is, if $[a, b] = [a', b']$ and $[c, d] = [c', d']$, then $[a, b] + [c, d] = [a', b'] + [c', d']$. To see that this is so, from $[a, b] = [a', b']$ we have that $ab' = ba'$; from $[c, d] = [c', d']$ we have that $cd' = dc'$. What we need is that these relations force the equality of $[a, b] + [c, d]$ and $[a', b'] + [c', d']$. From the definition of addition this boils down to showing that $[ad + bc, bd] = [a'd' + b'c', b'd']$, or, in equivalent terms, that $(ad + bc)b'd' = bd(a'd' + b'c')$. Using $ab' = ba'$, $cd' = dc'$

this becomes: $(ad + bc)b'd' = adb'd' + bcb'd' = ab'dd' + bb'cd' = ba'dd' + bb'dc' = bd(a'd' + b'c')$, which is the desired equality.

Clearly $[0, b]$ acts as a zero-element for this addition and $[-a, b]$ as the negative of $[a, b]$. It is a simple matter to verify that F is an abelian group under this addition.

We now turn to the multiplication in F. Again motivated by our preliminary heuristic discussion we define $[a, b][c, d] = [ac, bd]$. As in the case of addition, since $b \neq 0$, $d \neq 0$, $bd \neq 0$ and so $[ac, bd] \in F$. A computation, very much in the spirit of the one just carried out, proves that if $[a, b] = [a', b']$ and $[c, d] = [c', d']$ then $[a, b][c, d] = [a', b'][c', d']$. One can now show that the nonzero elements of F (that is, all the elements $[a, b]$ where $a \neq 0$) form an abelian group under multiplication in which $[d, d]$ acts as the unit element and where

$$[c, d]^{-1} = [d, c] \text{ (since } c \neq 0, [d, c] \text{ is in } F).$$

It is a routine computation to see that the distributive law holds in F. F is thus a field.

All that remains is to show that D can be imbedded in F. We shall exhibit an explicit isomorphism of D into F. Before doing so we first notice that for $x \neq 0, y \neq 0$ in D, $[ax, x] = [ay, y]$ because $(ax)y = x(ay)$; let us denote $[ax, x]$ by $[a, 1]$. Define $\phi: D \to F$ by $\phi(a) = [a, 1]$ for every $a \in D$. We leave it to the reader to verify that ϕ is an isomorphism of D into F, and that if D has a unit element 1, then $\phi(1)$ is the unit element of F. The theorem is now proved in its entirety.

Euclidean Rings

DEFINITION An integral domain R is said to be a *Euclidean ring* if for every $a \neq 0$ in R there is defined a nonnegative integer $d(a)$ such that

1. For all $a, b \in R$, both nonzero, $d(a) \leq d(ab)$.
2. For any $a, b \in R$, both nonzero, there exist $t, r \in R$ such that $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.

DEFINITION If $a, b \in R$ then $d \in R$ is said to be a *greatest common divisor* of a and b if

1. $d \mid a$ and $d \mid b$.
2. Whenever $c \mid a$ and $c \mid b$ then $c \mid d$.

We shall use the notation $d = (a, b)$ to denote that d is a greatest common divisor of a and b.

LEMMA

Let R be a Euclidean ring. Then any two elements a and b in R have a greatest common divisor d. Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

Proof. Let A be the set of all elements $ra + sb$ where r, s range over R. We claim that A is an ideal of R. For suppose that $x, y \in A$; therefore $x = r_1a + s_1b$, $y = r_2a + s_2b$, and so $x \pm y = (r_1 \pm r_2)a + (s_1 \pm s_2)b \in A$. Similarly, for any $u \in R$, $ux = u(r_1a + s_1b) = (ur_1)a + (us_1)b \in A$.

Since A is an ideal of R, by Theorem 3.7.1 there exists an element $d \in A$ such that every element in A is a mutiple of d. By dint of the fact that $d \in A$ and that every element of A is of the form $ra + sb$, $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$. Now by the corollary to Theorem 3.7.1, R has a unit element 1; thus $a = 1a + 0b \in A$, $b = 0a + 1b \in A$. Being in A, they are both multiples of d, whence $d \mid a$ and $d \mid b$.

Suppose, finally, that $c \mid a$ and $c \mid b$; then $c \mid \lambda a$ and $c \mid \mu b$ so that c certainly divides $\lambda a + \mu b = d$. Therefore d has all the requisite conditions for a greatest common divisor and the lemma is proved.

DEFINITION Let R be a commutative ring with unit element. An element $a \in R$ is a *unit* in R if there exists an element $b \in R$ such that $ab = 1$.

LEMMA

Let R be an integral domain with unit element and suppose that for $a, b \in R$ both $a \mid b$ and $b \mid a$ are true. Then $a = ub$, where u is a unit in R.

Proof. Since $a \mid b$, $b = xa$ for some $x \in R$; since $b \mid a$, $a = yb$ for some $y \in R$. Thus $b = x(yb) = (xy)b$; but these are elements of an integral domain, so that we can cancel the b and obtain $xy = 1$; y is thus a unit in R and $a = yb$, proving the lemma.

DEFINITION Let R be a commutative ring with unit element. Two elements a and b in R are said to be *associates* if $b = ua$ for some unit u in R.

LEMMA

Let R be a Euclidean ring and $a, b \in R$. If $b \neq 0$ is not a unit

in R, then $d(a) < d(ab)$.

Proof. Consider the ideal $A = (a) = \{xa \mid x \in R\}$ of R. By condition 1 for a Euclidean ring, $d(a) \leq d(xa)$ for $x \neq 0$ in R. Thus the d-value of a is the minimum for the d-value of any element in A. Now $ab \in A$; if $d(ab) = d(a)$, by the proof used in establishing Theorem 3.7.1, since the d-value of ab is minimal in regard to A, every element in A is a multiple of ab. In particular, since $a \in A$, a must be a multiple of ab; whence $a = abx$ for some $x \in R$. Since all this is taking place in an integral domain we obtain $bx = 1$. In this way b is a unit in R, in contradiction to the fact that it was not a unit. The net result of this is that $d(a) < d(ab)$.

DEFINITION In the Euclidean ring R a nonunit π is said to be a *prime element* of R if whenever $\pi = ab$, where a, b are in R, then one of a or b is a unit in R.

A prime element is thus an element in R which cannot be factored in R in a nontrivial way.

LEMMA

Let R be a Euclidean ring. Then every element in R is either a unit in R or can be written as the product of a finite number of prime elements of R.

Proof. The proof is by induction on $d(a)$.

If $d(a) = d(1)$ then a is a unit in R (Problem 3), and so in this case, the assertion of the lemma is correct.

We assume that the lemma is true for all elements x in R such that $d(x) < d(a)$. On the basis of this assumption we aim to prove it for a. This would complete the induction and prove the lemma.

If a is a prime element of R there is nothing to prove. So suppose that $a = bc$ where neither b nor c is a unit in R. By Lemma 3.7.3, $d(b) < d(bc) = d(a)$ and $d(c) < d(bc) = d(a)$. Thus by our induction hypothesis b and c can be written as a product of a finite number of prime elements of R; $b = \pi_1\pi_2 \cdots \pi_n$, $c = \pi'_1\pi'_2 \cdots \pi'_m$ where the π's and π''s are prime elements of R. Consequently $a = bc = \pi_1\pi_2 \cdots \pi_n\pi'_1\pi'_2 \cdots \pi'_m$ and in this way a has been factored as a product of a finite number of prime elements. This completes the proof.

DEFINITION In the Euclidean ring R, a and b in R are said to be *relatively prime* if their greatest common divisor is a unit of R.

LEMMA

Let R be a Euclidean ring. Suppose that for $a, b, c \in R$, $a \mid bc$ but $(a, b) = 1$. Then $a \mid c$.

Proof. As we have seen in Lemma 3.7.1, the greatest common divisor of a and b can be realized in the form $\lambda a + \mu b$. Thus by our assumptions, $\lambda a + \mu b = 1$. Multiplying this relation by c we obtain $\lambda ac + \mu bc = c$. Now $a \mid \lambda ac$, always, and $a \mid \mu bc$ since $a \mid bc$ by assumption; therefore $a \mid (\lambda ac + \mu bc) = c$. This is, of course, the assertion of the lemma.

THEOREM

(UNIQUE FACTORIZATION THEOREM) *Let R be a Euclidean ring and $a \neq 0$ a nonunit in R. Suppose that $a = \pi_1 \pi_2 \cdots \pi_n = \pi'_1 \pi'_2 \cdots \pi'_m$ where the π_i and π'_j are prime elements of R. Then $n = m$ and each π_i, $1 \leq i \leq n$ is an associate of some π'_j, $1 \leq j \leq m$ and conversely each π'_k is an associate of some π_q.*

Proof. Look at the relation $a = \pi_1 \pi_2 \cdots \pi_n = \pi'_1 \pi'_2 \cdots \pi'_m$. But $\pi_1 \mid \pi_1 \pi_2 \cdots \pi_n$, hence $\pi_1 \mid \pi'_1 \pi'_2 \cdots \pi'_m$. By Lemma 3.7.6, π_1 must divide some π'_i; since π_1 and π'_i are both prime elements of R and $\pi_1 \mid \pi'_i$ they must be associates and $\pi'_i = u_1 \pi_1$, where u_1 is a unit in R. Thus $\pi_1 \pi_2 \cdots \pi_n = \pi'_1 \pi'_2 \cdots \pi'_m = u_1 \pi_1 \pi'_2 \cdots \pi'_{i-1} \pi'_{i+1} \cdots \pi'_m$; cancel off π_1 and we are left with $\pi_2 \cdots \pi_n = u_1 \pi'_2 \cdots \pi'_{i-1} \pi'_{i+1} \cdots \pi'_m$. Repeat the argument on this relation with π_2. After n steps, the left side becomes 1, the right side a product of a certain number of π' (the excess of m over n). This would force $n \leq m$ since the π' are not units. Similarly, $m \leq n$, so that $n = m$. In the process we have also showed that every π_i has some π'_i as an associate and conversely.

Polynomial Rings

DEFINITION If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$ are in $F[x]$, then $p(x) = q(x)$ if and only if for every integer $i \geq 0$, $a_i = b_i$.

Thus two polynomials are declared to be equal if and only if their corresponding coefficients are equal.

DEFINITION If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$ are both in $F[x]$, then $p(x) + q(x) = c_0 + c_1x + \cdots + c_tx^t$ where for each i, $c_i = a_i + b_i$.

In other words, add two polynomials by adding their coefficients and collecting terms. To add $1 + x$ and $3 - 2x + x^2$ we consider $1 + x$ as $1 + x + 0x^2$ and add, according to the recipe given in the definition, to obtain as their sum $4 - x + x^2$.

DEFINITION If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$, then $p(x)q(x) = c_0 + c_1x + \cdots + c_kx^k$ where $c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + \cdots + a_0b_t$.

DEFINITION If $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ and $a_n \neq 0$ then the *degree* of $f(x)$, written as $\deg f(x)$, is n.

LEMMA

If $f(x)$, $g(x)$ are two nonzero elements of $F[x]$, then

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

Proof. Suppose that $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$ and that $a_m \neq 0$ and $b_n \neq 0$. Therefore $\deg f(x) = m$ and $\deg g(x) = n$. By definition, $f(x)g(x) = c_0 + c_1x + \cdots + c_kx^k$ where $c_t = a_tb_0 + a_{t-1}b_1 + \cdots + a_1b_{t-1} + a_0b_t$. We claim that $c_{m+n} = a_mb_n \neq 0$ and $c_i = 0$ for $i > m + n$. That $c_{m+n} = a_mb_n$ can be seen at a glance by its definition. What about c_i for $i > m + n$? c_i is the sum of terms of the form a_jb_{i-j}; since $i = j + (i - j) > m + n$ then either $j > m$ or $(i - j) > n$. But then one of a_j or b_{i-j} is 0, so that $a_jb_{i-j} = 0$; since c_i is the sum of a bunch of zeros it itself is 0, and our claim has been established. Thus the highest nonzero coefficient of $f(x)g(x)$ is c_{m+n}, whence $\deg f(x)g(x) = m + n = \deg f(x) + \deg g(x)$.

COROLLARY *If $f(x)$, $g(x)$ are nonzero elements in $F[x]$ then* $\deg f(x) \leq \deg f(x)g(x)$.

Proof. Since $\deg f(x)g(x) = \deg f(x) + \deg g(x)$, and since $\deg g(x) \geq 0$, this result is immediate from the lemma.

LEMMA 3.9.2 (The Division Algorithm) *Given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$, then there exist two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.*

If the degree of $f(x)$ is smaller than that of $g(x)$ there is nothing to prove, for merely put $t(x) = 0$, $r(x) = f(x)$, and we certainly have that $f(x) = 0g(x) + f(x)$ where $\deg f(x) < \deg g(x)$ or $f(x) = 0$.

So we may assume that $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$ where $a_m \neq 0$, $b_n \neq 0$ and $m \geq n$.

Let $f_1(x) = f(x) - (a_m/b_n)x^{m-n}g(x)$; thus $\deg f_1(x) \leq m - 1$, so by induction on the degree of $f(x)$ we may assume that $f_1(x) = t_1(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. But then $f(x) - (a_m/b_n)x^{m-n}g(x) = t_1(x)g(x) + r(x)$, from which, by transposing, we arrive at $f(x) = ((a_m/b_n)x^{m-n} + t_1(x))g(x) + r(x)$. If we put $t(x) = (a_m/b_n)x^{m-n} + t_1(x)$ we do indeed have that $f(x) = t(x)g(x) + r(x)$ where $t(x)$, $r(x) \in F[x]$ and where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. This proves the lemma.

DEFINITION A polynomial $p(x)$ in $F[x]$ is said to be *irreducible* over F if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$, then one of $a(x)$ or $b(x)$ has degree 0 (i.e., is a constant).

Irreducibility depends on the field; for instance the polynomial $x^2 + 1$ is irreducible over the real field but not over the complex field, for there $x^2 + 1 = (x + i)(x - i)$ where $i^2 = -1$.

LEMMA 3.9.5 *Any polynomial in $F[x]$ can be written in a unique manner as a product of irreducible polynomials in $F[x]$.*

LEMMA 3.9.6 *The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is irreducible over F.*

Polynomials over the Rational Field

DEFINITION The polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$, where the $a_0, a_1, a_2, \ldots, a_n$ are integers is said to be *primitive* if the greatest common divisor of $a_0, a_1, \ldots, a_n$ is 1.

LEMMA 3.10.1 *If $f(x)$ and $g(x)$ are primitive polynomials, then $f(x)g(x)$ is a primitive polynomial.*

Proof. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$. Suppose that the lemma was false; then all the coefficients of $f(x)g(x)$ would be divisible by some integer larger than 1, hence by some prime number p. Since $f(x)$ is primitive, p does not divide some coefficient a_i. Let a_j be the first coefficient of $f(x)$ which p does not divide. Similarly let b_k be the first coefficient of $g(x)$ which p does not divide. In $f(x)g(x)$ the coefficient of x^{j+k}, c_{j+k}, is

$$c_{j+k} = a_j b_k + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0) + (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0 b_{j+k}). \quad (1)$$

Now by our choice of b_k, $p \mid b_{k-1}, b_{k-2}, \ldots$ so that $p \mid (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0)$. Similarly, by our choice of a_j, $p \mid a_{j-1}, a_{j-2}, \ldots$ so that $p \mid (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0 b_{k+j})$. By assumption, $p \mid c_{j+k}$. Thus by (1), $p \mid a_j b_k$, which is nonsense since $p \nmid a_j$ and $p \nmid b_k$. This proves the lemma.

DEFINITION The *content* of the polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, where the a's are integers, is the greatest common divisor of the integers $a_0, a_1, \ldots, a_n$.

Clearly, given any polynomial $p(x)$ with integer coefficients it can be written as $p(x) = dq(x)$ where d is the content of $p(x)$ and where $q(x)$ is a primitive polynomial.

THEOREM 3.10.1 (GAUSS' LEMMA) *If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.*

Proof. Suppose that $f(x) = u(x)v(x)$ where $u(x)$ and $v(x)$ have rational coefficients. By clearing of denominators and taking out common factors we can then write $f(x) = (a/b)\lambda(x)\mu(x)$ where a and b are integers and where both $\lambda(x)$ and $\mu(x)$ have integer coefficients and are primitive. Thus $bf(x) = a\lambda(x)\mu(x)$. The content of the left-hand side is b, since $f(x)$ is primitive; since both $\lambda(x)$ and $\mu(x)$ are primitive, by Lemma 3.10.1 $\lambda(x)\mu(x)$ is primitive, so that the content of the right-hand side is a. Therefore $a = b$, $(a/b) = 1$, and $f(x) = \lambda(x)\mu(x)$ where $\lambda(x)$ and $\mu(x)$ have integer coefficients. This is the assertion of the theorem.

DEFINITION A polynomial is said to be *integer monic* if all its coefficients are integers and its highest coefficient is 1.

Thus an integer monic polynomial is merely one of the form $x^n + a_1 x^{n-1} + \cdots + a_n$ where the a's are integers. Clearly an integer monic polynomial is primitive.

COROLLARY *If an integer monic polynomial factors as the product of two non-constant polynomials having rational coefficients then it factors as the product of two integer monic polynomials.*

THEOREM 3.10.2 (THE EISENSTEIN CRITERION) *Let* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ *be a polynomial with integer coefficients. Suppose that for some prime number* p, $p \nmid a_n$, $p \mid a_1, p \mid a_2, \ldots, p \mid a_0$, $p^2 \nmid a_0$. *Then* $f(x)$ *is irreducible over the rationals.*

Proof. Without loss of generality we may assume that $f(x)$ is primitive, for taking out the greatest common factor of its coefficients does not disturb the hypotheses, since $p \nmid a_n$. If $f(x)$ factors as a product of two rational polynomials, by Gauss' lemma it factors as the product of two polynomials having integer coefficients. Thus if we assume that $f(x)$ is reducible, then

$$f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s),$$

where the b's and c's are integers and where $r > 0$ and $s > 0$. Reading off the coefficients we first get $a_0 = b_0c_0$. Since $p \mid a_0$, p must divide one of b_0 or c_0. Since $p^2 \nmid a_0$, p cannot divide both b_0 and c_0. Suppose that $p \mid b_0$, $p \nmid c_0$. Not all the coefficients $b_0, \ldots, b_r$ can be divisible by p; otherwise all the coefficients of $f(x)$ would be divisible by p, which is manifestly false since $p \nmid a_n$. Let b_k be the first b not divisible by p, $k \leq r < n$. Thus $p \mid b_{k-1}$ and the earlier b's. But $a_k = b_kc_0 + b_{k-1}c_1 + b_{k-2}c_2 + \cdots + b_0c_k$, and $p \mid a_k, p \mid b_{k-1}, b_{k-2}, \ldots, b_0$, so that $p \mid b_kc_0$. However, $p \nmid c_0, p \nmid b_k$, which conflicts with $p \mid b_kc_0$. This contradiction proves that we could not have factored $f(x)$ and so $f(x)$ is indeed irreducible.

Possible Questions

PART-B (6 Mark)

1. Show that if f(x),g(x) are two nonzero elements of F[x], then prove that deg (f(x)g(x)) = deg f(x)+deg g(x).
2. Let R be a commutative ring with unit element whose only ideals are 0 and R itself then prove that R is a field.
3. State and prove Gauss Lemma.
4. State and prove the Eisenstein Criterion.
5. Prove that if f(x) and g(x) are primitive polynomials, then prove that f(x)g(x) is a primitive polynomials.
6. Given two polynomials f(x) and g(x) in F[x],then prove that there exist two polynomials t(x) and r(x) in F[x] such that f(x)=t(x)g(x)+r(x),where r(x)=0 or deg r(x)<deg g(x).
7. If p is a prime number of the form 4n+1.then prove that $p=a^2+b^2$ for some integer a,b.
8. State and prove Fermat theorem

PART-C (10 Mark)

1. State and prove the Eisenstein Criterion.
2. Show that if R is a unique factorization domain, and then proves that the product of two primitive polynomials in R[x] is again a primitive polynomial in R[x].
3. Prove that every integral domain can be imbedded in a field.

