REPRESENTATIONS OF A FINITE GROUP IN POSITIVE CHARACTERISTIC

AMRITANSHU PRASAD

Abstract. An element x of a finite group G is said to be *p-regular* if its order is not divisible by p. Brauer gave several proofs of the fact that the number of isomorphism classes of irreducible representations of G over an algebraically closed field of characteristic p is the same as the number of conjugacy classes in G that consist of p-regular elements. One such proof is presented here.

Let G be a finite group, and K be any field. Then the group algebra $K[G]$ is a K-vector space with basis consisting of the elements of G:

$$K[G] = \Big\{ \sum_{g\in G} a_g g \mid a_g \in K \Big\}.$$

Multiplication is defined by linearly extending the product on basis elements

$$g \cdot h = gh \text{ for } g, h \in G$$

to $K[G]$. The group algebra was introduced by the German mathematician *Ferdinand Georg Frobenius* in 1897 to study the representations of finite groups.

Exercise 1. Let $n > 1$ be an integer. Let $\mathbf{Z}/n\mathbf{Z}$ denote the cyclic group with n elements. Show that $K[\mathbf{Z}/n\mathbf{Z}]$ is isomorphic to $K[t]/(t^n - 1)$.

In this article, the term $K[G]$-module will be used to refer to a a vector space M over K, together with an algebra homomorphism $R : K[G] \to \mathrm{End}_K(M)$, where $\mathrm{End}_K(M)$ denotes the algebra of K-linear maps from M to itself. In practice, for any $a \in K[G]$ and $m \in M$, the element $R(a)(m)$ of M will be denoted simply by am. For any vector space M, let $GL(M)$ denote the group of invertible K-linear maps from M to itself. Recall that a representation of G over the field K consists of a vector space M over K and a function $r : G \to GL(M)$ such that $r(gh) = r(g)r(h)$ for all $g, h \in G$. Such a vector space becomes a $K[G]$-module under the action

$$\Big(\sum_{g\in G} a_g g\Big) m = \sum_{g\in G} a_g r(g) m \qquad \text{for all } m \in V.$$

The representation r can be recovered from the $K[G]$-module structure by restricting to the basis elements of $K[G]$ coming from G. In fact, the study of $K[G]$-modules is equivalent to the study of representations of G over K (in a category-theoretic sense, which will not be formulated here). This article takes the module-theoretic viewpoint.

Two modules (or representations) are said to be *isomorphic* if there is an isomorphism between their underlying vector spaces which preserves the actions of the algebra (or group). A module defined by R and M as above is called *simple* if M is non-trivial and does not admit a non-trivial proper subspace that is invariant under $R(a)$ for every $a \in K[G]$. Similarly, a representation defined by r and M as above is called *irreducible* if M is non-trivial and does not admit a non-trivial proper subspace that is invariant under $r(g)$ for every $g \in G$. Simple $K[G]$-modules correspond to irreducible representations of G over K. Irreducible representations may be considered to be the building blocks of all representations, a point of view which is partially justified by the Jordan-Hölder theorem.

Frobenius showed that the number of isomorphism classes of irreducible representations of a finite group G over an algebraically closed field K of characteristic zero (such as the field of complex numbers) is equal to the number of conjugacy classes in G. In many modern textbooks this is deduced from the fact that the characters of irreducible representations form a basis of the space of class functions (see e.g., [Art94]). This result fails when the characteristic of K divides the order of the group G, as was pointed out by the American mathematician *Leonard Eugene Dickson* in the first decade of the twentieth century. The determination of the number of isomorphism classes of irreducible representations in this case remained open for a long time and was finally solved by another German mathematician, *Richard Brauer*, in 1935.

Even though Brauer was already a leading representation theorist, he lost his position at the University of Königsberg in Germany in 1933, after Hitler assumed dictatorial powers and started implementing his anti-semitic policies. Brauer moved to the United States, and then to Canada, and went on to become the most influential figure in modern representation theory. The result of Brauer that is discussed here is only the first of many discoveries that he made on representations in positive characteristic by analysing the ring-theoretic properties of group algebras. The most striking of these is known as *the theory of blocks*, which has been applied with great success to the study of the structure and the classification of finite simple groups. The reader who is interested in Brauer's life and work is referred to Curtis's remarkable book [Cur99], from where the proof of Brauer's theorem given here (originally due to Brauer himself) has been adapted. The standard reference for results on non-semisimple algebras and modular representations is [CR62]. A picture of developments in the general theory of modular representations up to 1980 is found in [Fei82]. Many newer developments can be found in [Ben91a] and [Ben91b].

Brauer's theorem is easy to