KARPAGAM ACADEMY OF HIGHER EDUCATION
DEPARTMENT OF MATHEMATICS
ALBEBRA (18MMP101)

Questions	choice 1	choice 2	choice 3	choice 4	Answer
UNIT - II					
If in a ring R there is an element 1 in R such that a.1=1.a=a then R is --------	ring with unit element	commutative ring	zero	none	ring with unit element
If the multiplication of R such that a.b=b.a then R is --------	ring with unit element	commutative ring	zero	none	commutative ring
A commutative ring with unity without zero divisors is called -------	integral domain	zero	identity	commutative ring	integral domain
A commutative ring with unity ---------- is called integral domain	without zero divisors	with zero divisors	zero	identity	without zero divisors
A commutative division ring is ---------	ring	Field	integral domain	zero	Field
Another name of division ring is----------	Field	integral domain	skew Field	group	Field
Every ---------- is a field	integral domain	finite integral domain	infinite integral domain	ring	finite integral domain
An element a of a ring R is said to be idempotent if -------	a=1	$a^2=1$	$a^2=a$	$a^2=0$	$a^2=a$
An element a of a ring R is said to be ---------- if $a^2=a$	idempotent	nilpotent	identity	none	idempotent
An element a of a ring R is said to be ---------- if $a^2=0$	idempotent	nilpotent	identity	none	nilpotent
A commutative ring is an ---------- if it has no zero divisors	Division ring	field	integral domain	Eucledian ring	integral domain
A ring is said to be ---------- if its nonzero elements form a group under multiplication	Division ring	field	integral domain	Eucledian ring	Division ring
A ring is said to be division ring if its nonzero elements form a ---------- under multiplication	Division ring	group	integral domain	Eucledian ring	group
A commutative ring is an integral domain if it has ----------	Division ring	field	no zero divisiors	zero divisiors	no zero divisiors
A finite integral domain is a ----------	Division ring	field	integral domain	Eucledian ring	field
A ---------- is a field-	Division ring	finite integral domain	integral domain	ring	finite integral domain
A homomorphism of R into R' is said to be an ---------- if it is a one-to one mapping	isomorphism	automorphism	homomorphism	monomorphism	isomorphism
A homomorphism of R into R' is said to be an isomrphism if it is a ----------mapping	one-one	onto	into	into & onto	one-one
A homomorphism of R into R' is said to be an isomrphism if and only if I(Φ)= -------	one	zero	two	three	zero
A ---------- ring is an integral domain if it has no zero divisors	Division ring	field	commutative ring	Eucledian ring	commutative ring
A---------- possesses a unit element	Division ring	field	integral domain	Eucledian ring	Eucledian ring
A non-empty set I is called ---------- if it is both left and right ideal K	one-sided ideal	two-sided ideal	field	integral domain	two-sided ideal
A non-empty set I is called two sided ideal if it is ----------	left ideal	right ideal	field	both left and right ideal	both left and right ideal
The polynomial is said to be --------- if the G.C.D is one	primitive	field	integral domain	Eucledian ring	primitive
The polynomial is said to be primitive if the G.C.D is ----------	two	one	zero	four	one
A polynomial is said to be integer monic if all its coefficients are ----------	integers	rational	real	complex	integers
A polynomial is said to be ---------- if all its coefficients are integers	integer monic	rational monic	real monic	complex monic	integer monic
J(i) is a ----------	integral domain	Euclidean ring	Field	skew field	Euclidean ring
.---------- is a Eucledian ring.	F(i)	J(i)	M(i)	A(i)	J(i)
If a∈R is an ---------- and a/bc, then a/b or a/c	zero divisor	primitive	irreducible	integers	irreducible
_____ is a commutative ring with unit element	(R, +,.)	(Z, *,.)	(R, *,.)	(R, +,*)	(R, +,.)
(R, +,.) is a _____ with unit element	field	commutative ring	Eucledian ring	ring	commutative ring
_____ is an Integral domain.	skew Field	Field	ring	group	Field
Field is an _____	integer monic	Eucledian ring	integers	integral domain	integral domain
The smallest such positive integer n is called _____ if no positive integer then r is said to be a characteristic zero or infinite.	Euclidean ring R	the characteristics of a ring R	infinite integral domain	Division ring R	the characteristics of a ring R
The smallest such positive integer n is called the characteristics of a ring R if no _____ integer then r is said to be a characteristic zero or infinite.	positive	real	rational	complex	positive

The smallest such positive integer n is called the characteristics of a ring R if no positive integer then r is said to be a _____	characteristic zero or infinite	characteristic one	characteristic finite	characteristic ring	characteristic zero or infinite
A_____ has no proper ideals	field	group	Field	ring	field
A field has no _____	right ideal	proper ideals	one-sided ideal	two-sided ideal	proper ideals
An _____ generated by a single element of itself it called a principle ideal	group	ideal	Field	ring	ideal
An ideal generated by a _____ element of itself it called a principle ideal	two-sided ideal	one-sided ideal	double	single	single
An ideal generated by a single element of itself it called a _____	integral domain	principle ideal	ideal	Eucledian ring	principle ideal
An ---------- possess a unit element.	integer monic	Division ring	Euclidean ring	integral domain	Euclidean ring
An Euclidean ring possess a _____ element.	field	unit	double	no	unit
An _____ is said to be of characteristics zero if the relation Ma = 0, where a ≠0 is in D and where m is an integer can hold only if m=0	skew Field	Integral domain D	Division ring R	the characteristics of a ring R	Integral domain D
A ---------- of R into R' is said to be an isomorphism if it is one- one mapping.	homomorphism	isomorphism	automorphism	monomorphism	homomorphism
A homomorphism of R into R' is said to be an ---------- if it is one- one mapping.	isomorphism	identity	integral domain	Eucledian ring	isomorphism
A homomorphism of R into R' is said to be an isomorphism if it is --------- mapping.	onto	one- one	into	into & onto	one- one
We cannot define the ---------- of the zero polynomial.	sum	degree	order	power	degree
A---------- is a constant if it degree is zero.	monomial	trinomial	polynomial	binomial	polynomial

UNIT-III

Fields – Extension Fields-Finite Extension of F – Some basic Definitions and Theorem – Roots of a Polynomial – More about Roots – The elements of Galois theory.

Fields Extension Fields

DEFINITION The *degree* of K over F is the dimension of K as a vector space over F.

DEFINITION The polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$, where the $a_0, a_1, a_2, \ldots, a_n$ are integers is said to be *primitive* if the greatest common divisor of $a_0, a_1, \ldots, a_n$ is 1.

DEFINITION If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$ are both in $F[x]$, then $p(x) + q(x) = c_0 + c_1x + \cdots + c_tx^t$ where for each i, $c_i = a_i + b_i$.

In other words, add two polynomials by adding their coefficients and collecting terms. To add $1 + x$ and $3 - 2x + x^2$ we consider $1 + x$ as $1 + x + 0x^2$ and add, according to the recipe given in the definition, to obtain as their sum $4 - x + x^2$.

DEFINITION If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$, then $p(x)q(x) = c_0 + c_1x + \cdots + c_kx^k$ where $c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + \cdots + a_0b_t$.

DEFINITION If $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ and $a_n \neq 0$ then the *degree* of $f(x)$, written as $\deg f(x)$, is n.

THEOREM 5.1.1 *If L is a finite extension of K and if K is a finite extension of F, then L is a finite extension of F. Moreover, $[L:F] = [L:K][K:F]$.*

Proof. The strategy we employ in the proof is to write down explicitly a basis of L over F. In this way not only do we show that L is a finite extension of F, but we actually prove the sharper result and the one which is really the heart of the theorem, namely that $[L:F] = [L:K][K:F]$.

Suppose, then, that $[L:K] = m$ and that $[K:F] = n$. Let $v_1, \ldots, v_m$ be a basis of L over K and let $w_1, \ldots, w_n$ be a basis of K over F. What could possibly be nicer or more natural than to have the elements $v_i w_j$, where $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, serve as a basis of L over F? Whatever else, they do at least provide us with the right number of elements. We now proceed to show that they do in fact form a basis of L over F. What do we need to establish this? First we must show that every element in L is a linear combination of them with coefficients in F, and then we must demonstrate that these mn elements are linearly independent over F.

Let t be any element in L. Since every element in L is a linear combination of $v_1, \ldots, v_m$ with coefficients in K, in particular, t must be of this form. Thus $t = k_1 v_1 + \cdots + k_m v_m$, where the elements $k_1, \ldots, k_m$ are all in K. However, every element in K is a linear combination of $w_1, \ldots, w_n$ with coefficients in F. Thus $k_1 = f_{11} w_1 + \cdots + f_{1n} w_n, \ldots, k_i = f_{i1} w_1 + \cdots + f_{in} w_n, \ldots, k_m = f_{m1} w_1 + \cdots + f_{mn} w_n$, where every f_{ij} is in F.

Substituting these expressions for $k_1, \ldots, k_m$ into $t = k_1 v_1 + \cdots + k_m v_m$, we obtain $t = (f_{11} w_1 + \cdots + f_{1n} w_n) v_1 + \cdots + (f_{m1} w_1 + \cdots + f_{mn} w_n) v_m$ Multiplying this out, using the distributive and associative laws, we finally arrive at $t = f_{11} v_1 w_1 + \cdots + f_{1n} v_1 w_n + \cdots + f_{ij} v_i w_j + \cdots + f_{mn} v_m w_n$. Since the f_{ij} are in F, we have realized t as a linear combination over F of the elements $v_i w_j$. Therefore, the elements $v_i w_j$ do indeed span all of L over F, and so they fulfill the first requisite property of a basis.

We still must show that the elements $v_i w_j$ are linearly independent over F. Suppose that $f_{11}v_1w_1 + \cdots + f_{1n}v_1w_n + \cdots + f_{ij}v_iw_j + \cdots + f_{mn}v_mw_n = 0$, where the f_{ij} are in F. Our objective is to prove that each $f_{ij} = 0$. Regrouping the above expression yields $(f_{11}w_1 + \cdots + f_{1n}w_n)v_1 + \cdots + (f_{i1}w_1 + \cdots + f_{in}w_n)v_i + \cdots + (f_{m1}w_1 + \cdots + f_{mn}w_n)v_m = 0$.

Since the w_i are in K, and since $K \supset F$, all the elements $k_i = f_{i1}w_1 + \cdots + f_{in}w_n$ are in K. Now $k_1v_1 + \cdots + k_mv_m = 0$ with $k_1, \ldots, k_m \in K$. But, by assumption, $v_1, \ldots, v_m$ form a basis of L over K, so, in particular they must be linearly independent over K. The net result of this is that $k_1 = k_2 = \cdots = k_m = 0$. Using the explicit values of the k_i, we get

$$f_{i1}w_1 + \cdots + f_{in}w_n = 0 \qquad \text{for} \quad i = 1, 2, \ldots, m.$$

But now we invoke the fact that the w_i are linearly independent over F; this yields that each $f_{ij} = 0$. In other words, we have proved that the v_iw_j are linearly independent over F. In this way they satisfy the other requisite property for a basis.

We have now succeeded in proving that the mn elements v_iw_j form a basis of L over F. Thus $[L:F] = mn$; since $m = [L:K]$ and $n = [K:F]$ we have obtained the desired result $[L:F] = [L:K][K:F]$.

Suppose that L, K, F are three fields in the relation $L \supset K \supset F$ and, suppose further that $[L:F]$ is finite. Clearly, any elements in L linearly independent over K are, all the more so, linearly independent over F. Thus the assumption that $[L:F]$ is finite forces the conclusion that $[L:K]$ is finite. Also, since K is a subspace of L, $[K:F]$ is finite. By the theorem, $[L:F] = [L:K][K:F]$, whence $[K:F] \mid [L:F]$. We have proved the

COROLLARY *If L is a finite extension of F and K is a subfield of L which contains F, then $[K:F] \mid [L:F]$.*

Thus, for instance, if $[L:F]$ is a prime number, then there can be no fields properly between F and L. A little later, in Section 5.4, when we discuss the construction of certain geometric figures by straightedge and compass, this corollary will be of great significance.

DEFINITION An element $a \in K$ is said to be *algebraic over F* if there exist elements $\alpha_0, \alpha_1, \ldots, \alpha_n$ in F, not all 0, such that $\alpha_0 a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$.

If the polynomial $q(x) \in F[x]$, the ring of polynomials in x over F, and if $q(x) = \beta_0 x^m + \beta_1 x^{m-1} + \cdots + \beta_m$, then for any element $b \in K$, by $q(b)$ we shall mean the element $\beta_0 b^m + \beta_1 b^{m-1} + \cdots + \beta_m$ in K. In the expression commonly used, $q(b)$ is the *value* of the polynomial $q(x)$ obtained by substituting b for x. The element b is said to *satisfy* $q(x)$ if $q(b) = 0$.

THEOREM 5.1.2 *The element $a \in K$ is algebraic over F if and only if $F(a)$ is a finite extension of F.*

Proof. As is so very common with so many such "if and only if" propositions, one-half of the proof will be quite straightforward and easy, whereas the other half will be deeper and more complicated.

Suppose that $F(a)$ is a finite extension of F and that $[F(a):F] = m$. Consider the elements $1, a, a^2, \ldots, a^m$; they are all in $F(a)$ and are $m+1$ in number. By Lemma 4.2.4, these elements are linearly dependent over F. Therefore, there are elements $\alpha_0, \alpha_1, \ldots, \alpha_m$ in F, not all 0, such that $\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_m a^m = 0$. Hence a is algebraic over F and satisfies the nonzero polynomial $p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$ in $F[x]$ of degree at most $m = [F(a):F]$. This proves the "if" part of the theorem.

Now to the "only if" part. Suppose that a in K is algebraic over F. By assumption, a satisfies some nonzero polynomial in $F[x]$; let $p(x)$ be a polynomial in $F[x]$ of smallest positive degree such that $p(a) = 0$. We claim that $p(x)$ is irreducible over F. For, suppose that $p(x) = f(x)g(x)$, where $f(x), g(x) \in F[x]$; then $0 = p(a) = f(a)g(a)$ (see Problem 1) and, since $f(a)$ and $g(a)$ are elements of the field K, the fact that their product is 0 forces $f(a) = 0$ or $g(a) = 0$. Since $p(x)$ is of lowest positive degree with $p(a) = 0$, we must conclude that one of $\deg f(x) \geq \deg p(x)$ or $\deg g(x) \geq \deg p(x)$ must hold. But this proves the irreducibility of $p(x)$.

We define the mapping ψ from $F[x]$ into $F(a)$ as follows. For any $h(x) \in F[x]$, $h(x)\psi = h(a)$. We leave it to the reader to verify that ψ is a ring homomorphism of the ring $F[x]$ into the field $F(a)$ (see Problem 1). What is V, the kernel of ψ? By the very definition of ψ, $V = \{h(x) \in F[x] \mid h(a) = 0\}$. Also, $p(x)$ is an element of lowest degree in the ideal V of $F[x]$. By the results of Section 3.9, every element in V is a multiple of $p(x)$, and since $p(x)$ is irreducible, by Lemma 3.9.6, V is a maximal ideal

of $F[x]$. By Theorem 3.5.1, $F[x]/V$ is a field. Now by the general homomorphism theorem for rings (Theorem 3.4.1), $F[x]/V$ is isomorphic to the image of $F[x]$ under ψ. Summarizing, we have shown that the image of $F[x]$ under ψ is a subfield of $F(a)$. This image contains $x\psi = a$ and, for every $\alpha \in F$, $\alpha\psi = \alpha$. Thus the image of $F[x]$ under ψ is a subfield of $F[a]$ which contains both F and a; by the very definition of $F(a)$ we are forced to conclude that the image of $F[x]$ under ψ is *all* of $F(a)$. Put more succinctly, $F[x]/V$ is isomorphic to $F(a)$.

Now, $V = (p(x))$, the ideal generated by $p(x)$; from this we claim that the dimension of $F[x]/V$, as a vector space over F, is precisely equal to $\deg p(x)$ (see Problem 2). In view of the isomorphism between $F[x]/V$ and $F(a)$ we obtain the fact that $[F(a):F] = \deg p(x)$. Therefore, $[F(a):F]$ is certainly finite; this is the contention of the "only if" part of the theorem. Note that we have actually proved more, namely that $[F(a):F]$ is equal to the degree of the polynomial of least degree satisfied by a over F.

Suppose that $p(x)$ is of degree n; thus $p(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n$ where the α_i are in F. By assumption, $a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$, whence $a^n = -\alpha_1 a^{n-1} - \alpha_2 a^{n-2} - \cdots - \alpha_n$. What about a^{n+1}? From the above, $a^{n+1} = -\alpha_1 a^n - \alpha_2 a^{n-1} - \cdots - \alpha_n a$; if we substitute the expression for a^n into the right-hand side of this relation, we realize a^{n+1} as a linear combination of the elements $1, a, \ldots, a^{n-1}$ over F. Continuing this way, we get that a^{n+k}, for $k \geq 0$, is a linear combination over F of $1, a, a^2, \ldots, a^{n-1}$.

Now consider $T = \{\beta_0 + \beta_1 a + \cdots + \beta_{n-1} a^{n-1} \mid \beta_0, \beta_1, \ldots, \beta_{n-1} \in F\}$. Clearly, T is closed under addition; in view of the remarks made in the paragraph above, it is also closed under multiplication. Whatever further it may be, T has at least been shown to be a ring. Moreover, T contains both F and a. We now wish to show that T is more than just a ring, that it is, in fact, a field.

Let $0 \neq u = \beta_0 + \beta_1 a + \cdots + \beta_{n-1} a^{n-1}$ be in T and let $h(x) = \beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1} \in F[x]$. Since $u \neq 0$, and $u = h(a)$, we have that $h(a) \neq 0$, whence $p(x) \nmid h(x)$. By the irreducibility of $p(x)$, $p(x)$ and $h(x)$ must therefore be relatively prime. Hence we can find polynomials $s(x)$ and $t(x)$ in $F[x]$ such that $p(x)s(x) + h(x)t(x) = 1$. But then $1 = p(a)s(a) + h(a)t(a) = h(a)t(a)$, since $p(a) = 0$; putting into this that

$u = h(a)$, we obtain $ut(a) = 1$. The inverse of u is thus $t(a)$; in $t(a)$ all powers of a higher than $n - 1$ can be replaced by linear combinations of $1, a, \ldots, a^{n-1}$ over F, whence $t(a) \in T$. We have shown that every nonzero element of T has its inverse in T; consequently, T is a field. However, $T \subset F(a)$, yet F and a are both contained in T, which results in $T = F(a)$. We have identified $F(a)$ as the set of all expressions $\beta_0 + \beta_1 a + \cdots + \beta_{n-1}a^{n-1}$.

Now T is spanned over F by the elements $1, a, \ldots, a^{n-1}$ in consequence of which $[T:F] \leq n$. However, the elements $1, a, a^2, \ldots, a^{n-1}$ are linearly independent over F, for any relation of the form $\gamma_0 + \gamma_1 a + \cdots + \gamma_{n-1}a^{n-1}$, with the elements $\gamma_i \in F$, leads to the conclusion that a satisfies the polynomial $\gamma_0 + \gamma_1 x + \cdots + \gamma_{n-1}x^{n-1}$ over F of degree less than n. This contradiction proves the linear independence of $1, a, \ldots, a^{n-1}$, and so these elements actually form a basis of T over F, whence, in fact, we now know that $[T:F] = n$. Since $T = F(a)$, the result $[F(a):F] = n$ follows.

DEFINITION The element $a \in K$ is said to be *algebraic of degree n* over F if it satisfies a nonzero polynomial over F of degree n but no nonzero polynomial of lower degree.

THEOREM 5.1.3 *If $a \in K$ is algebraic of degree n over F, then $[F(a):F] = n$.*

This result adapts itself to many uses. We give now, as an immediate consequence thereof, the very interesting

THEOREM 5.1.4 *If a, b in K are algebraic over F then $a \pm b$, ab, and a/b (if $b \neq 0$) are all algebraic over F. In other words, the elements in K which are algebraic over F form a subfield of K.*

Proof. Suppose that a is algebraic of degree m over F while b is algebraic of degree n over F. By Theorem 5.1.3 the subfield $T = F(a)$ of K is of degree m over F. Now b is algebraic of degree n over F, *a fortiori* it is algebraic of degree at most n over T which contains F. Thus the subfield $W = T(b)$ of K, again by Theorem 5.1.3, is of degree at most n over T. But $[W:F] = [W:T][T:F]$ by Theorem 5.1.1; therefore, $[W:F] \leq mn$ and so W is a finite extension of F. However, a and b are both in W, whence all of $a \pm b$, ab, and a/b are in W. By Theorem 5.1.2, since $[W:F]$ is finite, these elements must be algebraic over F, thereby proving the theorem.

COROLLARY *If a and b in K are algebraic over F of degrees m and n, respectively, then $a \pm b$, ab, and a/b (if $b \neq 0$) are algebraic over F of degree at most mn.*

In the proof of the last theorem we made two extensions of the field F. The first we called T; it was merely the field $F(a)$. The second we called W and it was $T(b)$. Thus $W = (F(a))(b)$; it is customary to write it as $F(a, b)$. Similarly, we could speak about $F(b, a)$; it is not too difficult to prove that $F(a, b) = F(b, a)$. Continuing this pattern, we can define $F(a_1, a_2, \ldots, a_n)$ for elements $a_1, \ldots, a_n$ in K.

DEFINITION The extension K of F is called an *algebraic extension* of F if every element in K is algebraic over F.

THEOREM 5.1.5 *If L is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.*

Proof. Let u be any arbitrary element of L; our objective is to show that u satisfies some nontrivial polynomial with coefficients in F. What information do we have at present? We certainly do know that u satisfies some polynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$, where $\sigma_1, \ldots, \sigma_n$ are in K. But K is algebraic over F; therefore, by several uses of Theorem 5.1.3, $M = F(\sigma_1, \ldots, \sigma_n)$ is a finite extension of F. Since u satisfies the polynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$ whose coefficients are in M, u is algebraic over M. Invoking Theorem 5.1.2 yields that $M(u)$ is a finite extension of M. However, by Theorem 5.1.1, $[M(u):F] = [M(u):M][M:F]$, whence $M(u)$ is a finite extension of F. But this implies that u is algebraic over F, completing proof of the theorem.

A quick description of Theorem 5.1.5: algebraic over algebraic is algebraic.

The preceding results are of special interest in the particular case in which F is the field of rational numbers and K the field of complex numbers.

DEFINITION A complex number is said to be an *algebraic number* if it is algebraic over the field of rational numbers.

Roots of Polynomials

DEFINITION If $p(x) \in F[x]$, then an element a lying in some extension field of F is called a *root* of $p(x)$ if $p(a) = 0$.

We begin with the familiar result known as the *Remainder Theorem.*

LEMMA 5.3.1 *If $p(x) \in F[x]$ and if K is an extension of F, then for any element $b \in K$, $p(x) = (x - b)q(x) + p(b)$ where $q(x) \in K[x]$ and where* $\deg q(x) = \deg p(x) - 1$.

Proof. Since $F \subset K$, $F[x]$ is contained in $K[x]$, whence we can consider $p(x)$ to be lying in $K[x]$. By the division algorithm for polynomials in $K[x]$, $p(x) = (x - b)q(x) + r$, where $q(x) \in K[x]$ and where $r = 0$ or $\deg r < \deg (x - b) = 1$. Thus either $r = 0$ or $\deg r = 0$; in either case r must be an element of K. But exactly what element of K is it? Since $p(x) = (x - b)q(x) + r$, $p(b) = (b - b)q(b) + r = r$. Therefore, $p(x) = (x - b)q(x) + p(b)$. That the degree of $q(x)$ is one less than that of $p(x)$ is easy to verify and is left to the reader.

COROLLARY *If $a \in K$ is a root of $p(x) \in F[x]$, where $F \subset K$, then in $K[x]$,* $(x - a) \mid p(x)$.

Proof. From Lemma 5.3.1, in $K[x]$, $p(x) = (x - a)q(x) + p(a) = (x - a)q(x)$ since $p(a) = 0$. Thus $(x - a) \mid p(x)$ in $K[x]$.

DEFINITION The element $a \in K$ is a root of $p(x) \in F[x]$ of *multiplicity* m if $(x - a)^m \mid p(x)$, whereas $(x - a)^{m+1} \nmid p(x)$.

LEMMA 5.3.2 *A polynomial of degree n over a field can have at most n roots in any extension field.*

Proof. We proceed by induction on n, the degree of the polynomial $p(x)$. If $p(x)$ is of degree 1, then it must be of the form $\alpha x + \beta$ where α, β are in a field F and where $\alpha \neq 0$. Any a such that $p(a) = 0$ must then imply that $\alpha a + \beta = 0$, from which we conclude that $a = (-\beta/\alpha)$. That is, $p(x)$ has the unique root $-\beta/\alpha$, whence the conclusion of the lemma certainly holds in this case.

Assuming the result to be true in any field for all polynomials of degree less than n, let us suppose that $p(x)$ is of degree n over F. Let K be any extension of F. If $p(x)$ has no roots in K, then we are certainly done, for the number of roots in K, namely zero, is definitely at most n. So, suppose that $p(x)$ has at least one root $a \in K$ and that a is a root of multiplicity m. Since $(x-a)^m \mid p(x)$, $m \leq n$ follows. Now $p(x) = (x-a)^m q(x)$, where $q(x) \in K[x]$ is of degree $n-m$. From the fact that $(x-a)^{m+1} \nmid p(x)$, we get that $(x-a) \nmid q(x)$, whence, by the corollary to Lemma 5.3.1, a is not a root of $q(x)$. If $b \neq a$ is a root, in K, of $p(x)$, then $0 = p(b) = (b-a)^m q(b)$; however, since $b - a \neq 0$ and since we are in a field, we conclude that $q(b) = 0$. That is, any root of $p(x)$, in K, other than a, must be a root of $q(x)$. Since $q(x)$ is of degree $n - m < n$, by our induction hypothesis, $q(x)$ has at most $n - m$ roots in K, which, together with the other root a, counted m times, tells us that $p(x)$ has at most $m + (n - m) = n$ roots in K. This completes the induction and proves the lemma.

Proof. Let $F[x]$ be the ring of polynomials in x over F and let $V = (p(x))$ be the ideal of $F[x]$ generated by $p(x)$. By Lemma 3.9.6, V is a maximal ideal of $F[x]$, whence by Theorem 3.5.1, $E = F[x]/V$ is a field. This E will be shown to satisfy the conclusions of the theorem.

First we want to show that E is an extension of F; however, in fact, it is not! But let $\bar{F}$ be the image of F in E; that is, $\bar{F} = \{\alpha + V \mid \alpha \in F\}$. We assert that $\bar{F}$ is a field isomorphic to F; in fact, if ψ is the mapping from $F[x]$ into $F[x]/V = E$ defined by $f(x)\psi = f(x) + V$, then the restriction of ψ to F induces an isomorphism of F onto $\bar{F}$. (Prove!) Using this isomorphism, we identify F and $\bar{F}$; *in this way we can consider E to be an extension of F.*

We claim that E is a finite extension of F of degree $n = \deg p(x)$, for the elements $1 + V, x + V, (x+V)^2 = x^2 + V, \ldots, (x+V)^i = x^i + V, \ldots, (x+V)^{n-1} = x^{n-1} + V$ form a basis of E over F. (Prove!) For convenience of notation let us denote the element $x\psi = x + V$ in the field E as a. Given $f(x) \in F[x]$, what is $f(x)\psi$? We claim that it is merely $f(a)$, for, since ψ is a homomorphism, if $f(x) = \beta_0 + \beta_1 x + \cdots + \beta_k x^k$, then $f(x)\psi = \beta_0\psi + (\beta_1\psi)(x\psi) + \cdots + (\beta_k\psi)(x\psi)^k$, and using the identification indicated above of $\beta\psi$ with β, we see that $f(x)\psi = f(a)$.

In particular, since $p(x) \in V$, $p(x)\psi = 0$; however, $p(x)\psi = p(a)$. *Thus the element* $a = x\psi$ *in* E *is a root of* $p(x)$. The field E has been shown to satisfy all the properties required in the conclusion of Theorem 5.3.1, and so this theorem is now proved.

An immediate consequence of this theorem is the

COROLLARY *If* $f(x) \in F[x]$, *then there is a finite extension* E *of* F *in which* $f(x)$ *has a root. Moreover,* $[E:F] \leq \deg f(x)$.

Proof. Let $p(x)$ be an irreducible factor of $f(x)$; any root of $p(x)$ is a root of $f(x)$. By the theorem there is an extension E of F with $[E:F] = \deg p(x) \leq \deg f(x)$ in which $p(x)$, and so, $f(x)$ has a root.

Although it is, in actuality, a corollary to the above corollary, the next theorem is of such great importance that we single it out as a theorem.

THEOREM 5.3.2 *Let* $f(x) \in F[x]$ *be of degree* $n \geq 1$. *Then there is an extension* E *of* F *of degree at most* $n!$ *in which* $f(x)$ *has* n *roots (and so, a full complement of roots).*

Proof. In the statement of the theorem, a root of multiplicity m is, of course, counted as m roots.

By the above corollary there is an extension E_0 of F with $[E_0:F] \leq n$ in which $f(x)$ has a root α. Thus in $E_0[x]$, $f(x)$ factors as $f(x) = (x - \alpha)q(x)$, where $q(x)$ is of degree $n - 1$. Using induction (or continuing the above process), there is an extension E of E_0 of degree at most $(n - 1)!$ in which $q(x)$ has $n - 1$ roots. Since any root of $f(x)$ is either α or a root of $q(x)$, we obtain in E all n roots of $f(x)$. Now, $[E:F] = [E:E_0][E_0:F] \leq (n - 1)!n = n!$ All the pieces of the theorem are now established.

Theorem 5.3.2 asserts the existence of a finite extension E in which the given polynomial $f(x)$, of degree n, over F has n roots. If $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, $a_0 \neq 0$ and if the n roots in E are $\alpha_1, \ldots, \alpha_n$, making use of the corollary to Lemma 5.3.1, $f(x)$ can be factored over E as $f(x) = a_0(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$. Thus $f(x)$ splits up completely over E as a product of *linear* (first degree) factors. Since a finite extension of F exists with this property, a *finite extension of F of minimal degree* exists which also enjoys this property of decomposing $f(x)$ as a product of linear factors. For such a minimal extension, no proper subfield has the property that $f(x)$ factors over it into the product of linear factors. This prompts the

DEFINITION If $f(x) \in F[x]$, a finite extension E of F is said to be a *splitting field* over F for $f(x)$ if over E (that is, in $E[x]$), but not over any proper subfield of E, $f(x)$ can be factored as a product of linear factors.

LEMMA 5.3.3 *τ^* defines an isomorphism of $F[x]$ onto $F'[t]$ with the property that $\alpha\tau^* = \alpha'$ for every $\alpha \in F$.*

If $f(x)$ is in $F[x]$ we shall write $f(x)\tau^*$ as $f'(t)$. Lemma 5.3.3 immediately implies that factorizations of $f(x)$ in $F[x]$ result in like factorizations of $f'(t)$ in $F'[t]$, and vice versa. In particular, $f(x)$ is irreducible in $F[x]$ if and only if $f'(t)$ is irreducible in $F'[t]$.

However, at the moment, we are not particularly interested in polynomial rings, but rather, in extensions of F. Let us recall that in the proof of Theorem 5.1.2 we employed quotient rings of polynomial rings to obtain suitable extensions of F. In consequence it should be natural for us to study the relationship between $F[x]/(f(x))$ and $F'[t]/(f'(t))$, where $(f(x))$ denotes the ideal generated by $f(x)$ in $F[x]$ and $(f'(t))$ that generated by $f'(t)$ in $F'[t]$. The next lemma, which is relevant to this question, is actually part of a more general, purely ring-theoretic result, but we shall content ourselves with it as applied in our very special setting.

LEMMA 5.3.4 *There is an isomorphism τ^{**} of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$ with the property that for every $\alpha \in F$, $\alpha\tau^{**} = \alpha'$, $(x + (f(x)))\tau^{**} = t + (f'(t))$.*

Proof. Before starting with the proof proper, we should make clear what is meant by the last part of the statement of the lemma. As we have already done several times, we can consider F as imbedded in $F[x]/(f(x))$ by identifying the element $\alpha \in F$ with the coset $\alpha + (f(x))$ in $F[x]/(f(x))$. Similarly, we can consider F' to be contained in $F'[t]/(f'(t))$. The isomorphism τ^{**} is then supposed to satisfy $[\alpha + (f(x))]\tau^{**} = \alpha' + (f'(t))$.

We seek an isomorphism τ^{**} of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$. What could be simpler or more natural than to try the τ^{**} defined by $[g(x) + (f(x))]\tau^{**} = g'(t) + (f'(t))$ for every $g(x) \in F[x]$? We leave it as an exercise to fill in the necessary details that the τ^{**} so defined is well defined and is an isomorphism of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$ with the properties needed to fulfill the statement of Lemma 5.3.4.

THEOREM 5.3.3 *If $p(x)$ is irreducible in $F[x]$ and if v is a root of $p(x)$, then $F(v)$ is isomorphic to $F'(w)$ where w is a root of $p'(t)$; moreover, this isomorphism σ can so be chosen that*

1. $v\sigma = w$.
2. $\alpha\sigma = \alpha'$ *for every* $\alpha \in F$.

Proof. Let v be a root of the irreducible polynomial $p(x)$ lying in some extension K of F. Let $M = \{f(x) \in F[x] \mid f(v) = 0\}$. Trivially M is an ideal of $F[x]$, and $M \neq F[x]$. Since $p(x) \in M$ and is an irreducible polynomial, we have that $M = (p(x))$. As in the proof of Theorem 5.1.2, map $F[x]$ into $F(v) \subset K$ by the mapping ψ defined by $q(x)\psi = q(v)$ for every $q(x) \in F[x]$. We saw earlier (in the proof of Theorem 5.1.2) that ψ maps $F[x]$ onto $F(v)$. The kernel of ψ is precisely M, so must be $(p(x))$. By the fundamental homomorphism theorem for rings there is an isomorphism ψ^* of $F[x]/(p(x))$ onto $F(v)$. Note further that $\alpha\psi^* = \alpha$ for every $\alpha \in F$. Summing up: ψ^* is an isomorphism of $F[x]/(p(x))$ onto $F(v)$ leaving every element of F fixed and with the property that $v = [x + (p(x))]\psi^*$.

Since $p(x)$ is irreducible in $F[x]$, $p'(t)$ is irreducible in $F'[t]$ (by Lemma 5.3.3), and so there is an isomorphism θ^* of $F'[t]/(p'(t))$ onto $F'(w)$ where w is a root of $p'(t)$ such that θ^* leaves every element of F' fixed and such that $[t + (p'(t)]\theta^* = w$.

We now stitch the pieces together to prove Theorem 5.3.3. By Lemma 5.3.4 there is an isomorphism τ^{**} of $F[x]/(p(x))$ onto $F'[t]/(p'(t))$ which coincides with τ on F and which takes $x + (p(x))$ onto $t + (p'(t))$. Consider the mapping $\sigma = (\psi^*)^{-1}\tau^{**}\theta^*$ (motivated by

$$F(v) \xrightarrow{(\psi^*)^{-1}} \frac{F[x]}{(p(x))} \xrightarrow{\tau^{**}} \frac{F'[t]}{(p'(t))} \xrightarrow{\theta^*} F'(w))$$

of $F(v)$ onto $F'(w)$. It is an isomorphism of $F(v)$ onto $F'(w)$ since all the mapping ψ^*, τ^{**}, and θ^* are isomorphisms and onto. Moreover, since $v = [x + (p(x))]\psi^*$, $v\sigma = (v(\psi^*)^{-1})\tau^{**}\theta^* = ([x + (p(x)]\tau^{**})\theta^* = [t + (p'(t))]\theta^* = w$. Also, for $\alpha \in F$, $\alpha\sigma = (\alpha(\psi^*)^{-1})\tau^{**}\theta^* = (\alpha\tau^{**})\theta^* = \alpha'\theta^* = \alpha'$. We have shown that σ is an isomorphism satisfying all the requirements of the isomorphism in the statement of the theorem. Thus Theorem 5.3.3 has been proved.

COROLLARY *If $p(x) \in F[x]$ is irreducible and if a, b are two roots of $p(x)$, then $F(a)$ is isomorphic to $F(b)$ by an isomorphism which takes a onto b and which leaves every element of F fixed.*

The Elements of Galois Theory

THEOREM 5.6.1 *If K is a field and if $\sigma_1, \ldots, \sigma_n$ are distinct automorphisms of K, then it is impossible to find elements $a_1, \ldots, a_n$, not all 0, in K such that $a_1\sigma_1(u) + a_2\sigma_2(u) + \cdots + a_n\sigma_n(u) = 0$ for all $u \in K$.*

Proof. Suppose we could find a set of elements $a_1, \ldots, a_n$ in K, not all 0, such that $a_1\sigma_1(u) + \cdots + a_n\sigma_n(u) = 0$ for all $u \in K$. Then we could find such a relation having as few nonzero terms as possible; on renumbering we can assume that this minimal relation is

$$a_1\sigma_1(u) + \cdots + a_m\sigma_m(u) = 0 \tag{1}$$

where $a_1, \ldots, a_m$ are all different from 0.

If m were equal to 1 then $a_1\sigma_1(u) = 0$ for all $u \in K$, leading to $a_1 = 0$, contrary to assumption. Thus we may assume that $m > 1$. Since the automorphisms are distinct there is an element $c \in K$ such that $\sigma_1(c) \neq \sigma_m(c)$. Since $cu \in K$ for all $u \in K$, relation (1) must also hold for cu, that is, $a_1\sigma_1(cu) + a_2\sigma_2(cu) + \cdots + a_m\sigma_m(cu) = 0$ for all $u \in K$. Using the hypothesis that the σ's are automorphisms of K, this relation becomes

$$a_1\sigma_1(c)\sigma_1(u) + a_2\sigma_2(c)\sigma_2(u) + \cdots + a_m\sigma_m(c)\sigma_m(u) = 0. \tag{2}$$

Multiplying relation (1) by $\sigma_1(c)$ and subtracting the result from (2) yields

$$a_2(\sigma_2(c) - \sigma_1(c))\sigma_2(u) + \cdots + a_m(\sigma_m(c) - \sigma_1(c))\sigma_m(u) = 0. \tag{3}$$

If we put $b_i = a_i(\sigma_i(c) - \sigma_1(c))$ for $i = 2, \ldots, m$, then the b_i are in K, $b_m = a_m(\sigma_m(c) - \sigma_1(c)) \neq 0$, since $a_m \neq 0$, and $\sigma_m(c) - \sigma_1(c) \neq 0$ yet $b_2\sigma_2(u) + \cdots + b_m\sigma_m(u) = 0$ for all $u \in K$. This produces a shorter relation, contrary to the choice made; thus the theorem is proved.

DEFINITION If G is a group of automorphisms of K, then the *fixed field* of G is the set of all elements $a \in K$ such that $\sigma(a) = a$ for all $\sigma \in G$.

LEMMA 5.6.1 *The fixed field of G is a subfield of K.*

Proof. Let a, b be in the fixed field of G. Thus for all $\sigma \in G$, $\sigma(a) = a$ and $\sigma(b) = b$. But then $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b$ and $\sigma(ab) = \sigma(a)\sigma(b) = ab$; hence $a \pm b$ and ab are again in the fixed field of G. If $b \neq 0$, then $\sigma(b^{-1}) = \sigma(b)^{-1} = b^{-1}$, hence b^{-1} also falls in the fixed field of G. Thus we have verified that the fixed field of G is indeed a subfield of K.

DEFINITION Let K be a field and let F be a subfield of K. Then the *group of automorphisms of K relative to F*, written $G(K, F)$, is the set of *all* automorphisms of K leaving every element of F fixed; that is, the automorphism σ of K is in $G(K, F)$ if and only if $\sigma(\alpha) = \alpha$ for every $\alpha \in F$.

THEOREM 5.6.2 *If K is a finite extension of F, then $G(K, F)$ is a finite group and its order, $o(G(K, F))$ satisfies $o(G(K, F)) \leq [K:F]$.*

Proof. Let $[K:F] = n$ and suppose that $u_1, \ldots, u_n$ is a basis of K over F. Suppose we can find $n + 1$ distinct automorphisms $\sigma_1, \sigma_2, \ldots, \sigma_{n+1}$

in $G(K, F)$. By the corollary to Theorem 4.3.3 the system of n homogeneous linear equations in the $n + 1$ unknowns $x_1, \ldots, x_{n+1}$:

$$\begin{aligned}
&\sigma_1(u_1)x_1 + \sigma_2(u_1)x_2 + \cdots + \sigma_{n+1}(u_1)x_{n+1} = 0 \\
&\vdots \\
&\sigma_1(u_i)x_1 + \sigma_2(u_i)x_2 + \cdots + \sigma_{n+1}(u_i)x_{n+1} = 0 \\
&\vdots \\
&\sigma_1(u_n)x_1 + \sigma_2(u_n)x_2 + \cdots + \sigma_{n+1}(u_n)x_{n+1} = 0
\end{aligned}$$

has a nontrivial solution (not all 0) $x_1 = a_1, \ldots, x_{n+1} = a_{n+1}$ in K. Thus

$$a_1\sigma_1(u_i) + a_2\sigma_2(u_i) + \cdots + a_{n+1}\sigma_{n+1}(u_i) = 0 \qquad (1)$$

for $i = 1, 2, \ldots, n$.

Since every element in F is left fixed by each σ_i and since an arbitrary element t in K is of the form $t = \alpha_1 u_1 + \cdots + \alpha_n u_n$ with $\alpha_1, \ldots, \alpha_n$ in F, then from the system of equations (1) we get $a_1\sigma_1(t) + \cdots + a_{n+1}\sigma_{n+1}(t) = 0$ for all $t \in K$. But this contradicts the result of Theorem 5.6.1. Thus Theorem 5.6.2 has been proved.

Theorem 5.6.2 is of central importance in the Galois theory. However, aside from its key role there, it serves us well in proving a classic result concerned with symmetric rational functions. This result on symmetric functions in its turn will play an important part in the Galois theory.

First a few remarks on the field of rational functions in n-variables over a field F. Let us recall that in Section 3.11 we defined the ring of polynomials in the n-variables $x_1, \ldots, x_n$ over F and from this defined the field of rational functions in $x_1, \ldots, x_n$, $F(x_1, \ldots, x_n)$, over F as the ring of all quotients of such polynomials.

DEFINITION K is a *normal extension* of F if K is a finite extension of F such that F is the fixed field of $G(K, F)$.

Possible Questions

PART-B (6 Mark)

1. Prove that a polynomial of degree n over a field can have at most n roots in any extension field.
2. Show that if L is a finite extension of K and if K is a finite extension of F, then prove that L is a finite extension of F. Moreover [L: F] = [L: K] [K: F].
3. Show that if K is a finite extension of F, then G(K,F) is a finite group and its order. O(G(K,F)) satisfies O(G(K,F)) [K:F].
4. State and prove Remainder theorem.
5. Prove that the element a $\in$K is algebraic over F if and only if F(a) is a finite extension of F.
6. If p(x) is irreducible in F[x] and if v is a root of p(x), then F[v] is isomorphic to F'[w] where w is a root of p'(t); moreover, this isomorphism σ can so be chosen that

i. v σ = w
ii. α σ = α' for every $\alpha \epsilon$ F.

7. Show that the element a K is algebraic over F if and only if F(a) is a finite extension of F.
8. Prove that if P(x) ϵF[x] and if K is an extension of F, then for any element b ϵ K,
9. P(x) = (x-b) q(x) + p(b) where q(x) ϵ K[x] and where deg q(x) ϵ K[x] and where degq(x) = deg p(x)-1.
10. Prove that the polynomial f(x) $\in$F(x) has a multiple root if and only if f(x) and f'(x) have a nontrivial common factor.

PART-C (10 Mark)

1. State and prove Division Algorithm.
2. Show that if K is a finite extension of F, then G(K,F) is a finite group and its order. O(G(K,F)) satisfies O(G(K,F)) [K:F].

KARPAGAM ACADEMY OF HIGHER EDUCATION
DEPARTMENT OF MATHEMATICS
ALBEBRA (18MMP101)

UNIT - III

Questions	choice 1	choice 2	choice 3	choice 4	Answer
A field K is said to be an extension of F if ----------	F⊆K	F=K	K⊆F	F<K	F⊆K
A field K is said to be an ---------- F if F⊆K	zero divisor	primitive	irreducible	extension	extension
The ---------- is the dimension of K as a vector space over F	degree of F over K	degree of K over F	degree of F	none	degree of K over F
The degree of K over F is the ---------- of K as a vector space over F	degree of F over K	dimension	degree of F	none	dimension
If L is a finite extension of K and K is a finite extension of F,then---- --------	L is a finite extension of K	K is a finite extension of K	L is a finite extension of F	K is a finite extension of L	L is a finite extension of F
If---------- and K is a finite extension of F,then L is a finite extension of F	L is a finite extension of K	K is a finite extension of K	L is a finite extension of F	K is a finite extension of L	L is a finite extension of K
If L is a finite extension of K and ---------- ,then L is a finite extension of F	L is a finite extension of K	K is a finite extension of F	L is a finite extension of F	K is a finite extension of L	K is a finite extension of F
If a∈K is algebraic of degree n over F,then ----------	[F(a):F] = n	[F(a):F] =m	[F(a):F] =0	[F(a):F] = a	[F(a):F] = n
If a∈K is ----------,then [F(a):F] = n	algebraic of degree n over F	algebraic of degree n over F	algebraic of degree n over F	algebraic of degree n over F	algebraic of degree n over F
If a and b in K are ----------F then a+b, a-b, ab, a/b are all algebraic over F	algebraic over K	algebraic over F	algebraic of degree F	algebraicof degree K	algebraic over F
The elements in K which are algebraic over F form a ---------of K	field	subfield	root	group	subfield
If α is constructible then α lies in some extension of the rationals of degree ------	power of 2	power of 3	not a power of 3	not a power of 2	power of 2
If the ----------α satisfies an irreducible polynomial over the field of rational numbers of degree k,and if k is not a power of 2 ,then α is not constuctible.	real number	rational number	irrational number	complex number	real number
If the real number α satisfies an irreducible polynomial over the field of rational numbers of degree k,and if k is----------,then α is not constuctible.	power of 2	power of 3	not a power of 3	not a power of 2	not a power of 2
G(K,F) is a ---------- of the group of all automorphisms of K	group	sub group	normal subgroup	none	sub group
If U is an ideal of the ring Rthen R/U is a ---------- and is a homomorphic image of R	field	group	sub group	ring	ring
If U is an ideal of the ring Rthen R/U is a ring and is a ---------- image of R	homomorphic	isomorphic	homeomorphic	automorphic	homomorphic
If U is --------- of the ring Rthen R/U is a ring and is a homomorphic image of R	group	ring	ideal	field	ideal
If R is a commutative ring with a unit element and M is an ---------- of R then M is a maximal ideal of R iff R/M is a field	group	ring	ideal	field	ideal
If R is a commutative ring with a unit element and M is an ideal of R then M is a maximal ideal of R iff R/M is a -------	group	ring	ideal	field	field
If R is a commutative ring with a unit element and M is an ideal of R then M is a ---------- of R iff R/M is a field	maximal ideal	ring	ideal	minimal ideal	maximal ideal
If R is a commutative ring with a unit element and M is an ideal of R then M is a maximal ideal of R iff--------- is a field	R	R/M	R and M	M	R/M
Every -------- can be imbedded in a field	integral domaim	ring	ideal	field	integral domaim
Every integral domaim can be imbedded in a ----------	integral domaim	ring	ideal	field	field
A---------- possesses a unit element	integral domain	ring	ideal	Eucledian ring	Eucledian ring
If --------- U of a ring R contains a unit of R then U=R	Euclidean ring	ring	ideal	field	ideal
If an ideal U of a --------- R contains a unit of R then U=R	Euclidean ring	ring	field	ideal	ring
If an ideal U of a ring R contains a unit of R then--------	U=R	U<R	U>R	U≤R	U=R
A --------- said to be generating set of V if L(S) = V.	set S	ring	ideal U	Euclidean ring	set S
A set S said to be ---------- of V if L(S) = V.	maximal ideal	ideal	generating set	field	generating set
A set S said to be generating set of V if --------.	L(S) = V	L(S) = 0	L(V) =S	L(S) = 1	L(S) = V

Any ---------- F is a finite extension of F.	ring	field	ideal	group	field
Any field F is a ----------of F.	primitive	irreducible	extension	finite extension	finite extension
An element a ∈k is said to be ---------- over F if it is not algebraic over F	generating set	transcendental	extension	finite extension	transcendental
An element a ∈k is said to be transcendental over F if it is ----------	not algebraic over F	algebraic over F	finite extension of L	not a finite extension of L	not algebraic over F
A ---------- K is said to be an extension F if F⊆K	field	ring	ideal	group	field
A ---------- is said to be an algebraic number if it is algebraic over field of rational number.	real number	rational number	irrational number	complex number	complex number
A complex number is said to be an ---------- if it is algebraic over field of rational number.	rational number	irrational number	algebraic number	real number	algebraic number
A complex number is said to be an algebraic number if it is ---------- over field of rational number.	real	algebraic	integers	rational	algebraic
A complex number is said to be an algebraic number if it is algebraic over ----- of rational number.	field	ring	ideal	group	field
A complex number is said to be an algebraic number if it is algebraic over field of ----------.	real number	irrational number	rational number	algebraic number	rational number
An ---------- of a fields F is said to be simple extension if k = F(a) for some a∈k	Euclidean ring R	transcendental k	extension k	finite extension k	extension k
An extension k of a fields F is said to be ---------- if k = F(a) for some a∈k	Euclidean ring	transcendental	extension	simple extension	simple extension
An extension k of a fields F is said to be simple extension if ---------- for some a∈k	k = F(0)	k = F(a)	k = F(1)	k = F(a *1)	k = F(a)
A ---------- is called Prefect if all its Finite extension of F is separable.	field	ring	ideal	group	field
A field F is called ----------if all its Finite extension of F is separable.	algebraic	Prefect	prime	normal	Prefect
A field F is called Prefect if all its---------- of F is separable.	primitive	irreducible	extension	finite extension	finite extension
A field F is called Prefect if all its Finite extension of F is ----------	irreducible	transcendental	separable	inseparable	separable

UNIT-IV

Linear Transformations-The Algebra Of Linear Transformation – Characteristic Root-Matrices-Canonical Forms –Triangular form-Nilpotent Transformations–Jordan form.

DEFINITION Let K be a field and let F be a subfield of K. Then the *group of automorphisms of K relative to F*, written $G(K, F)$, is the set of *all* automorphisms of K leaving every element of F fixed; that is, the automorphism σ of K is in $G(K, F)$ if and only if $\sigma(\alpha) = \alpha$ for every $\alpha \in F$.

DEFINITION K is a *normal extension* of F if K is a finite extension of F such that F is the fixed field of $G(K, F)$.

DEFINITION If $f(x) \in F[x]$, a finite extension E of F is said to be a *splitting field* over F for $f(x)$ if over E (that is, in $E[x]$), but not over any proper subfield of E, $f(x)$ can be factored as a product of linear factors.

DEFINITION If $p(x) \in F[x]$, then an element a lying in some extension field of F is called a *root* of $p(x)$ if $p(a) = 0$.

The Algebra of Linear Transformations

For $T_1, T_2 \in \text{Hom}(V, V)$, since $vT_1 \in V$ for any $v \in V$, $(vT_1)T_2$ makes sense. As we have done for mappings of any set into itself, we define T_1T_2 by $v(T_1T_2) = (vT_1)T_2$ for any $v \in V$. We now claim that $T_1T_2 \in \text{Hom}(V, V)$. To prove this, we must show that for all $\alpha, \beta \in F$ and all $u, v \in V$, $(\alpha u + \beta v)(T_1T_2) = \alpha(u(T_1T_2)) + \beta(v(T_1T_2))$. We compute

$$\begin{aligned}(\alpha u + \beta v)(T_1T_2) &= ((\alpha u + \beta v)T_1)T_2 \\ &= (\alpha(uT_1) + \beta(vT_1))T_2 \\ &= \alpha(uT_1)T_2 + \beta(vT_1)T_2 \\ &= \alpha(u(T_1T_2)) + \beta(v(T_1T_2)).\end{aligned}$$

We leave as an exercise the following properties of this product in $\text{Hom}(V, V)$:

1. $(T_1 + T_2)T_3 = T_1T_3 + T_2T_3$;
2. $T_3(T_1 + T_2) = T_3T_1 + T_3T_2$;
3. $T_1(T_2T_3) = (T_1T_2)T_3$;
4. $\alpha(T_1T_2) = (\alpha T_1)T_2 = T_1(\alpha T_2)$;

for all $T_1, T_2, T_3 \in \text{Hom}(V, V)$ and all $\alpha \in F$.

Note that properties 1, 2, 3, above, are exactly what are required to make of $\text{Hom}(V, V)$ an associative ring. Property 4 intertwines the character of $\text{Hom}(V, V)$, as a vector space over F, with its character as a ring.

DEFINITION A *linear transformation* on V, over F, is an element of $A_F(V)$.

We shall, at times, refer to $A(V)$ as the *ring, or algebra, of linear transformations on* V.

DEFINITION An associative ring A is called an *algebra* over F if A is a vector space over F such that for all $a, b \in A$ and $\alpha \in F$, $\alpha(ab) = (\alpha a)b = a(\alpha b)$.

LEMMA 6.1.1 *If A is an algebra, with unit element, over F, then A is isomorphic to a subalgebra of $A(V)$ for some vector space V over F.*

Proof. Since A is an algebra over F, it must be a vector space over F. We shall use $V = A$ to prove the theorem.

If $a \in A$, let $T_a: A \to A$ be defined by $vT_a = va$ for every $v \in A$. We assert that T_a is a linear transformation on $V(=A)$. By the right-distributive law $(v_1 + v_2)T_a = (v_1 + v_2)a = v_1a + v_2a = v_1T_a + v_2T_a$. Since A is an algebra, $(\alpha v)T_a = (\alpha v)a = \alpha(va) = \alpha(vT_a)$ for $v \in A$, $\alpha \in F$. Thus T_a is indeed a linear transformation on A.

Consider the mapping $\psi: A \to A(V)$ defined by $a\psi = T_a$ for every $a \in A$. We claim that ψ is an isomorphism of A into $A(V)$. To begin with, if $a, b \in A$ and $\alpha, \beta \in F$, then for all $v \in A$, $vT_{\alpha a+\beta b} = v(\alpha a + \beta b) = \alpha(va) + \beta(vb)$ [by the left-distributive law and the fact that A is an algebra over F] $= \alpha(vT_a) + \beta(vT_b) = v(\alpha T_a + \beta T_b)$ since both T_a and T_b are linear transformations. In consequence, $T_{\alpha a+\beta b} = \alpha T_a + \beta T_b$, whence ψ is a vector-space homomorphism of A into $A(V)$. Next, we compute, for

$a, b \in A$, $vT_{ab} = v(ab) = (va)b = (vT_a)T_b = v(T_aT_b)$ (we have used the associative law of A in this computation), which implies that $T_{ab} = T_aT_b$. In this way, ψ is also a ring-homomorphism of A. So far we have proved that ψ is a homomorphism of A, as an algebra, into $A(V)$. All that remains is to determine the kernel of ψ. Let $a \in A$ be in the kernel of ψ; then $a\psi = 0$, whence $T_a = 0$ and so $vT_a = 0$ for all $v \in V$. Now $V = A$, and A has a unit element, e, hence $eT_a = 0$. However, $0 = eT_a = ea = a$, proving that $a = 0$. The kernel of ψ must therefore merely consist of 0, thus implying that ψ is an isomorphism of A into $A(V)$. This completes the proof of the lemma.

LEMMA 6.1.2 *Let A be an algebra, with unit element, over F, and suppose that A is of dimension m over F. Then every element in A satisfies some nontrivial polynomial in $F[x]$ of degree at most m.*

Proof. Let e be the unit element of A; if $a \in A$, consider the $m + 1$ elements $e, a, a^2, \ldots, a^m$ in A. Since A is m-dimensional over F, by Lemma 4.2.4, $e, a, a^2, \ldots, a^m$, being $m + 1$ in number, must be linearly dependent over F. In other words, there are elements $\alpha_0, \alpha_1, \ldots, \alpha_m$ in F, not all 0, such that $\alpha_0 e + \alpha_1 a + \cdots + \alpha_m a^m = 0$. But then a satisfies the non-trivial polynomial $q(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$, of degree at most m, in $F[x]$.

If V is a finite-dimensional vector space over F, of dimension n, by Corollary 1 to Theorem 4.3.1, $A(V)$ is of dimension n^2 over F. Since $A(V)$ is an algebra over F, we can apply Lemma 6.1.2 to it to obtain that every element in $A(V)$ satisfies a polynomial over F of degree at most n^2. This fact will be of central significance in all that follows, so we single it out as

THEOREM 6.1.1 *If V is an n-dimensional vector space over F, then, given any element T in $A(V)$, there exists a nontrivial polynomial $q(x) \in F[x]$ of degree at most n^2, such that $q(T) = 0$.*

DEFINITION An element $T \in A(V)$ is called *right-invertible* if there exists an $S \in A(V)$ such that $TS = 1$. (Here 1 denotes the unit element of $A(V)$.)

Similarly, we can define left-invertible, if there is a $U \in A(V)$ such that $UT = 1$. If T is both right- and left-invertible and if $TS = UT = 1$, it is an easy exercise that $S = U$ and that S is unique.

DEFINITION An element T in $A(V)$ is *invertible* or *regular* if it is both right- and left-invertible; that is, if there is an element $S \in A(V)$ such that $ST = TS = 1$. We write S as T^{-1}.

THEOREM 6.1.2 *If V is finite-dimensional over F, then $T \in A(V)$ is invertible if and only if the constant term of the minimal polynomial for T is not 0.*

Proof. Let $p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_k x^k$, $\alpha_k \neq 0$, be the minimal polynomial for T over F.

If $\alpha_0 \neq 0$, since $0 = p(T) = \alpha_k T^k + \alpha_{k-1} T^{k-1} + \cdots + \alpha_1 T + \alpha_0$, we obtain

$$1 = T\left(-\frac{1}{\alpha_0} (\alpha_k T^{k-1} + \alpha_{k-1} T^{k-2} + \cdots + \alpha_1) \right)$$
$$= \left(-\frac{1}{\alpha_0} (\alpha_k T^{k-1} + \cdots + \alpha_1) \right) T.$$

Therefore,

$$S = -\frac{1}{\alpha_0} (\alpha_k T^{k-1} + \cdots + \alpha_1)$$

acts as an inverse for T, whence T is invertible.

Suppose, on the other hand, that T is invertible, yet $\alpha_0 = 0$. Thus $0 = \alpha_1 T + \alpha_2 T^2 + \cdots + \alpha_k T^k = (\alpha_1 + \alpha_2 T + \cdots + \alpha_k T^{k-1}) T$. Multiplying this relation from the right by T^{-1} yields $\alpha_1 + \alpha_2 T + \cdots + \alpha_k T^{k-1} = 0$, whereby T satisfies the polynomial $q(x) = \alpha_1 + \alpha_2 x + \cdots + \alpha_k x^{k-1}$ in $F[x]$. Since the degree of $q(x)$ is less than that of $p(x)$, this is impossible. Consequently, $\alpha_0 \neq 0$ and the other half of the theorem is established.

COROLLARY 1 *If V is finite-dimensional over F and if $T \in A(V)$ is invertible, then T^{-1} is a polynomial expression in T over F.*

Proof. Since T is invertible, by the theorem, $\alpha_0 + \alpha_1 T + \cdots + \alpha_k T^k = 0$ with $\alpha_0 \neq 0$. But then

$$T^{-1} = -\frac{1}{\alpha_0} (\alpha_1 + \alpha_2 T + \cdots + \alpha_k T^{k-1}).$$

COROLLARY 2 *If V is finite-dimensional over F and if $T \in A(V)$ is singular, then there exists an $S \neq 0$ in $A(V)$ such that $ST = TS = 0$.*

Proof. Because T is not regular, the constant term of its minimal polynomial must be 0. That is, $p(x) = \alpha_1 x + \cdots + \alpha_k x^k$, whence $0 = \alpha_1 T + \cdots + \alpha_k T^k$. If $S = \alpha_1 + \cdots + \alpha_k T^{k-1}$, then $S \neq 0$ (since $\alpha_1 + \cdots + \alpha_k x^{k-1}$ is of lower degree than $p(x)$) and $ST = TS = 0$.

COROLLARY 3 *If V is finite-dimensional over F and if $T \in A(V)$ is right-invertible, then it is invertible.*

Proof. Let $TU = 1$. If T were singular, there would be an $S \neq 0$ such that $ST = 0$. However, $0 = (ST)U = S(TU) = S1 = S \neq 0$, a contradiction. Thus T is regular.

THEOREM 6.1.3 *If V is finite-dimensional over F, then $T \in A(V)$ is singular if and only if there exists a $v \neq 0$ in V such that $vT = 0$.*

Proof. By Corollary 2 to Theorem 6.1.2, T is singular if and only if there is an $S \neq 0$ in $A(V)$ such that $ST = TS = 0$. Since $S \neq 0$ there is an element $w \in V$ such that $wS \neq 0$.

Let $v = wS$; then $vT = (wS)T = w(ST) = w0 = 0$. We have produced a nonzero vector v in V which is annihilated by T. Conversely, if $vT = 0$ with $v \neq 0$, we leave as an exercise the fact that T is not invertible.

DEFINITION If $T \in A(V)$, then the *range* of T, VT, is defined by $VT = \{vT \mid v \in V\}$.

The range of T is easily shown to be a subvector space of V. It merely consists of all the images by T of the elements of V. Note that the range of T is all of V if and only if T is onto.

THEOREM 6.1.4 *If V is finite-dimensional over F, then $T \in A(V)$ is regular if and only if T maps V onto V.*

Proof. As happens so often, one-half of this is almost trivial; namely, if T is regular then, given $v \in V$, $v = (vT^{-1})T$, whence $VT = V$ and T is onto.

On the other hand, suppose that T is not regular. We must show that T is not onto. Since T is singular, by Theorem 6.1.3, there exists a vector $v_1 \neq 0$ in V such that $v_1 T = 0$. By Lemma 4.2.5 we can fill out, from v_1, to a basis $v_1, v_2, \ldots, v_n$ of V. Then every element in VT is a linear combination of the elements $w_1 = v_1 T$, $w_2 = v_2 T, \ldots, w_n = v_n T$. Since $w_1 = 0$, VT is spanned by the $n - 1$ elements $w_2, \ldots, w_n$; therefore $\dim VT \leq n - 1 < n = \dim V$. But then VT must be different from V; that is, T is not onto.

Theorem 6.1.4 points out that we can distinguish regular elements from singular ones, in the finite-dimensional case, according as their ranges are or are not all of V. If $T \in A(V)$ this can be rephrased as: T is regular if and only if $\dim(VT) = \dim V$. This suggests that we could use $\dim(VT)$ not only as a test for regularity, but even as a measure of the degree of singularity (or, lack of regularity) for a given $T \in A(V)$.

DEFINITION If V is finite-dimensional over F, then the *rank* of T is the dimension of VT, the range of T, over F.

LEMMA 6.1.3 *If V is finite-dimensional over F then for $S, T \in A(V)$.*

1. $r(ST) \leq r(T)$;
2. $r(TS) \leq r(T)$;

(*and so*, $r(ST) \leq \min\{r(T), r(S)\}$)

3. $r(ST) = r(TS) = r(T)$ *for S regular in $A(V)$.*

Proof. We go through 1, 2, and 3 in order.

1. Since $VS \subset V$, $V(ST) = (VS)T \subset VT$, whence, by Lemma 4.2.6, $\dim(V(ST)) \leq \dim VT$; that is, $r(ST) \leq r(T)$.

2. Suppose that $r(T) = m$. Therefore, VT has a basis of m elements, $w_1, w_2, \ldots, w_m$. But then $(VT)S$ is spanned by $w_1S, w_2S, \ldots, w_mS$, hence has dimension at most m. Since $r(TS) = \dim(V(TS)) = \dim((VT)S) \leq m = \dim VT = r(T)$, part 2 is proved.

3. If S is invertible then $VS = V$, whence $V(ST) = (VS)T = VT$. Thereby, $r(ST) = \dim(V(ST)) = \dim(VT) = r(T)$. On the other hand, if VT has $w_1, \ldots, w_m$ as a basis, the regularity of S implies that $w_1S, \ldots, w_mS$ are linearly independent. (Prove!) Since these span $V(TS)$ they form a basis of $V(TS)$. But then $r(TS) = \dim(V(TS)) = \dim(VT) = r(T)$.

COROLLARY *If $T \in A(V)$ and if $S \in A(V)$ is regular, then $r(T) = r(STS^{-1})$.*

Proof. By part 3 of the lemma, $r(STS^{-1}) = r(S(TS^{-1})) = r((TS^{-1})S) = r(T)$.

Characteristic Roots

DEFINITION If $T \in A(V)$ then $\lambda \in F$ is called a *characteristic root* (or *eigenvalue*) of T if $\lambda - T$ is singular.

THEOREM 6.2.1 *The element $\lambda \in F$ is a characteristic root of $T \in A(V)$ if and only if for some $v \neq 0$ in V, $vT = \lambda v$.*

Proof. If λ is a characteristic root of T then $\lambda - T$ is singular, whence, by Theorem 6.1.3, there is a vector $v \neq 0$ in V such that $v(\lambda - T) = 0$. But then $\lambda v = vT$.

On the other hand, if $vT = \lambda v$ for some $v \neq 0$ in V, then $v(\lambda - T) = 0$, whence, again by Theorem 6.1.3, $\lambda - T$ must be singular, and so, λ is a characteristic root of T.

LEMMA 6.2.1 *If $\lambda \in F$ is a characteristic root of $T \in A(V)$, then for any polynomial $q(x) \in F[x]$, $q(\lambda)$ is a characteristic root of $q(T)$.*

Proof. Suppose that $\lambda \in F$ is a characteristic root of T. By Theorem 6.2.1, there is a nonzero vector v in V such that $vT = \lambda v$. What about vT^2?

Now $vT^2 = (\lambda v)T = \lambda(vT) = \lambda(\lambda v) = \lambda^2 v$. Continuing in this way, we obtain that $vT^k = \lambda^k v$ for all positive integers k. If $q(x) = \alpha_0 x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$, $\alpha_i \in F$, then $q(T) = \alpha_0 T^m + \alpha_1 T^{m-1} + \cdots + \alpha_m$, whence $vq(T) = v(\alpha_0 T^m + \alpha_1 T^{m-1} + \cdots + \alpha_m) = \alpha_0(vT^m) + \alpha_1(vT^{m-1}) + \cdots + \alpha_m v = (\alpha_0 \lambda^m + \alpha_1 \lambda^{m-1} + \cdots + \alpha_m)v = q(\lambda)v$ by the remark made above. Thus $v(q(\lambda) - q(T)) = 0$, hence, by Theorem 6.2.1, $q(\lambda)$ is a characteristic root of $q(T)$.

THEOREM 6.2.2 *If $\lambda \in F$ is a characteristic root of $T \in A(V)$, then λ is a root of the minimal polynomial of T. In particular, T only has a finite number of characteristic roots in F.*

Proof. Let $p(x)$ be the minimal polynomial over F of T; thus $p(T) = 0$. If $\lambda \in F$ is a characteristic root of T, there is a $v \neq 0$ in V with $vT = \lambda v$. As in the proof of Lemma 6.2.1, $vp(T) = p(\lambda)v$; but $p(T) = 0$, which thus implies that $p(\lambda)v = 0$. Since $v \neq 0$, by the properties of a vector space, we must have that $p(\lambda) = 0$. Therefore, λ is a root of $p(x)$. Since $p(x)$ has only a finite number of roots (in fact, since $\deg p(x) \leq n^2$ where $n = \dim_F V$, $p(x)$ has at most n^2 roots) in F, there can only be a finite number of characteristic roots of T in F.

If $T \in A(V)$ and if $S \in A(V)$ is regular, then $(STS^{-1})^2 = STS^{-1}STS^{-1} = ST^2S^{-1}$, $(STS^{-1})^3 = ST^3S^{-1}, \ldots, (STS^{-1})^i = ST^iS^{-1}$. Consequently, for any $q(x) \in F[x]$, $q(STS^{-1}) = Sq(T)S^{-1}$. In particular, if $q(T) = 0$, then $q(STS^{-1}) = 0$. Thus if $p(x)$ is the minimal polynomial for T, then it follows easily that $p(x)$ is also the minimal polynomial for STS^{-1}. We have proved

LEMMA 6.2.2 *If $T, S \in A(V)$ and if S is regular, then T and STS^{-1} have the same minimal polynomial.*

DEFINITION The element $0 \neq v \in V$ is called a *characteristic vector* of T belonging to the characteristic root $\lambda \in F$ if $vT = \lambda v$.

THEOREM 6.2.3 *If $\lambda_1, \ldots, \lambda_k$ in F are distinct characteristic roots of $T \in A(V)$ and if $v_1, \ldots, v_k$ are characteristic vectors of T belonging to $\lambda_1, \ldots, \lambda_k$, respectively, then $v_1, \ldots, v_k$ are linearly independent over F.*

Proof. For the theorem to require any proof, k must be larger than 1; so we suppose that $k > 1$.

If $v_1, \ldots, v_k$ are linearly dependent over F, then there is a relation of the form $\alpha_1 v_1 + \cdots + \alpha_k v_k = 0$, where $\alpha_1, \ldots, \alpha_k$ are all in F and not all of them are 0. In all such relations, there is one having as few nonzero coefficients as possible. By suitably renumbering the vectors, we can assume this shortest relation to be

$$\beta_1 v_1 + \cdots + \beta_j v_j = 0, \qquad \beta_1 \neq 0, \ldots, \beta_j \neq 0. \tag{1}$$

We know that $v_i T = \lambda_i v_i$, so, applying T to equation (1), we obtain

$$\lambda_1 \beta_1 v_1 + \cdots + \lambda_j \beta_j v_j = 0. \tag{2}$$

Multiplying equation (1) by λ_1 and subtracting from equation (2), we obtain

$$(\lambda_2 - \lambda_1)\beta_2 v_2 + \cdots + (\lambda_j - \lambda_1)\beta_j v_j = 0.$$

Now $\lambda_i - \lambda_1 \neq 0$ for $i > 1$, and $\beta_i \neq 0$, whence $(\lambda_i - \lambda_1)\beta_i \neq 0$. But then we have produced a shorter relation than that in (1) between $v_1, v_2, \ldots, v_k$. This contradiction proves the theorem.

COROLLARY 1 *If $T \in A(V)$ and if $\dim_F V = n$ then T can have at most n distinct characteristic roots in F.*

Proof. Any set of linearly independent vectors in V can have at most n elements. Since any set of distinct characteristic roots of T, by Theorem 6.2.3, gives rise to a corresponding set of linearly independent characteristic vectors, the corollary follows.

COROLLARY 2 *If $T \in A(V)$ and if $\dim_F V = n$, and if T has n distinct characteristic roots in F, then there is a basis of V over F which consists of characteristic vectors of T.*

Matrices

DEFINITION Let V be an n-dimensioned vector space over F and let $v_1, \ldots, v_n$ be a basis for V over F. If $T \in A(V)$ then the *matrix of T in the basis $v_1, \ldots, v_n$*, written as $m(T)$, is

$$m(T) = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{pmatrix},$$

where $v_i T = \sum_j \alpha_{ij} v_j$.

A matrix then is an ordered, square array of elements of F, with, as yet, no further properties, which represents the effect of a linear transformation on a given basis.

Let us examine an example. Let F be a field and let V be the set of all polynomials in x of degree $n-1$ or less over F. On V let D be defined by $(\beta_0 + \beta_1 x + \cdots + \beta_{n-1}x^{n-1})D = \beta_1 + 2\beta_2 x + \cdots + i\beta_i x^{i-1} + \cdots + (n-1)\beta_{n-1}x^{n-2}$. It is trivial that D is a linear transformation on V; in fact, it is merely the differentiation operator.

What is the matrix of D? The questions is meaningless unless we specify a basis of V. Let us first compute the matrix of D in the basis $v_1 = 1$, $v_2 = x$, $v_3 = x^2, \ldots, v_i = x^{i-1}, \ldots, v_n = x^{n-1}$. Now,

$$
\begin{aligned}
v_1D &= 1D = 0 = 0v_1 + 0v_2 + \cdots + 0v_n \\
v_2D &= xD = 1 = 1v_1 + 0v_2 + \cdots + 0v_n \\
&\vdots \\
v_iD &= x^{i-1}D = (i-1)x^{i-2} \\
&= 0v_1 + 0v_2 + \cdots + 0v_{i-2} + (i-1)v_{i-1} + 0v_i \\
&\quad + \cdots + 0v_n \\
&\vdots \\
v_nD &= x^{n-1}D = (n-1)x^{n-2} \\
&= 0v_1 + 0v_2 + \cdots + 0v_{n-2} + (n-1)v_{n-1} + 0v_n.
\end{aligned}
$$

Going back to the very definition of the matrix of a linear transformation in a given basis, we see the matrix of D in the basis $v_1, \ldots, v_n$, $m_1(D)$, is in fact

$$
m_1(D) = \begin{pmatrix}
0 & 0 & 0 & \ldots & 0 & 0 \\
1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 2 & 0 & \ldots & 0 & 0 \\
0 & 0 & 3 & \ldots & 0 & 0 \\
0 & 0 & 0 & \ldots & (n-1) & 0
\end{pmatrix}
$$

However, there is nothing special about the basis we just used, or in how we numbered its elements. Suppose we merely renumber the elements of this basis; we then get an equally good basis $w_1 = x^{n-1}$, $w_2 = x^{n-2}, \ldots, w_i = x^{n-i}, \ldots, w_n = 1$. What is the matrix of the same linear transformation D in this basis? Now,

$$
\begin{aligned}
w_1D &= x^{n-1}D = (n-1)x^{n-2} \\
&= 0w_1 + (n-1)w_2 + 0w_3 + \cdots + 0w_n \\
&\vdots \\
w_iD &= x^{n-i}D = (n-i)x^{n-i-1} \\
&= 0w_1 + \cdots + 0w_i + (n-i)w_{i+1} + 0w_{i+2} + \cdots + 0w_n \\
&\vdots \\
w_nD &= 1D = 0 = 0w_1 + 0w_2 + \cdots + 0w_n,
\end{aligned}
$$

whence $m_2(D)$, the matrix of D in this basis is

$$m_2(D) = \begin{pmatrix} 0 & (n-1) & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & (n-2) & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & (n-3) & \dots & 0 & 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & \\ \vdots & & & & & & \\ 0 & 0 & 0 & \dots & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & \dots & 0 & 0 \end{pmatrix}.$$

Canonical Forms: Triangular Form

Let V be an n-dimensional vector space over a field F.

DEFINITION The linear transformations $S, T \in A(V)$ are said to be *similar* if there exists an invertible element $C \in A(V)$ such that $T = CSC^{-1}$.

DEFINITION The subspace W of V is *invariant under* $T \in A(V)$ if $WT \subset W$.

LEMMA 6.4.1 *If $W \subset V$ is invariant under T, then T induces a linear transformation $\bar{T}$ on V/W, defined by $(v + W)\bar{T} = vT + W$. If T satisfies*

the polynomial $q(x) \in F[x]$, then so does $\bar{T}$. If $p_1(x)$ is the minimal polynomial for $\bar{T}$ over F and if $p(x)$ is that for T, then $p_1(x) \mid p(x)$.

Proof. Let $\bar{V} = V/W$; the elements of $\bar{V}$ are, of course, the cosets $v + W$ of W in V. Given $\bar{v} = v + W \in \bar{V}$ define $\bar{v}\bar{T} = vT + W$. To verify that $\bar{T}$ has all the formal properties of a linear transformation on $\bar{V}$ is an easy matter *once it has been established that $\bar{T}$ is well defined on $\bar{V}$*. We thus content ourselves with proving this fact.

Suppose that $\bar{v} = v_1 + W = v_2 + W$ where $v_1, v_2 \in V$. We must show that $v_1T + W = v_2T + W$. Since $v_1 + W = v_2 + W$, $v_1 - v_2$ must be in W, and since W is invariant under T, $(v_1 - v_2)T$ must also be in W. Consequently $v_1T - v_2T \in W$, from which it follows that $v_1T + W = v_2T + W$, as desired. We now know that $\bar{T}$ defines a linear transformation on $\bar{V} = V/W$.

If $\bar{v} = v + W \in \bar{V}$, then $\bar{v}(\overline{T^2}) = vT^2 + W = (vT)T + W = (vT + W)\bar{T} = ((v + W)\bar{T})\bar{T} = \bar{v}(\bar{T})^2$; thus $(\overline{T^2}) = (\bar{T})^2$. Similarly, $(\overline{T^k}) = (\bar{T})^k$ for any $k \geq 0$. Consequently, for any polynomial $q(x) \in F[x]$, $\overline{q(T)} = q(\bar{T})$. For any $q(x) \in F[x]$ with $q(T) = 0$, since $\bar{0}$ is the zero transformation on $\bar{V}$, $0 = \overline{q(T)} = q(\bar{T})$.

Let $p_1(x)$ be the minimal polynomial over F satisfied by $\bar{T}$. If $q(\bar{T}) = 0$ for $q(x) \in F[x]$, then $p_1(x) \mid q(x)$. If $p(x)$ is the minimal polynomial for T over F, then $p(T) = 0$, whence $p(\bar{T}) = 0$; in consequence, $p_1(x) \mid p(x)$.

THEOREM 6.4.1 *If $T \in A(V)$ has all its characteristic roots in F, then there is a basis of V in which the matrix of T is triangular.*

Proof. The proof goes by induction on the dimension of V over F.

If $\dim_F V = 1$, then every element in $A(V)$ is a scalar, and so the theorem is true here.

Suppose that the theorem is true for all vector spaces over F of dimension $n-1$, and let V be of dimension n over F.

The linear transformation T on V has all its characteristic roots in F; let $\lambda_1 \in F$ be a characteristic root of T. There exists a nonzero vector v_1 in V such that $v_1 T = \lambda_1 v_1$. Let $W = \{\alpha v_1 \mid \alpha \in F\}$; W is a one-dimensional subspace of V, and is invariant under T. Let $\bar{V} = V/W$; by Lemma 4.2.6, $\dim \bar{V} = \dim V - \dim W = n-1$. By Lemma 6.4.1, T induces a linear transformation $\bar{T}$ on $\bar{V}$ whose minimal polynomial over F divides the minimal polynomial of T over F. Thus all the roots of the minimal polynomial of $\bar{T}$, being roots of the minimal polynomial of T, must lie in F. The linear transformation $\bar{T}$ in its action on $\bar{V}$ satisfies the hypothesis of the theorem; since $\bar{V}$ is $(n-1)$-dimensional over F, by our induction hypothesis, there is a basis $\bar{v}_2, \bar{v}_3, \ldots, \bar{v}_n$ of $\bar{V}$ over F such that

$$\begin{aligned}
\bar{v}_2\bar{T} &= \alpha_{22}\bar{v}_2 \\
\bar{v}_3\bar{T} &= \alpha_{32}\bar{v}_2 + \alpha_{33}\bar{v}_3 \\
&\vdots \\
\bar{v}_i\bar{T} &= \alpha_{i2}\bar{v}_2 + \alpha_{i3}\bar{v}_3 + \cdots + \alpha_{ii}\bar{v}_i \\
&\vdots \\
\bar{v}_n\bar{T} &= \alpha_{n2}\bar{v}_2 + \alpha_{n3}\bar{v}_3 + \cdots + \alpha_{nn}\bar{v}_n.
\end{aligned}$$

Let $v_2, \ldots, v_n$ be elements of V mapping into $\bar{v}_2, \ldots, \bar{v}_n$, respectively. Then $v_1, v_2, \ldots, v_n$ form a basis of V (see Problem 3, end of this section). Since $\bar{v}_2\bar{T} = \alpha_{22}\bar{v}_2$, $\bar{v}_2\bar{T} - \alpha_{22}\bar{v}_2 = 0$, whence $v_2 T - \alpha_{22}v_2$ must be in W. Thus $v_2 T - \alpha_{22}v_2$ is a multiple of v_1, say $\alpha_{21}v_1$, yielding, after transposing, $v_2 T = \alpha_{21}v_1 + \alpha_{22}v_2$. Similarly, $v_i T - \alpha_{i2}v_2 - \alpha_{i3}v_3 - \cdots - \alpha_{ii}v_i \in W$, whence $v_i T = \alpha_{i1}v_1 + \alpha_{i2}v_2 + \cdots + \alpha_{ii}v_i$. The basis $v_1, \ldots, v_n$ of V over

Since $\bar{v}_2\bar{T} = \alpha_{22}\bar{v}_2$, $\bar{v}_2\bar{T} - \alpha_{22}\bar{v}_2 = 0$, whence $v_2 T - \alpha_{22}v_2$ must be in W. Thus $v_2 T - \alpha_{22}v_2$ is a multiple of v_1, say $\alpha_{21}v_1$, yielding, after transposing, $v_2 T = \alpha_{21}v_1 + \alpha_{22}v_2$. Similarly, $v_i T - \alpha_{i2}v_2 - \alpha_{i3}v_3 - \cdots - \alpha_{ii}v_i \in W$, whence $v_i T = \alpha_{i1}v_1 + \alpha_{i2}v_2 + \cdots + \alpha_{ii}v_i$. The basis $v_1, \ldots, v_n$ of V over

F provides us with a basis where every $v_i T$ is a linear combination of v_i and its predecessors in the basis. Therefore, the matrix of T in this basis is triangular. This completes the induction and proves the theorem.

THEOREM 6.4.2 *If V is n-dimensional over F and if $T \in A(V)$ has all its characteristic roots in F, then T satisfies a polynomial of degree n over F.*

Proof. By Theorem 6.4.1, we can find a basis $v_1, \ldots, v_n$ of V over F such that:

$$\begin{aligned} v_1 T &= \lambda_1 v_1 \\ v_2 T &= \alpha_{21} v_1 + \lambda_2 v_2 \\ &\vdots \\ v_i T &= \alpha_{i1} v_1 + \cdots + \alpha_{i,i-1} v_{i-1} + \lambda_i v_i, \end{aligned}$$

for $i = 1, 2, \ldots, n$.

Equivalently

$$\begin{aligned} v_1(T - \lambda_1) &= 0 \\ v_2(T - \lambda_2) &= \alpha_{21} v_1 \\ &\vdots \\ v_i(T - \lambda_1) &= \alpha_{i1} v_1 + \cdots + \alpha_{i,i-1} v_{i-1}, \end{aligned}$$

for $i = 1, 2, \ldots, n$.

What is $v_2(T - \lambda_2)(T - \lambda_1)$? As a result of $v_2(T - \lambda_2) = \alpha_{21} v_1$ and $v_1(T - \lambda_1) = 0$, we obtain $v_2(T - \lambda_2)(T - \lambda_1) = 0$. Since

$$\begin{aligned} (T - \lambda_2)(T - \lambda_1) &= (T - \lambda_1)(T - \lambda_2), \\ v_1(T - \lambda_2)(T - \lambda_1) &= v_1(T - \lambda_1)(T - \lambda_2) = 0. \end{aligned}$$

Continuing this type of computation yields

$$\begin{aligned} v_1(T - \lambda_i)(T - \lambda_{i-1}) \cdots (T - \lambda_1) &= 0, \\ v_2(T - \lambda_i)(T - \lambda_{i-1}) \cdots (T - \lambda_1) &= 0, \\ &\vdots \\ v_i(T - \lambda_i)(T - \lambda_{i-1}) \cdots (T - \lambda_1) &= 0. \end{aligned}$$

For $i = n$, the matrix $S = (T - \lambda_n)(T - \lambda_{n-1}) \cdots (T - \lambda_1)$ satisfies $v_1 S = v_2 S = \cdots = v_n S = 0$. Then, since S annihilates a basis of V, S must annihilate all of V. Therefore, $S = 0$. Consequently, T satisfies the polynomial $(x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$ in $F[x]$ of degree n, proving the theorem.

Canonical Forms: Nilpotent Transformations

LEMMA 6.5.1 *If $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$, where each subspace V_i is of dimension n_i and is invariant under T, an element of $A(V)$, then a basis of V can be found so that the matrix of T in this basis is of the form*

$$\begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & A_k \end{pmatrix}$$

where each A_i is an $n_i \times n_i$ matrix and is the matrix of the linear transformation induced by T on V_i.

Proof. Choose a basis of V as follows: $v_1^{(1)}, \dots, v_{n_1}^{(1)}$ is a basis of V_1, $v_1^{(2)}, v_2^{(2)}, \dots, v_{n_2}^{(2)}$ is a basis of V_2, and so on. Since each V_i is invariant under T, $v_j^{(i)} T \in V_i$ so is a linear combination of $v_1^{(i)}, v_2^{(i)}, \dots, v_{n_i}^{(i)}$, and of only these. Thus the matrix of T in the basis so chosen is of the desired form. That each A_i is the matrix of T_i, the linear transformation induced on V_i by T, is clear from the very definition of the matrix of a linear transformation.

LEMMA 6.5.2 *If $T \in A(V)$ is nilpotent, then $\alpha_0 + \alpha_1 T + \cdots + \alpha_m T^m$, where the $\alpha_i \in F$, is invertible if $\alpha_0 \neq 0$.*

Proof. If S is nilpotent and $\alpha_0 \neq 0 \in F$, a simple computation shows that

$$(\alpha_0 + S)\left(\frac{1}{\alpha_0} - \frac{S}{\alpha_0^2} + \frac{S^2}{\alpha_0^3} + \cdots + (-1)^{r-1}\frac{S^{r-1}}{\alpha_0^r}\right) = 1,$$

if $S^r = 0$. Now if $T^r = 0$, $S = \alpha_1 T + \alpha_2 T^2 + \cdots + \alpha_m T^m$ also must satisfy $S^r = 0$. (Prove!) Thus for $\alpha_0 \neq 0$ in F, $\alpha_0 + S$ is invertible.

Notation. M_t will denote the $t \times t$ matrix

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & & \dots & 0 & 1 \\ 0 & 0 & & \dots & 0 & 0 \end{pmatrix},$$

all of whose entries are 0 except on the superdiagonal, where they are all 1's.

DEFINITION If $T \in A(V)$ is nilpotent, then k is called the *index of nilpotence* of T if $T^k = 0$ but $T^{k-1} \neq 0$.

THEOREM 6.5.1 *If $T \in A(V)$ is nilpotent, of index of nilpotence n_1, then a basis of V can be found such that the matrix of T in this basis has the form*

$$\begin{pmatrix} M_{n_1} & 0 & \dots & 0 \\ 0 & M_{n_2} & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & M_{n_r} \end{pmatrix},$$

where $n_1 \geq n_2 \geq \cdots \geq n_r$ and where $n_1 + n_2 + \cdots + n_r = \dim_F V$.

Proof. The proof will be a little detailed, so as we proceed we shall separate parts of it out as lemmas.

Since $T^{n_1} = 0$ but $T^{n_1-1} \neq 0$, we can find a vector $v \in V$ such that $vT^{n_1-1} \neq 0$. We claim that the vectors $v, vT, \dots, vT^{n_1-1}$ are linearly independent over F. For, suppose that $\alpha_1 v + \alpha_2 vT + \cdots + \alpha_{n_1} vT^{n_1-1} = 0$ where the $\alpha_i \in F$; let α_s be the first nonzero α, hence

$$vT^{s-1}(\alpha_s + \alpha_{s+1}T + \cdots + \alpha_{n_1}T^{n_1-s}) = 0.$$

Since $\alpha_s \neq 0$, by Lemma 6.5.2, $\alpha_s + \alpha_{s+1}T + \cdots + \alpha_{n_1}T^{n_1-s}$ is invertible, and therefore $vT^{s-1} = 0$. However, $s < n_1$, thus this contradicts that $vT^{n_1-1} \neq 0$. Thus no such nonzero α_s exists and $v, vT, \dots, vT^{n_1-1}$ have been shown to be linearly independent over F.

Let V_1 be the subspace of V spanned by $v_1 = v$, $v_2 = vT, \dots, v_{n_1} = vT^{n_1-1}$; V_1 is invariant under T, and, in the basis above, the linear transformation induced by T on V_1 has as matrix M_{n_1}.

LEMMA 6.5.3 *If $u \in V_1$ is such that $uT^{n_1-k} = 0$, where $0 < k \leq n_1$, then $u = u_0T^k$ for some $u_0 \in V_1$.*

Proof. Since $u \in V_1$, $u = \alpha_1 v + \alpha_2 vT + \cdots + \alpha_k vT^{k-1} + a_{k+1}vT^k + \cdots + \alpha_{n_1}vT^{n_1-1}$. Thus $0 = uT^{n_1-k} = \alpha_1 vT^{n_1-k} + \cdots + \alpha_k vT^{n_1-1}$. However, $vT^{n_1-k}, \dots, vT^{n_1-1}$ are linearly independent over F, whence $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$, and so, $u = \alpha_{k+1}vT^k + \cdots + \alpha_{n_1}vT^{n_1-1} = u_0T^k$, where $u_0 = \alpha_{k+1}v + \cdots + \alpha_{n_1}vT^{n_1-k-1} \in V_1$.

LEMMA 6.5.4 *There exists a subspace W of V, invariant under T, such that $V = V_1 \oplus W$.*

Proof. Let W be a subspace of V, of largest possible dimension, such that

1. $V_1 \cap W = (0)$;
2. W is invariant under T.

We want to show that $V = V_1 + W$. Suppose not; then there exists an element $z \in V$ such that $z \notin V_1 + W$. Since $T^{n_1} = 0$, there exists an integer k, $0 < k \leq n_1$, such that $zT^k \in V_1 + W$ and such that $zT^i \notin V_1 + W$ for $i < k$. Thus $zT^k = u + w$, where $u \in V_1$ and where $w \in W$. But then $0 = zT^{n_1} = (zT^k)T^{n_1-k} = uT^{n_1-k} + wT^{n_1-k}$; however, since both V_1 and W are invariant under T, $uT^{n_1-k} \in V_1$ and $wT^{n_1-k} \in W$. Now, since $V_1 \cap W = (0)$, this leads to $uT^{n_1-k} = -wT^{n_1-k} \in V_1 \cap W = (0)$, resulting in $uT^{n_1-k} = 0$. By Lemma 6.5.3, $u = u_0T^k$ for some $u_0 \in V_1$; therefore, $zT^k = u + w = u_0T^k + w$. Let $z_1 = z - u_0$; then $z_1T^k = zT^k - u_0T^k = w \in W$, and since W is invariant under T this yields $z_1T^m \in W$ for all $m \geq k$. On the other hand, if $i < k$, $z_1T^i = zT^i - u_0T^i \notin V_1 + W$, for otherwise zT^i must fall in $V_1 + W$, contradicting the choice of k.

Let W_1 be the subspace of V spanned by W and $z_1, z_1T, \ldots, z_1T^{k-1}$. Since $z_1 \notin W$, and since $W_1 \supset W$, the dimension of W_1 must be larger than that of W. Moreover, since $z_1T^k \in W$ and since W is invariant under T, W_1 must be invariant under T. By the maximal nature of W there must be an element of the form $w_0 + \alpha_1 z_1 + \alpha_2 z_1T + \cdots + \alpha_k z_1T^{k-1} \neq 0$ in $W_1 \cap V_1$, where $w_0 \in W$. Not all of $\alpha_1, \ldots, \alpha_k$ can be 0; otherwise we would have $0 \neq w_0 \in W \cap V_1 = (0)$, a contradiction. Let α_s be the first nonzero α; then $w_0 + z_1T^{s-1}(\alpha_s + \alpha_{s+1}T + \cdots + \alpha_kT^{k-s}) \in V_1$. Since $\alpha_s \neq 0$, by Lemma 6.5.2, $\alpha_s + \alpha_{s+1}T + \cdots + \alpha_kT^{k-s}$ is invertible and its inverse, R, is a polynomial in T. Thus W and V_1 are invariant under R; however, from the above, $w_0R + z_1T^{s-1} \in V_1R \subset V_1$, forcing $z_1T^{s-1} \in V_1 + WR \subset V_1 + W$. Since $s - 1 < k$ this is impossible; therefore $V_1 + W = V$. Because $V_1 \cap W = (0)$, $V = V_1 \oplus W$, and the lemma is proved.

The hard work, for the moment, is over; we now complete the proof of Theorem 6.5.1.

By Lemma 6.5.4, $V = V_1 \oplus W$ where W is invariant under T. Using the basis $v_1, \ldots, v_{n_1}$ of V_1 and any basis of W as a basis of V, by Lemma 6.5.1, the matrix of T in this basis has the form

$$\begin{pmatrix} M_{n_1} & 0 \\ 0 & A_2 \end{pmatrix},$$

where A_2 is the matrix of T_2, the linear transformation induced on W by T. Since $T^{n_1} = 0$, $T_2^{n_2} = 0$ for some $n_2 \leq n_1$. Repeating the argument used for T on V for T_2 on W we can decompose W as we did V (or, invoke an induction on the dimension of the vector space involved). Continuing this way, we get a basis of V in which the matrix of T is of the form

$$\begin{pmatrix} M_{n_1} & 0 & \ldots & 0 \\ 0 & M_{n_2} & & \\ \vdots & & \ddots & \vdots \\ 0 & \ldots & & M_{n_r} \end{pmatrix}.$$

That $n_1 + n_2 + \cdots + n_r = \dim V$ is clear, since the size of the matrix is $n \times n$ where $n = \dim V$.

DEFINITION The integers $n_1, n_2, \ldots, n_r$ are called the *invariants* of T.

DEFINITION If $T \in A(V)$ is nilpotent, the subspace M of V, of dimension m, which is invariant under T, is called *cyclic with respect to* T if

1. $MT^m = (0)$, $MT^{m-1} \neq (0)$;
2. there is an element $z \in M$ such that $z, zT, \ldots, zT^{m-1}$ form a basis of M.

(Note: Condition 1 is actually implied by Condition 2).

LEMMA 6.5.5 *If M, of dimension m, is cyclic with respect to T, then the dimension of MT^k is $m - k$ for all $k \leq m$.*

Proof. A basis of MT^k is provided us by taking the image of any basis of M under T^k. Using the basis $z, zT, \ldots, zT^{m-1}$ of M leads to a basis zT^k, $zT^{k+1}, \ldots, zT^{m-1}$ of MT^k. Since this basis has $m - k$ elements, the lemma is proved.

THEOREM 6.5.2 *Two nilpotent linear transformations are similar if and only if they have the same invariants.*

Proof. The discussion preceding the theorem has proved that if the two nilpotent linear transformations have different invariants, then they cannot be similar, for their respective matrices

$$\begin{pmatrix} M_{n_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & M_{n_r} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} M_{m_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & M_{m_s} \end{pmatrix}$$

cannot be similar.

In the other direction, if the two nilpotent linear transformations S and T have the same invariants $n_1 \geq \cdots \geq n_r$, by Theorem 6.5.1 there are bases $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ of V such that the matrix of S in $v_1, \ldots, v_n$ and that of T in $w_1, \ldots, w_n$, are each equal to

$$\begin{pmatrix} M_{n_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & M_{n_r} \end{pmatrix}.$$

But if A is the linear transformation defined on V by $v_iA = w_i$, then $S = ATA^{-1}$ (Prove! Compare with Problem 32 at the end of Section 6.3), whence S and T are similar.

Canonical Forms: A Decomposition of V: Jordan Form

LEMMA 6.6.1 *Suppose that $V = V_1 \oplus V_2$, where V_1 and V_2 are subspaces of V invariant under T. Let T_1 and T_2 be the linear transformations induced by T on V_1 and V_2, respectively. If the minimal polynomial of T_1 over F is $p_1(x)$ while that of T_2 is $p_2(x)$, then the minimal polynomial for T over F is the least common multiple of $p_1(x)$ and $p_2(x)$.*

Proof. If $p(x)$ is the minimal polynomial for T over F, as we have seen above, both $p(T_1)$ and $p(T_2)$ are zero, whence $p_1(x) \mid p(x)$ and $p_2(x) \mid p(x)$. But then the least common multiple of $p_1(x)$ and $p_2(x)$ must also divide $p(x)$.

On the other hand, if $q(x)$ is the least common multiple of $p_1(x)$ and $p_2(x)$, consider $q(T)$. For $v_1 \in V_1$, since $p_1(x) \mid q(x)$, $v_1 q(T) = v_1 q(T_1) = 0$; similarly, for $v_2 \in V_2$, $v_2 q(T) = 0$. Given any $v \in V$, v can be written as $v = v_1 + v_2$, where $v_1 \in V_1$ and $v_2 \in V_2$, in consequence of which $vq(T) = (v_1 + v_2)q(T) = v_1 q(T) + v_2 q(T) = 0$. Thus $q(T) = 0$ and T satisfies $q(x)$. Combined with the result of the first paragraph, this yields the lemma.

COROLLARY *If $V = V_1 \oplus \cdots \oplus V_k$ where each V_i is invariant under T and if $p_i(x)$ is the minimal polynomial over F of T_i, the linear transformation induced by T on V_i, then the minimal polynomial of T over F is the least common multiple of $p_1(x), p_2(x), \ldots, p_k(x)$.*

THEOREM 6.6.1 *For each* $i = 1, 2, \ldots, k$, $V_i \neq (0)$ *and* $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$. *The minimal polynomial of* T_i *is* $q_i(x)^{l_i}$.

Proof. If $k = 1$ then $V = V_1$ and there is nothing that needs proving. Suppose then that $k > 1$.

We first want to prove that each $V_i \neq (0)$. Towards this end, we introduce the k polynomials:

$$\begin{aligned} h_1(x) &= q_2(x)^{l_2} q_3(x)^{l_3} \cdots q_k(x)^{l_k}, \\ h_2(x) &= q_1(x)^{l_1} q_3(x)^{l_3} \cdots q_k(x)^{l_k}, \ldots, \\ h_i(x) &= \prod_{j \neq i} q_j(x)^{l_j}, \ldots, \\ &\vdots \\ h_k(x) &= q_1(x)^{l_1} q_2(x)^{l_2} \cdots q_{k-1}(x)^{l_{k-1}}. \end{aligned}$$

Since $k > 1$, $h_i(x) \neq p(x)$, whence $h_i(T) \neq 0$. Thus, given i, there is a $v \in V$ such that $w = vh_i(T) \neq 0$. But $wq_i(T)^{l_i} = v(h_i(T)q_i(T)^{l_i}) = vp(T) = 0$. In consequence, $w \neq 0$ is in V_i and so $V_i \neq (0)$. In fact, we have shown a little more, namely, that $Vh_i(T) \neq (0)$ is in V_i. Another remark about the $h_i(x)$ is in order now: if $v_j \in V_j$ for $j \neq i$, since $q_j(x)^{l_j} \mid h_i(x)$, $v_j h_i(T) = 0$.

The polynomials $h_1(x), h_2(x), \ldots, h_k(x)$ are relatively prime. (Prove!) Hence by Lemma 3.9.4 we can find polynomials $a_1(x), \ldots, a_k(x)$ in $F[x]$ such that $a_1(x)h_1(x) + \cdots + a_k(x)h_k(x) = 1$. From this we get $a_1(T)h_1(T) + \cdots + a_k(T)h_k(T) = 1$, whence, given $v \in V$, $v = v1 = v(a_1(T)h_1(T) + \cdots + a_k(T)h_k(T)) = va_1(T)h_1(T) + \cdots + va_k(T)h_k(T)$. Now, each $va_i(T)h_i(T)$ is in $Vh_i(T)$, and since we have shown above that $Vh_i(T) \subset V_i$, we have now exhibited v as $v = v_1 + \cdots + v_k$, where each $v_i = va_i(T)h_i(T)$ is in V_i. Thus $V = V_1 + V_2 + \cdots + V_k$.

We must now verify that this sum is a direct sum. To show this, it is enough to prove that if $u_1 + u_2 + \cdots + u_k = 0$ with each $u_i \in V_i$, then each $u_i = 0$. So, suppose that $u_1 + u_2 + \cdots + u_k = 0$ and that some u_i, say u_1, is not 0. Multiply this relation by $h_1(T)$; we obtain $u_1h_1(T) + \cdots + u_kh_1(T) = 0h_1(T) = 0$. However, $u_jh_1(T) = 0$ for $j \neq 1$ since $u_j \in V_j$; the equation thus reduces to $u_1h_1(T) = 0$. But $u_1q_1(T)^{l_1} = 0$ and since $h_1(x)$ and $q_1(x)$ are relatively prime, we are led to $u_1 = 0$ (Prove!) which is, of course, inconsistent with the assumption that $u_1 \neq 0$. So far we have succeeded in proving that $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$.

To complete the proof of the theorem, we must still prove that the minimal polynomial of T_i on V_i is $q(x)^{l_i}$. By the definition of V_i, since $V_iq_i(T)^{l_i} = 0$, $q_i(T_i)^{l_i} = 0$, whence the minimal equation of T_i must be a divisor of $q_i(x)^{l_i}$, thus of the form $q_i(x)^{f_i}$ with $f_i \leq l_i$. By the corollary to Lemma 6.6.1 the minimal polynomial of T over F is the least common multiple of $q_1(x)^{f_1}, \ldots, q_k(x)^{f_k}$ and so must be $q_1(x)^{f_1} \cdots q_k(x)^{f_k}$. Since this minimal polynomial is in fact $q_1(x)^{l_1} \cdots q_k(x)^{l_k}$ we must have that $f_1 \geq l_1$, $f_2 \geq l_2, \ldots, f_k \geq l_k$. Combined with the opposite inequality above, this yields the desired result $l_i = f_i$ for $i = 1, 2, \ldots, k$ and so completes the proof of the theorem.

If all the characteristic roots of T should happen to lie in F, then the minimal polynomial of T takes on the especially nice form $q(x) = (x - \lambda_1)^{l_1} \cdots (x - \lambda_k)^{l_k}$ where $\lambda_1, \ldots, \lambda_k$ are the distinct characteristic roots of T. The irreducible factors $q_i(x)$ above are merely $q_i(x) = x - \lambda_i$. Note that on V_i, T_i only has λ_i as a characteristic root.

DEFINITION The matrix

$$\begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & & \ldots & . \\ . & & & & . \\ . & & & & . \\ . & & & & 1 \\ 0 & & & \ldots & \lambda \end{pmatrix},$$

with λ's on the diagonal, 1's on the superdiagonal, and 0's elsewhere, is a basic *Jordan block belonging to* λ.

Possible Questions

PART-B (6 Mark)

1. If $u \in v_1$ is such that $uT^{n_1-k} = 0$, where $0 < k \leq n_1$,then prove that $u = u_0T^k$ for some $u_0 \epsilon V_1$.
2. Prove that two nilpotent linear transformations are similar if and only if they have the same invariants.
3. Prove that if V is n-dimensional over F and if $T \epsilon$ A(V) has all its characteristic roots in F, then prove that T satisfies a polynomial of degree n over F.
4. If M, of dimension of m, is cyclic with respect to T, then the dimension of MT^k is m-k for all $k \leq m$.
5. Show that the element S and T in $A_F(V)$ are similar in $A_F(V)$ iff they have the same elementary divisors.
6. Let A be an algebra with unit element, over F, and suppose that A is of dimension m over F. then every element in A satisfies some nontrivial polynomial in F[x] of degree at most m.
7. Prove that if $T \epsilon$ A(v) has all its characteristic roots in F, then prove that there is a basis of V in which the matrix of T is triangular.
8. Prove that there exist a subspace W of V, invariant under T, then $V=V_1 \oplus W$.
9. Prove that if V is n-dimensional over F and if $T \epsilon A(V)$ has all its characteristic roots in F, then prove that T satisfies a polynomial of degree n over F.

PART-C (10 Mark)

1. Show that if $T \in A(v)$ is nilpotent, then prove that $\alpha_0 + \alpha_1 T + \alpha_2 T^2 + ... + \alpha_m T^m$ where $\alpha_i \in F$ is invertible if $\alpha_0 \neq 0$
2. Prove that if V is n-dimensional over F and if $T \epsilon$ A(V) has all its characteristic roots in F, then prove that T satisfies a polynomial of degree n over F.
3. Prove that two nilpotent linear transformations are similar if and only if they have the same invariants.

KARPAGAM ACADEMY OF HIGHER EDUCATION
DEPARTMENT OF MATHEMATICS
ALBEBRA (18MMP101)

UNIT - IV

Questions	choice 1	choice 2	choice 3	choice 4	Answer
F[x] is a----------	Euclidean ring	ring	integral	field	integral
The set of all vector space-homomorphisms of V into itself ----------	Hom(V,W)	Hom(W,V)	Hom(V,V)	Hom(W,W)	Hom(V,V)
Hom(V,V) is the set of all vector space-homomorphisms of V into itself	V into V	V into W	W into W	W into V	V into V
A linear transformation on V,over F is an element of ----------	$A_F(W)$	$B_F(V)$	$A_F(V)$	$W_F(V)$	$A_F(V)$
A linear transformation on ---------- is an element of $A_F(V)$	W over F	V over V	F over F	V over F	V over F
A complexnumber is said to be an algebraic number if it is algebraic over the field of ----------	complexnumber	real number	rational number	irrational number	rational number
The number e is ----------	complexnumbe	real number	irrational	transcendental	transcendental
If $f(x) \in F(x)$ then there is a ---------- E of F in which f(x)has a root .	finite extension	extension	normal extension	simple extension	finite extension
τ^* defines an ---------- of F[x] onto F'[t] with the property that $\alpha\tau^*=\alpha'$ for every $\alpha \in F$	isomorphism	automorphism	homomorphism	monomorphism	isomorphism
τ^* defines an isomorphism of ---------- with the property that $\alpha\tau^*=\alpha'$ for every $\alpha \in F$	F[x] onto F'[t]	f[x] intof'[t]	f[x] ontof'[t]	F[x] into F'[t]	F[x] onto F'[t]
An element $T \in A(V)$ is called ---------- if there exists an $S \in A(V)$ such that TS =1	both invertible	right-invertible	left-invertible	invertible	right-invertible
An element ---------- is called right-invertible if there exists an $S \in A(V)$ such that TS =1	$V \in A(V)$	$T \in A(T)$	$T \in A(V)$	$T \in A(T)$	$T \in A(V)$
An element $T \in A(V)$ is called right-invertible if there exists an $S \in A(V)$ such that ----------	TS =1	TS=0	ST =1	TS =2	TS =1
A ---------- is said to be an algebraic number if it is algebraic over the field of rational numbers	complexnumber	real number	rational number	irrational number	complexnumber
A complexnumber is said to be an -------- if it is algebraic over the field of rational numbers	complexnumber	algebraic mumder	rational number	irrational number	algebraic mumder
τ^* defines an isomorphism of F[x] onto F'[t] with the property that---------- for every $\alpha \in F$	at*=a'	a=a*	at*=a	a=a'	at*=a'
If α is constructible then α lies in some ---------- of the rationals of degree a powerof	finite extension	extension	normal extension	simple extension	extension
If α is constructible then α lies in some extension of the rationals of degree a powerof --------	2	3	0	1	2
The ---------- of F is a simple extension of F if $K=F(\alpha)$ for some α in K	finite extension K	extension K	c)normal extension	simple extension	extension K
The extension K of F is a---------- if $K=F(\alpha)$ for some α in K	finite extension K	extension K	c)normal extension	simple extension of F	simple extension of F
The extension K of F is a simple extension of F if--------- for some α in K	K=F(a)	$K \subset F(\alpha)$	$K=f(\alpha)$	$K=F(\alpha)$	$K=F(\alpha)$
---------- is separable over F, F(a,b) is a simple extension of F	a or b	a and b	ab	a,b	a or b
If one of aor b is ---------- over F, F(a,b) is a simple extension of F	non-separable	separable	reduciable	irreducible	separable
If one of aor b is separable over F F(a,b) is a of F---------- of F	finite extension	extension	normal extension	simple extension	simple extension

The of elements in K which are --------over F forms a sub field of K	non-separable	separable	reduciable	irreducible	separable
The set of elements in K which are separable over F forms a sub field of K	field	group	sub group	subfield	subfield
If is a group of automorphisms of K then the ----------of G is the set of all elements $\alpha \in K$ such that $\sigma(\alpha)=\alpha$ for all $\sigma \in G$	field	fixed field	normal field	subfield	fixed field
f G is a group of automorphisms of K then the fixed field of G is the set of all elements $\alpha \in K$ such that -------- for all $\sigma \in G$	$\sigma(a)=a$	$K(a)=a$	$\sigma(a)=K$	$\sigma(a)=K$	$\sigma(a)=K$
If G is a group ----- of K then the fixed field of G is the set of all elements $\alpha \in K$ such that $\sigma(\alpha)=\alpha$ for all $\sigma \in G$	isomorphism	automorphism	homomorphism	monomorphism	automorphism
G(K,F) isa subgroup of the group of all ---------- of K	isomorphism	automorphism	homomorphism	monomorphism	automorphism
If K is a ---------- then G(K,F) is a finite group and its order o(G(K,F)) satisfieso(G(K,F))<=[K.F]	finite extension of K	extension K	normal extension	simple extension of F	finite extension of K
If K is a finite extension of F then G(K,F) is a finite group and its order o(G(K,F)) satisfies -----	o(G)=[K,F]	o(G)=F	o(G(K,F))<=[K.F]	o(G)=K	o(G(K,F))<=[K.F]
K is a ---------- of F if K is a finite extension of F such that F is the fixed field of G(K,F)	finite extension	extension	normal extension	simple extension	normal extension
K is a normal extension of F if K is a ---------- of F such that F is the fixed field of G(K,F)	finite extension	extension	normal extension	simple extension	finite extension
K is a normal extension of F if K is a finite extension of F such that F is the -------- of G(K,F)	field	fixed field	normal field	subfield	fixed field
K isa ---------- of F if and only if K is the splitting field of some polynomial overF	finite extension	extension	normal extension	simple extension	normal extension
K is a normal extension of F if and only if K is the---------- of some polynomial overF	field	splitting field	fixed field	simple field	splitting field
If G is a ---------- and if G^- is a homomorphic image of G then G^- is solvable	sovlable group	field	group	simple field	sovlable group
If G is a sovlable group and if G^- is a---------- image of G then G^- is solvable	isomorphism	automorphism	homomorphism	monomorphism	homomorphism
If G is a solvable group and if G^- is a homomorphic image of G then G^- is ---------	non-separable	separable	reduciable	solvable	solvable
Sn is---------- for n≥5	separable	not solvable	sovlable	non-separable	not solvable
Sn is not solvable for ----------	n>5	n≥5	n<5	n<4	n≥5
If $p(x) \in F[x]$ is ---------- by radicals over F then the Galois group over F of p(x) is a solvable group	non-separable	separable	reduciable	solvable	solvable
If $p(x) \in F[x]$ is solvable by radicals over F then the--------- over F of p(x) is a solvable group	sovlable group	Galois group	group	simple field	Galois group
If $p(x) \in F[x]$ is solvable by radicals over F then the Galois group over F of p(x) is a ----------	separable group	not solvable group	sovlable group	non-separable group	sovlable group
If V is -------- over F then the rank of T is the dimension of VT the range of T over F	field	infinite dimensional	finite dimensional	dimensional	finite dimensional

If V is finite dimensional over F then the rank of T is the dimension of the range of T over F	FT	F	V	VT	VT
If ---------- A(V) has no two sided ideal other than (0) and A(V)	dim(V)=1	dim (V) >1	dim (v)<1	dim (v)≠1	dim (V) >1
If dim (V) >1 A(V) has---------- other than (0) and A(V)	no two sided ideal	two sided ideal	one sided ideal	no one sided ideal	no two sided ideal
If dim (V) >1 A(V) has no two sided ideal other than ----------	0	(0) and A(V)	(0)or A(V)	A(V)	(0) and A(V)

UNIT-V

Trace and Transpose – Trace of T-Symmetric Matrix –Determinants–Hermitian Transformation, Unitary Transformation and Normal Transformation – Real quadratic forms.

Trace and Transpose

DEFINITION The *trace* of A is the sum of the elements on the main diagonal of A.

We shall write the trace of A as tr A; if $A = (\alpha_{ij})$, then

$$\text{tr } A = \sum_{i=1}^{n} \alpha_{ii}.$$

LEMMA 6.8.1 *For $A, B \in F_n$ and $\lambda \in F$,*

1. tr $(\lambda A) = \lambda$ tr A.
2. tr $(A + B) =$ tr $A +$ tr B.
3. tr $(AB) =$ tr (BA).

Proof. To establish parts 1 and 2 (which assert that the trace is a linear functional on F_n) is straightforward and is left to the reader. We only present the proof of part 3 of the lemma.

If $A = (\alpha_{ij})$ and $B = (\beta_{ij})$ then $AB = (\gamma_{ij})$ where

$$\gamma_{ij} = \sum_{k=1}^{n} \alpha_{ik}\beta_{kj}$$

and $BA = (\mu_{ij})$ where

$$\mu_{ij} = \sum_{k=1}^{n} \beta_{ik}\alpha_{kj}.$$

Thus

$$\text{tr } (AB) = \sum_i \gamma_{ii} = \sum_i \left(\sum_k \alpha_{ik}\beta_{ki} \right);$$

if we interchange the order of summation in this last sum, we get

$$\text{tr } (AB) = \sum_{k=1}^{n} \sum_{i=1}^{n} \alpha_{ik}\beta_{ki} = \sum_{k=1} \left(\sum_{i=1} \beta_{ki}\alpha_{ik} \right) = \sum_{k=1}^{n} \mu_{kk} = \text{tr } (BA).$$

COROLLARY *If A is invertible then* tr (ACA^{-1}) = tr C.

Proof. Let $B = CA^{-1}$; then tr (ACA^{-1}) = tr (AB) = tr (BA) = tr $(CA^{-1}A)$ = tr C.

DEFINITION If $T \in A(V)$ then tr T, the *trace* of T, is the trace of $m_1(T)$ where $m_1(T)$ is the matrix of T in some basis of V.

LEMMA 6.8.2 *If $T \in A(V)$ then* tr T *is the sum of the characteristic roots of T (using each characteristic root as often as its multiplicity).*

LEMMA 6.8.3 *If F is a field of characteristic 0, and if $T \in A_F(V)$ is such that* tr $T^i = 0$ *for all $i \geq 1$ then T is nilpotent.*

Proof. Since $T \in A_F(V)$, T satisfies some minimal polynomial $p(x) = x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$; from $T^m + \alpha_1 T^{m-1} + \cdots + \alpha_{m-1} T + \alpha_m = 0$, taking traces of both sides yields

$$\text{tr } T^m + \alpha_1 \text{ tr } T^{m-1} + \cdots + \alpha_{m-1} \text{ tr } T + \text{tr } \alpha_m = 0.$$

However, by assumption, tr $T^i = 0$ for $i \geq 1$, thus we get tr $\alpha_m = 0$; if dim $V = n$, tr $\alpha_m = n\alpha_m$ whence $n\alpha_m = 0$. But the characteristic of F is 0; therefore, $n \neq 0$, hence it follows that $\alpha_m = 0$. Since the constant term of the minimal polynomial of T is 0, by Theorem 6.1.2 T is singular and so 0 is a characteristic root of T.

We can consider T as a matrix in F_n and therefore also as a matrix in K_n, where K is an extension of F which in turn contains all the characteristic roots of T. In K_n, by Theorem 6.4.1, we can bring T to triangular form, and since 0 is a characteristic root of T, we can actually bring it to the form

$$\left(\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline \beta_2 & \alpha_2 & 0 & 0 \\ \vdots & & \ddots & \vdots \\ \beta_n & * & & \alpha_n \end{array}\right) = \left(\begin{array}{c|c} 0 & 0 \\ \hline * & T_2 \end{array}\right),$$

LEMMA 6.9.5 *Interchanging two rows of A changes the sign of its determinant.*

Proof. Since two rows are equal, by Lemma 6.9.4, $d(v_1, \ldots, v_{i-1}, v_i + v_j, v_{i+1}, \ldots, v_{j-1}, v_i + v_j, v_{j+1}, \ldots, v_n) = 0$. Using Lemma 6.9.3 several times, we can expand this to obtain $d(v_1, \ldots, v_{i-1}, v_i, \ldots, v_{j-1}, v_j, \ldots, v_n) + d(v_1, \ldots, v_{i-1}, v_j, \ldots, v_{j-1}, v_i, \ldots, v_n) + d(v_1, \ldots, v_{i-1}, v_i, \ldots, v_{j-1}, v_i, \ldots, v_n) + d(v_1, \ldots, v_{i-1}, v_j, \ldots, v_{j-1}, v_j, \ldots, v_n) = 0$. However, each of the last two terms has in it two equal rows, whence, by Lemma 6.9.4, each is 0. The above relation then reduces to $d(v_1, \ldots, v_{i-1}, v_i, \ldots, v_{j-1}, v_j, \ldots, v_n) + d(v_1, \ldots, v_{i-1}, v_j, \ldots, v_{j-1}, v_i, \ldots, v_n) = 0$, which is precisely the assertion of the lemma.

where

$$T_2 = \begin{pmatrix} \alpha_2 & 0 & 0 \\ & \ddots & \vdots \\ & * & \\ & & \alpha_n \end{pmatrix}$$

is an $(n-1) \times (n-1)$ matrix (the $*$'s indicate parts in which we are not interested in the explicit entries). Now

$$T^k = \left(\begin{array}{c|c} 0 & 0 \\ \hline * & T_2^k \end{array}\right)$$

hence $0 = \operatorname{tr} T^k = \operatorname{tr} T_2^k$. Thus T_2 is an $(n-1) \times (n-1)$ matrix with the property that $\operatorname{tr} T_2^k = 0$ for all $k \geq 1$. Either using induction on n, or repeating the argument on T_2 used for T, we get, since $\alpha_2, \ldots, \alpha_n$ are the characteristic roots of T_2, that $\alpha_2 = \cdots = \alpha_n = 0$. Thus when T is brought to triangular form, all its entries on the main diagonal are 0, forcing T to be nilpotent. (Prove!)

LEMMA 6.8.4 *If F is of characteristic 0 and if S and T, in $A_F(V)$, are such that $ST - TS$ commutes with S, then $ST - TS$ is nilpotent.*

Proof. For any $k \geq 1$ we compute $(ST - TS)^k$. Now $(ST - TS)^k = (ST - TS)^{k-1}(ST - TS) = (ST - TS)^{k-1}ST - (ST - TS)^{k-1}TS$. Since $ST - TS$ commutes with S, the term $(ST - TS)^{k-1}ST$ can be written in the form $S((ST - TS)^{k-1}T)$. If we let $B = (ST - TS)^{k-1}T$, we see that $(ST - TS)^k = SB - BS$; hence $\text{tr}((ST - TS)^k) = \text{tr}(SB - BS) = \text{tr}(SB) - \text{tr}(BS) = 0$ by Lemma 6.8.1. The previous lemma now tells us that $ST - TS$ must be nilpotent.

DEFINITION If $A = (\alpha_{ij}) \in F_n$ then the *transpose* of A, written as A', is the matrix $A' = (\gamma_{ij})$ where $\gamma_{ji} = \alpha_{ji}$ for each i and j.

LEMMA 6.8.5 *For all $A, B \in F_n$,*

1. $(A')' = A$.
2. $(A + B)' = A' + B'$.
3. $(AB)' = B'A'$.

Proof. The proofs of parts 1 and 2 are straightforward and are left to the reader; we content ourselves with proving part 3.

Suppose that $A = (\alpha_{ij})$ and $B = (\beta_{ij})$; then $AB = (\lambda_{ij})$ where

$$\lambda_{ij} = \sum_{k=1}^{n} \alpha_{ik}\beta_{kj}.$$

Therefore, by definition, $(AB)' = (\mu_{ij})$, where

$$\mu_{ij} = \lambda_{ji} = \sum_{k=1}^{n} \alpha_{jk}\beta_{ki}.$$

On the other hand, $A' = (\gamma_{ij})$ where $\gamma_{ij} = \alpha_{ji}$ and $B' = (\xi_{ij})$ where $\xi_{ij} = \beta_{ji}$, whence the (i, j) element of $B'A'$ is

$$\sum_{k=1}^{n} \xi_{ik}\gamma_{kj} = \sum_{k=1}^{n} \beta_{ki}\alpha_{jk} = \sum_{k=1}^{n} \alpha_{jk}\beta_{ki} = \mu_{ij}.$$

That is, $(AB)' = B'A'$ and we have verified part 3 of the lemma.

In part 3, if we specialize $A = B$ we obtain $(A^2)' = (A')^2$. Continuing, we obtain $(A^k)' = (A')^k$ for all positive integers k. When A is invertible, then $(A^{-1})' = (A')^{-1}$.

There is a further property enjoyed by the transpose, namely, if $\lambda \in F$ then $(\lambda A)' = \lambda A'$ for all $A \in F_n$. Now, if $A \in F_n$ satisfies a polynomial $\alpha_0 A^m + \alpha_1 A^{m-1} + \cdots + \alpha_m = 0$, we obtain $(\alpha_0 A^m + \cdots + \alpha_m)' = 0' = 0$. Computing out $(\alpha_0 A^m + \cdots + \alpha_m)'$ using the properties of the transpose, we obtain $\alpha_0 (A')^m + \alpha_1 (A')^{m-1} + \cdots + \alpha_m = 0$, that is to say, A' satisfies any polynomial over F which is satisfied by A. Since $A = (A')'$, by the same token, A satisfies any polynomial over F which is satisfied by A'. In particular, A and A' have the same minimal polynomial over F and so *they have the same characteristic roots.* One can show each root occurs with the same multiplicity in A and A'. This is evident once it is established that A and A' are actually similar (see Problem 14).

DEFINITION The matrix A is said to be a *symmetric matrix* if $A' = A$.

DEFINITION The matrix A is said to be a *skew-symmetric matrix* if $A' = -A$.

DEFINITION A mapping $*$ from F_n into F_n is called an *adjoint* on F_n if

1. $(A^*)^* = A$;
2. $(A + B)^* = A^* + B^*$;
3. $(AB)^* = B^*A^*$;

for all $A, B \in F_n$.

Determinants

DEFINITION If $A = (\alpha_{ij})$ then the *determinant of* A, written $\det A$, is the element $\sum_{\sigma \in S_n} (-1)^\sigma \alpha_{1\sigma(1)}\alpha_{2\sigma(2)} \cdots \alpha_{n\sigma(n)}$ in F.

We shall at times use the notation

$$\begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{vmatrix}$$

LEMMA 6.9.1 *The determinant of a triangular matrix is the product of its entries on the main diagonal.*

LEMMA 6.9.2 *If $A \in F_n$ and $\gamma \in F$ then $d(v_1, \ldots, v_{i-1}, \gamma v_i, v_{i+1}, \ldots, v_n) = \gamma d(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n)$.*

Note that the lemma says that if all the elements in one row of A are multiplied by a fixed element γ in F then the determinant of A is itself multiplied by γ.

Proof. Since only the entries in the ith row are changed, the expansion of $d(v_1, \ldots, v_{i-1}, \gamma v_i, v_{i+1}, \ldots, v_n)$ is

$$\sum_{\sigma \in S_n} (-1)^\sigma \alpha_{1\sigma(1)} \cdots \alpha_{i-1,\sigma(i-1)}(\gamma\alpha_{i\sigma(i)})\alpha_{i+1,\sigma(i+1)} \cdots \alpha_{n\sigma(n)};$$

since this equals $\gamma \sum_{\sigma \in S_n} (-1)^\sigma \alpha_{1\sigma(1)} \cdots \alpha_{i\sigma(i)} \cdots \alpha_{n\sigma(n)}$, it does indeed equal $\gamma d(v_1, \ldots, v_n)$.

LEMMA 6.9.4 *If two rows of A are equal (that is, $v_r = v_s$ for $r \neq s$), then* $\det A = 0$.

Proof. Let $A = (\alpha_{ij})$ and suppose that for some r, s where $r \neq s$, $\alpha_{rj} = \alpha_{sj}$ for all j. Consider the expansion

$$\det A = \sum_{\sigma \in S_n} (-1)^\sigma \alpha_{1\sigma(1)} \cdots \alpha_{r\sigma(r)} \cdots \alpha_{s\sigma(s)} \cdots \alpha_{n\sigma(n)}.$$

In the expansion we pair the terms as follows: For $\sigma \in S_n$ we pair the term $(-1)^\sigma \alpha_{1\sigma(1)} \cdots \alpha_{n\sigma(n)}$ with the term $(-1)^{\tau\sigma} \alpha_{1\tau\sigma(1)} \cdots \alpha_{n\tau\sigma(n)}$ where τ is the transposition $(\sigma(r), \sigma(s))$. Since τ is a transposition and $\tau^2 = 1$, this indeed gives us a pairing. However, since $\alpha_{r\sigma(r)} = \alpha_{s\sigma(r)}$, by assumption, and $\alpha_{r\sigma(r)} = \alpha_{st\sigma(s)}$, we have that $\alpha_{r\sigma(r)} = \alpha_{st\sigma(s)}$. Similarly, $\alpha_{s\sigma(s)} = \alpha_{rt\sigma(r)}$. On the other hand, for $i \neq r$ and $i \neq s$, since $\tau\sigma(i) = \sigma(i)$, $\alpha_{i\sigma(i)} = \alpha_{it\sigma(i)}$. Thus the terms $\alpha_{1\sigma(1)} \cdots \alpha_{n\sigma(n)}$ and $\alpha_{1\tau\sigma(1)} \cdots \alpha_{n\tau\sigma(n)}$ are equal. The first occurs with the sign $(-1)^\sigma$ and the second with the sign $(-1)^{\tau\sigma}$ in the expansion of $\det A$. Since τ is a transposition and so an odd permutation, $(-1)^{\tau\sigma} = -(-1)^\sigma$. Therefore in the pairing, the paired terms cancel each other out in the sum, whence $\det A = 0$. (The proof does not depend on the characteristic of F and holds equally well even in the case of characteristic 2.)

LEMMA 6.9.5 *Interchanging two rows of A changes the sign of its determinant.*

Proof. Since two rows are equal, by Lemma 6.9.4, $d(v_1, \ldots, v_{i-1}, v_i + v_j, v_{i+1}, \ldots, v_{j-1}, v_i + v_j, v_{j+1}, \ldots, v_n) = 0$. Using Lemma 6.9.3 several times, we can expand this to obtain $d(v_1, \ldots, v_{i-1}, v_i, \ldots, v_{j-1}, v_j, \ldots, v_n) + d(v_1, \ldots, v_{i-1}, v_j, \ldots, v_{j-1}, v_i, \ldots, v_n) + d(v_1, \ldots, v_{i-1}, v_i, \ldots, v_{j-1}, v_i, \ldots, v_n) + d(v_1, \ldots, v_{i-1}, v_j, \ldots, v_{j-1}, v_j, \ldots, v_n) = 0$. However, each of the last two terms has in it two equal rows, whence, by Lemma 6.9.4, each is 0. The above relation then reduces to $d(v_1, \ldots, v_{i-1}, v_i, \ldots, v_{j-1}, v_j, \ldots, v_n) + d(v_1, \ldots, v_{i-1}, v_j, \ldots, v_{j-1}, v_i, \ldots, v_n) = 0$, which is precisely the assertion of the lemma.

COROLLARY *If the matrix B is obtained from A by a permutation of the rows of A then* $\det A = \pm \det B$, *the sign being* $+1$ *if the permutation is even,* -1 *if the permutation is odd.*

THEOREM 6.9.1 *For* $A, B \in F_n$, $\det(AB) = (\det A)(\det B)$.

Proof. Let $A = (\alpha_{ij})$ and $B = (\beta_{ij})$; let the rows of B be the vectors $u_1, u_2, \ldots, u_n$. We introduce the n vectors $w_1, \ldots, w_n$ as follows:

$$\begin{aligned} w_1 &= \alpha_{11}u_1 + \alpha_{12}u_2 + \cdots + \alpha_{1n}u_n, \\ w_2 &= \alpha_{21}u_1 + \alpha_{22}u_2 + \cdots + \alpha_{2n}u_n, \\ &\vdots \\ w_n &= \alpha_{n1}u_1 + \alpha_{n2}u_2 + \cdots + \alpha_{nn}u_n. \end{aligned}$$

Consider $d(w_1, \ldots, w_n)$; expanding this out and making many uses of Lemmas 6.9.2 and 6.9.3, we obtain

$$d(w_1, \ldots, w_n) = \sum_{i_1, i_2, \ldots, i_n} \alpha_{1i_1}\alpha_{2i_2}\cdots\alpha_{ni_n} d(u_{i_1}, u_{i_2}, \ldots, u_{i_n}).$$

In this multiple sum $i_1, \ldots, i_n$ run independently from 1 to n. However, if any two $i_r = i_s$ then $u_{i_r} = u_{i_s}$ whence $d(u_{i_1}, \ldots, u_{i_r}, \ldots, u_{i_s}, \ldots, u_{i_n}) = 0$ by Lemma 6.9.4. In other words, the only terms in the sum that may give a nonzero contribution are those for which all of $i_1, i_2, \ldots, i_n$ are distinct, that is for which the mapping

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

is a permutation of $1, 2, \ldots, n$. Also any such permutation is possible. Finally note that by the corollary to Lemma 6.9.5, when

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

is a permutation, then $d(u_{i_1}, u_{i_2}, \ldots, u_{i_n}) = (-1)^\sigma d(u_1, \ldots, u_n) = (-1)^\sigma \det B$. Thus we get

$$\begin{aligned} d(w_1, \ldots, w_n) &= \sum_{\sigma \in S_n} \alpha_{1\sigma(1)} \cdots \alpha_{n\sigma(n)} (-1)^\sigma \det B \\ &= (\det B) \sum_{\sigma \in S_n} (-1)^\sigma \alpha_{1\sigma(1)} \cdots \alpha_{n\sigma(n)} \\ &= (\det B)(\det A). \end{aligned}$$

We now wish to identify $d(w_1, \ldots, w_n)$ as $\det(AB)$. However, since

$$w_1 = \alpha_{11}u_1 + \cdots + \alpha_{1n}u_n, w_2 = \alpha_{21}u_1 + \cdots + \alpha_{2n}u_n, \ldots, w_n = \alpha_{n1}u_1 + \cdots + \alpha_{nn}u_n$$

we get that $d(w_1, \ldots, w_n)$ is $\det C$ where the first row of C is w_1, the second is w_2, etc.

However, if we write out w_1, in terms of coordinates we obtain

$$\begin{aligned} w_1 &= \alpha_{11}u_1 + \cdots + \alpha_{1n}u_n = \alpha_{11}(\beta_{11}, \beta_{12}, \ldots, \beta_{1n}) \\ &\quad + \cdots + \alpha_{1n}(\beta_{n1}, \ldots, \beta_{nn}) \\ &= (\alpha_{11}\beta_{11} + \alpha_{12}\beta_{21} + \cdots + \alpha_{1n}\beta_{n1}, \alpha_{11}\beta_{12} + \cdots \\ &\quad + \alpha_{1n}\beta_{n2}, \ldots, \alpha_{11}\beta_{1n} + \cdots + \alpha_{1n}\beta_{nn}) \end{aligned}$$

which is the first row of AB. Similarly w_2 is the second row of AB, and so for the other rows. Thus we have $C = AB$. Since $\det(AB) = \det C = d(w_1, \ldots, w_n) = (\det A)(\det B)$, we have proved the theorem.

COROLLARY 1 *If A is invertible then* $\det A \neq 0$ *and* $\det(A^{-1}) = (\det A)^{-1}$.

Proof Since $AA^{-1} = 1$, $\det(AA^{-1}) = \det 1 = 1$. Thus by the theorem, $1 = \det(AA^{-1}) = (\det A)(\det A^{-1})$. This relation then states that $\det A \neq 0$ and $\det A^{-1} = 1/\det A$.

COROLLARY 2 *If A is invertible then for all B,* $\det(ABA^{-1}) = \det B$.

Proof. Using the theorem, as applied to $(AB)A^{-1}$, we get $\det((AB)A^{-1}) = \det(AB) \det(A^{-1}) = \det A \det B \det(A^{-1})$. Invoking Corollary 1, we reduce this further to $\det B$. Thus $\det(ABA^{-1}) = \det B$.

LEMMA 6.9.6 $\det A = \det (A')$.

Proof. Let $A = (\alpha_{ij})$ and $A' = (\beta_{ij})$; of course, $\beta_{ij} = \alpha_{ji}$. Now

$$\det A = \sum_{\sigma \in S_n} (-1)^\sigma \alpha_{1\sigma(1)} \cdots \alpha_{n\sigma(n)}$$

while

$$\det A' = \sum_{\sigma \in S_n} (-1)^\sigma \beta_{1\sigma(1)} \cdots \beta_{n\sigma(n)} = \sum_{\sigma \in S_n} (-1)^\sigma \alpha_{\sigma(1)1} \cdots \alpha_{\sigma(n)n}.$$

However, the term $(-1)^\sigma \alpha_{\sigma(1)1} \cdots \alpha_{\sigma(n)n}$ is equal to $(-1)^\sigma \alpha_{1\sigma^{-1}(1)} \cdots \alpha_{n\sigma^{-1}(n)}$. (Prove!) But σ and σ^{-1} are of the same parity, that is, if σ is odd, then so is σ^{-1}, whereas if σ is even then σ^{-1} is even. Thus

$$(-1)^\sigma \alpha_{1\sigma^{-1}(1)} \cdots \alpha_{n\sigma^{-1}(n)} = (-1)^{\sigma^{-1}} \alpha_{1\sigma^{-1}(1)} \cdots \alpha_{n\sigma^{-1}(n)}.$$

Finally as σ runs over S_n then σ^{-1} runs over S_n. Thus

$$\begin{aligned} \det A' &= \sum_{\sigma^{-1} \in S_n} (-1)^{\sigma^{-1}} \alpha_{1\sigma^{-1}(1)} \cdots \alpha_{n\sigma^{-1}(n)} \\ &= \sum_{\sigma \in S_n} (-1)^\sigma \alpha_{1\sigma(1)} \cdots \alpha_{n\sigma(n)} \\ &= \det A. \end{aligned}$$

In light of Lemma 6.9.6, interchanging the rows and columns of a matrix does not change its determinant. *But then Lemmas 6.9.2–6.9.5, which held for operations with rows of the matrix, hold equally for the columns of the same matrix.*

We make immediate use of the remark to derive *Cramer's rule* for solving a system of linear equations.

Given the system of linear equations

$$\begin{aligned} \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n &= \beta_1 \\ &\vdots \\ \alpha_{n1}x_1 + \cdots + \alpha_{nn}x_n &= \beta_n, \end{aligned}$$

we call $A = (\alpha_{ij})$ the matrix of the system and $\Delta = \det A$ the *determinant of the system.*

Suppose that $\Delta \neq 0$; that is,

$$\Delta = \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{vmatrix} \neq 0.$$

By Lemma 6.9.2 (as modified for columns instead of rows),

$$x_i\Delta = \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1i}x_i & \cdots & \alpha_{1n} \\ \vdots & & & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{ni}x_i & \cdots & \alpha_{nn} \end{vmatrix}.$$

However, as a consequence of Lemmas 6.9.3, 6.9.4, we can add any multiple of a column to another without changing the determinant (see Problem 5). Add to the ith column of $x_i\Delta$, x_1 times the first column, x_2 times the second, $\ldots$, x_j times the jth column (for $j \neq i$). Thus

$$x_i\Delta = \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1,i-1} & (\alpha_{11}x_1 + \alpha_{12}x_2 + \cdots + \alpha_{1n}x_n) & \alpha_{1,i+1} & \cdots & \alpha_{1n} \\ \vdots & & \vdots & \vdots & & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{n,i-1} & (\alpha_{n1}x_1 + \alpha_{n2}x_2 + \cdots + \alpha_{nn}x_n) & \alpha_{n,i+1} & \cdots & \alpha_{nn} \end{vmatrix}$$

and using $\alpha_{k1}x_1 + \cdots + \alpha_{kn}x_n = \beta_k$, we finally see that

$$x_i\Delta = \begin{vmatrix} \alpha_{11} & \cdots & \alpha_{1,i-1} & \beta_1 & \alpha_{1,i+1} & \cdots & \alpha_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \alpha_{1n} & \cdots & \alpha_{n,i-1} & \beta_n & \alpha_{n,i+1} & \cdots & \alpha_{nn} \end{vmatrix} = \Delta_i, \quad \text{say.}$$

Hence, $x_i = \Delta_i/\Delta$. This is

THEOREM 6.9.2 (CRAMER'S RULE) *If the determinant, Δ, of the system of linear equations*

$$\begin{aligned} \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n &= \beta_1 \\ &\vdots \\ \alpha_{n1}x_1 + \cdots + \alpha_{nn}x_n &= \beta_n \end{aligned}$$

is different from 0, then the solution of the system is given by $x_i = \Delta_i/\Delta$, where Δ_i is the determinant obtained from Δ by replacing in Δ the ith column by $\beta_1, \beta_2, \ldots, \beta_n$.

THEOREM 6.9.3 *A is invertible if and only if* $\det A \neq 0$.

Proof. If A is invertible, we have seen, in Corollary 1 to Theorem 6.9.1, that $\det A \neq 0$.

Suppose, on the other hand, that $\det A \neq 0$ where $A = (\alpha_{ij})$. By Cramer's rule we can solve the system

$$\begin{aligned} \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n &= \beta_1 \\ &\vdots \\ \alpha_{n1}x_1 + \cdots + \alpha_{nn}x_n &= \beta_n \end{aligned}$$

for $x_1, \ldots, x_n$ given arbitrary $\beta_1, \ldots, \beta_n$. Thus, as a linear transformation on $F^{(n)}$, A' is onto; in fact the vector $(\beta_1, \ldots, \beta_n)$ is the image under A' of $\left(\frac{\Delta_1}{\Delta}, \ldots, \frac{\Delta_n}{\Delta}\right)$. Being onto, by Theorem 6.1.4, A' is invertible, hence A is invertible (Prove!).

We can see Theorem 6.9.3 from an alternative, and possibly more interesting, point of view. Given $A \in F_n$ we can embed it in K_n where K is an extension of F chosen so that in K_n, A can be brought to triangular form. Thus there is a $B \in K_n$ such that

$$BAB^{-1} = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ & \lambda_2 & & \\ * & & \ddots & \vdots \\ & & & \lambda_n \end{pmatrix};$$

here $\lambda_1, \ldots, \lambda_n$ are all the characteristic roots of A, each occurring as often as its multiplicity as a characteristic root of A. Thus $\det A = \det(BAB^{-1}) = \lambda_1 \lambda_2 \cdots \lambda_n$ by Lemma 6.9.1. However, A is invertible if and only if none of its characteristic roots is 0; but $\det A \neq 0$ if and only if $\lambda_1 \lambda_2 \cdots \lambda_n \neq 0$, that is to say, if no characteristic root of A is 0. Thus A is invertible if and only if $\det A \neq 0$.

LEMMA 6.9.7 det A *is the product, counting multiplicities, of the characteristic roots of* A.

DEFINITION Given $A \in F_n$, the *secular equation* of A is the polynomial $\det(x - A)$ in $F[x]$.

Hermitian, Unitary, and Normal Transformations

DEFINITION The linear transformation $T \in A(V)$ is said to be *unitary* if $(uT, vT) = (u, v)$ for all $u, v \in V$.

LEMMA 6.10.2 *If* $(vT, vT) = (v, v)$ *for all* $v \in V$ *then* T *is unitary.*

Proof. The proof is in the spirit of that of Lemma 6.10.1. Let $u, v \in V$: by assumption $((u + v)T, (u + v)T) = (u + v, u + v)$. Expanding this out and simplifying, we obtain

$$(uT, vT) + (vT, uT) = (u, v) + (v, u), \tag{1}$$

for $u, v \in V$. In (1) replace v by iv; computing the necessary parts, this yields

$$-(uT, vT) + (vT, uT) = -(u, v) + (v, u). \tag{2}$$

Adding (1) and (2) results in $(uT, vT) = (u, v)$ for all $u, v \in V$, hence T is unitary.

THEOREM 6.10.1 *The linear transformation T on V is unitary if and only if it takes an orthonormal basis of V into an orthonormal basis of V.*

Proof. Suppose that $\{v_1, \ldots, v_n\}$ is an orthonormal basis of V; thus $(v_i, v_j) = 0$ for $i \neq j$ while $(v_i, v_i) = 1$. We wish to show that if T is unitary, then $\{v_1 T, \ldots, v_n T\}$ is also an orthonormal basis of V. But $(v_i T, v_j T) = (v_i, v_j) = 0$ for $i \neq j$ and $(v_i T, v_i T) = (v_i, v_i) = 1$, thus indeed $\{v_1 T, \ldots, v_n T\}$ is an orthonormal basis of V.

On the other hand, if $T \in A(V)$ is such that both $\{v_1, \ldots, v_n\}$ and $\{v_1 T, \ldots, v_n T\}$ are orthonormal bases of V, if $u, w \in V$ then

$$u = \sum_{i=1}^{n} \alpha_i v_i, \qquad w = \sum_{i=1}^{n} \beta_i v_i,$$

whence by the orthonormality of the v_i's,

$$(u, w) = \sum_{i=1}^{n} \alpha_i \bar{\beta}_i.$$

However,

$$uT = \sum_{i=1}^{n} \alpha_i v_i T \quad \text{and} \quad wT = \sum_{i=1}^{n} \beta_i v_i T$$

whence by the orthonormality of the $v_i T$'s,

$$(uT, wT) = \sum_{i=1}^{n} \alpha_i \bar{\beta}_i = (u, w),$$

proving that T is unitary.

DEFINITION If $T \in A(V)$ then the *Hermitian adjoint* of T, written as T^*, is defined by $(uT, v) = (u, vT^*)$ for all $u, v \in V$.

LEMMA 6.10.4 *If $T \in A(V)$ then $T^* \in A(V)$. Moreover,*

1. $(T^*)^* = T$;
2. $(S + T)^* = S^* + T^*$;
3. $(\lambda S)^* = \bar{\lambda} S^*$;
4. $(ST)^* = T^* S^*$;

for all $S, T \in A(V)$ and all $\lambda \in F$.

Proof. We must first prove that T^* is a linear transformation on V. If u, v, w are in V, then $(u, (v + w)T^*) = (uT, v + w) = (uT, v) + (uT, w) = (u, vT^*) + (u, wT^*) = (u, vT^* + wT^*)$, in consequence of which $(v + w)T^* = vT^* + wT^*$. Similarly, for $\lambda \in F$, $(u, (\lambda v)T^*) = (uT, \lambda v) = \bar{\lambda}(uT, v) = \bar{\lambda}(u, vT^*) = (u, \lambda(vT^*))$, whence $(\lambda v)T^* = \lambda(vT^*)$. We have thus proved that T^* is a linear transformation on V.

To see that $(T^*)^* = T$ notice that $(u, v(T^*)^*) = (uT^*, v) = \overline{(v, uT^*)} = \overline{(vT, u)} = (u, vT)$ for all $u, v \in V$ whence $v(T^*)^* = vT$ which implies that $(T^*)^* = T$. We leave the proofs of $(S + T)^* = S^* + T^*$ and of $(\lambda T)^* = \bar{\lambda}T^*$ to the reader. Finally, $(u, v(ST)^*) = (uST, v) = (uS, vT^*) = (u, vT^*S^*)$ for all $u, v \in V$; this forces $v(ST)^* = vT^*S^*$ for every $v \in V$ which results in $(ST)^* = T^*S^*$.

LEMMA 6.10.5 *$T \in A(V)$ is unitary if and only if $TT^* = 1$.*

Proof. If T is unitary, then for all $u, v \in V$, $(u, vTT^*) = (uT, vT) = (u, v)$ hence $TT^* = 1$. On the other hand, if $TT^* = 1$, then $(u, v) = (u, vTT^*) = (uT, vT)$, which implies that T is unitary.

THEOREM 6.10.2 *If $\{v_1, \ldots, v_n\}$ is an orthonormal basis of V and if the matrix of $T \in A(V)$ in this basis is (α_{ij}) then the matrix of T^* in this basis is (β_{ij}), where $\beta_{ij} = \bar{\alpha}_{ji}$.*

Proof. Since the matrices of T and T^* in this basis are, respectively, (α_{ij}) and (β_{ij}), then

$$v_iT = \sum_{i=1}^{n} \alpha_{ij}v_j \quad \text{and} \quad v_iT^* = \sum_{i=1}^{n} \beta_{ij}v_j.$$

Now

$$\beta_{ij} = (v_i T^*, v_j) = (v_i, v_j T) = \left(v_i, \sum_{i=1}^{n} \alpha_{jk} v_k\right) = \bar{\alpha}_{ji}$$

by the orthonormality of the v_i's. This proves the theorem.

DEFINITION $T \in A(V)$ is called *self-adjoint* or *Hermitian* if $T^* = T$.

If $T^* = -T$ we call *skew-Hermitian*. Given any $S \in A(V)$,

$$S = \frac{S + S^*}{2} + i\left(\frac{S - S^*}{2i}\right),$$

and since $(S + S^*)/2$ and $(S - S^*)/2i$ are Hermitian, $S = A + iB$ where both A and B are Hermitian.

THEOREM 6.10.3 *If $T \in A(V)$ is Hermitian, then all its characteristic roots are real.*

Proof. Let λ be a characteristic root of T; thus there is a $v \neq 0$ in V such that $vT = \lambda v$. We compute: $\lambda(v, v) = (\lambda v, v) = (vT, v) = (v, vT^*) = (v, vT) = (v, \lambda v) = \bar{\lambda}(v, v)$; since $(v, v) \neq 0$ we are left with $\lambda = \bar{\lambda}$ hence λ is real.

LEMMA 6.10.6 *If $S \in A(V)$ and if $vSS^* = 0$, then $vS = 0$.*

Proof. Consider (vSS^*, v); since $vSS^* = 0$, $0 = (vSS^*, v) = (vS, v(S^*)^*) = (vS, vS)$ by Lemma 6.10.4. In an inner-product space, this implies that $vS = 0$.

COROLLARY *If T is Hermitian and $vT^k = 0$ for $k \geq 1$ then $vT = 0$.*

Proof. We show that if $vT^{2^m} = 0$ then $vT = 0$; for if $S = T^{2^{m-1}}$, then $S^* = S$ and $SS^* = T^{2^m}$, whence $(vSS^*, v) = 0$ implies that $0 = vS = vT^{2^{m-1}}$. Continuing down in this way, we obtain $vT = 0$. If $vT^k = 0$, then $vT^{2^m} = 0$ for $2^m > k$, hence $vT = 0$.

DEFINITION $T \in A(V)$ is said to be *normal* if $TT^* = T^*T$.

LEMMA 6.10.7 *If N is a normal linear transformation and if $vN = 0$ for $v \in V$, then $vN^* = 0$.*

Proof. Consider (vN^*, vN^*); by definition, $(vN^*, vN^*) = (vN^*N, v) = (vNN^*, v)$, since $NN^* = N^*N$. However, $vN = 0$, whence, certainly, $vNN^* = 0$. In this way we obtain that $(vN^*, vN^*) = 0$, forcing $vN^* = 0$.

COROLLARY 1 *If λ is a characteristic root of the normal transformation N and if $vN = \lambda v$ then $vN^* = \bar{\lambda}v$.*

Proof. Since N is normal, $NN^* = N^*N$, therefore, $(N - \lambda)(N - \lambda)^* = (N - \lambda)(N^* - \bar{\lambda}) = NN^* - \lambda N^* - \bar{\lambda}N + \lambda\bar{\lambda} = N^*N - \lambda N^* - \bar{\lambda}N + \lambda\bar{\lambda} = (N^* - \bar{\lambda})(N - \lambda) = (N - \lambda)^*(N - \lambda)$, that is to say, $N - \lambda$ is normal. Since $v(N - \lambda) = 0$ by the normality of $N - \lambda$, from the lemma, $v(N - \lambda)^* = 0$, hence $vN^* = \bar{\lambda}v$.

COROLLARY 2 *If T is unitary and if λ is a characteristic root of T, then $|\lambda| = 1$.*

Proof. Since T is unitary it is normal. Let λ be a characteristic root of T and suppose that $vT = \lambda v$ with $v \neq 0$ in V. By Corollary 1, $vT^* = \bar{\lambda}v$, thus $v = vTT^* = \lambda vT^* = \lambda\bar{\lambda}v$ since $TT^* = 1$. Thus we get $\lambda\bar{\lambda} = 1$, which, of course, says that $|\lambda| = 1$.

LEMMA 6.10.8 *If N is normal and if $vN^k = 0$, then $vN = 0$.*

Proof. Let $S = NN^*$; S is Hermitian, and by the normality of N, $vS^k = v(NN^*)^k = vN^k(N^*)^k = 0$. By the corollary to Lemma 6.10.6, we deduce that $vS = 0$, that is to say, $vNN^* = 0$. Invoking Lemma 6.10.6 itself yields $vN = 0$.

COROLLARY *If N is normal and if for $\lambda \in F$, $v(N - \lambda)^k = 0$, then $vN = \lambda v$.*

Proof. From the normality of N it follows that $N - \lambda$ is normal, whence by applying the lemma just proved to $N - \lambda$ we obtain the corollary.

Real Quadratic Forms

DEFINITION Two real symmetric matrices A and B are *congruent* if there is a nonsingular real matrix T such that $B = TAT'$.

LEMMA 6.11.1 *Congruence is an equivalence relation.*

Proof. Let us write, when A is congruent to B, $A \cong B$.

1. $A \cong A$ for $A = 1A1'$.
2. If $A \cong B$ then $B = TAT'$ where T is nonsingular, hence $A = SBS'$ where $S = T^{-1}$. Thus $B \cong A$.
3. If $A \cong B$ and $B \cong C$ then $B = TAT'$ while $C = RBR'$, hence $C = RTAT'R' = (RT)A(RT)'$, and so $A \cong C$.

Possible Questions

PART-B (6 Mark)

1. If $\{v_1, v_2, \ldots, v_n\}$ is an Orthonormal basis of V and if the matrix of $T \epsilon A(V)$ in this basis is (α_{ij})then the matrix of T^* in this basis is $(\square_{ij})$, where $\square_{ij} = \overline{\alpha}_{ij.}$

2. If F is field of characteristic 0, and if $T \epsilon A_F(V)$ is such that tr $T^i=0$ for all $i \geq 1$ then prove that T is nilpotent.

3. The Linear transformation T on V is unitary if and only if it takes an orthonormal basis of V into an orthonormal basis of V.

4. Show that if two rows of a matrix A are equal, then prove that detA=0.

5. For A, $B \in F_n$ and $\lambda \in F$, prove
   (i) tr $(\lambda A) = \lambda$ tr (A)
   (ii) tr (A+B) = tr(A)+tr(B)
   (iii) tr (AB) = tr(BA).

6. Prove that if F is of characteristic 0 and if S and T, in $A_F(V)$,are such that ST-TS commutes with S, then prove that ST-TS is nilpotent.

7. Prove For A, $B \epsilon F_n$, det (AB) = (det A) (det B).

8. For A, $B \epsilon F_n$, prove that det (AB)=(det A)(det B).

9. If $T \epsilon A(V)$ is Hermitian, then all its characteristic roots are real.

PART-C (10 Mark)

1. For all A, $B \in F_n$ prove that
   (i) $(A')'=A$.
   (ii) $(A+B)'=A'+B'$
   (iii) $(AB)'=B'A'$.

2. If F is field of characteristic 0, and if $T \epsilon A_F(V)$ is such that tr $T^i=0$ for all $i \geq 1$ then prove that T is nilpotent.

3. Prove that if F is of characteristic 0 and if S and T, in $A_F(V)$,are such that ST-TS commutes with S, then prove that ST-TS is nilpotent.

KARPAGAM ACADEMY OF HIGHER EDUCATION
DEPARTMENT OF MATHEMATICS
ALBEBRA (18MMP101)

UNIT - V

Questions	choice 1	choice 2	choice 3	choice 4	Answer
If V is finite dimensional and ---------- there is an S∈A(V) such that E=TS ≠0 is an idempotent	T>0	T=0	T≠0	T<0	T≠0
If V is finite dimensional and T≠0 there is an S∈A(V) such that E=-------- is an idempotent	T>0	TS≠0	T≠0	TS=0	TS≠0
If V is finite dimensional and T≠0 there is an S∈A(V) such that E=TS ≠0 is an ----------	regular	idempotent	grounded	nilpotent	idempotent
The ---------- W of V is invariant under T∈A(V) if WT⊂W	subspace	space	field	sub field	subspace
The subspace W of V is invariant under T∈A(V) if----------	W over F	W⊂ TV	WT⊂T	W= TV	WT⊂T
The element λ ∈ F is a characteristic root of T ∈A(V) if and only if for some ------- in V, vT=λv	λ=0	λ≠0	v=0	v≠0	v≠0
The element λ ∈ F is a characteristic root of T ∈A(V) if and only if for some v≠0 in V,----------	vT=T	vT=λv	vT=v	Tv=T	vT=λv
If T ∈A(V) is nilpotent then k is called the ----------of Tk=0 but T^{k-1} ≠0	index of nilpotence	nilpotence	linear transformation	idempotent	index of nilpotence
The -------- of a matrix A is the sum of the elements on the main diagonal of A	transpose	inverse	trase	conjucate	trase
The trace of a matrix A is the ---------- of the elements on the main diagonal of A	sum	inverse	product	subtract	sum
The trace of a matrix A is the sum of the elements on the --------- of A	diagonal	main diagonal	elements	all elements	main diagonal
The matrix A is said tobe a---------- if A'=A	symmetric matrix	singular matrix	nonsingular matrix	skew-symmetric matrix	symmetric matrix
The matrix A is said to be a symmetric matrix if A'=A	A≠A'	A<A'	A>A'	A'=A	A'=A
The matrix A is said to be a---------- if A'=-A	symmetric matrix	singular matrix	nonsingular matrix	skew-symmetric matrix	skew-symmetric matrix
The matrix A is said to be a skew- symmetric matrix if --------	A≠A'	A<A'	A'=- A	A'=A	A'=- A
A and B are symmetric matrices,AB is ---------- iff AB=BA	symmetric matrix	singular matrix	nonsingular matrix	skew-symmetric matrix	symmetric matrix
A and B are symmetric matrices,AB is symmetric iff ----------	A=B	AB=BA	A≠B	AB≠BA	AB=BA
The determinant of a triangular matrix is the ---------- of its entries on the main diogonal	sum	inverse	product	subtract	product
The determinant of a triangular matrix is the product of its entries on the----------	diagonal	main diagonal	elements	all elements	main diagonal
The of a triangular matrix is the product of its entries on the main diogonal	transpose	inverse	trase	determinant	determinant
Interchanging two rows of A changing the sign of its ----------	transpose	inverse	trase	determinant	determinant
Interchanging two rows of A changing the---------- of its determinant	value	sign	sign and value	transpose	sign
Interchanging two columns of A changing the sign of its ----------	transpose	inverse	trase	determinant	determinant
Interchanging two columns of A changing the ------- of its determinant	value	sign	sign and value	transpose	sign

The characteristic roots of A are the roots with the correct multiplicity of the secular equation , ------- of A	det (x-A)	det(x-a)	dm (x-a)	dim(x+A)	det (x-A)
The ---------- of A are the roots with the correct multiplicity of the secular equation ,det (x-A) of A	root	multiple root	characteristic roots	product roots	characteristic roots
The characteristic roots of A are the roots with the correct multiplicity of the---------- , det(x-A) of A	linear equation	secular equation	non linear equation	non-secular equation	secular equation
A polynomial with coefficients which are ---------has all its roots in the complex field	real number	complex numbers	rational number	irrational number	complex numbers
A polynomial with coefficients which are complex numbers has all its------ in the complex field	root	multiple root	characteristic roots	product roots	root
A polynomial with coefficients which are complex numbers has all its roots in the ---	real field	rational field	complex field	irrational field	complex field
The ----------T ∈A(V) is said to be unitary if (uT,vT)=(u,v) for all u,v∈V	normal transformation	linear transformation	unitary	Nilpotent transformation	linear transformation
The linear transformation T ∈A(V) is said to be---------- if (uT,vT)=(u,v) for all u,v∈V	normal transformation	linear transformation	unitary	Nilpotent transformation	unitary
The linear transformation T ∈A(V) is said to be unitary if (uT,vT)= for all u,v∈V	(u,v)	uv	uT	vT	(u,v)
The ---------- Ton V is unitary if and only if it takes an orthonormal basis of V into an orthonormal basis of V	normal transformation	linear transformation	unitary	Nilpotent transformation	linear transformation
The linear transformation Ton V is unitary if and only if it takes an---------- of V into an orthonormal basis of V	basis	orthogonal basis	orthonormal basis	normal basis	orthonormal basis
The linear transformation Ton V is unitary if and only if it takes an orthonormal basis of V into an -------- of V	basis	orthogonal basis	orthonormal basis	normal basis	orthonormal basis
T∈A(V) is unitary if and only if----------	TT*=1	TT*>1	TT*<1	TT*≤1	TT*=1
T∈A(V) is --------- if and only if TT* =1	normal transformation	linear transformation	unitary	Nilpotent transformation	unitary
T∈A(V) is called harmitian if T*=T	normal transformation	harmition	unitary	Nilpotent transformation	harmition
T∈A(V) is called harmitian if ----------	T=T*	T=1	T≠T*	TT*=1	T≠T*
If T ∈A(V) isHermitian then all its --------- are real	root	multiple root	characteristic roots	product roots	characteristic roots
If T ∈A(V) isHermitian then all its characteristic roots are ----------	real	complex	rational	irrational	real
If T ∈A(V) is --------- then all its characteristic roots are real	normal transformation	harmition	unitary	Nilpotent transformation	harmition
If T ∈A(V) is --------- if TT*=T*T	normal	harmition	unitary	Nilpotent	normal
If T ∈A(V) is normal if ----------	T=T*	T=1	T=T*	TT*=1	T=T*
The Hermitian ---------- T is non negative if and only if its characterstic roots are non negative	normal transformation	linear transformation	unitary	Nilpotent transformation	linear transformation
The Hermitian linear transformation T is non negative if and only if its---------- are non negative	root	multiple root	characteristic roots	product roots	characteristic roots
The Hermitian linear transformation T is non negative if and only if its characterstic roots are ----------	non negative	negative	rational	irrational	non negative
The Hermitian linear transformation T is ----------if and only if its characterstic roots are non-negative	non negative	negative	rational	irrational	non negative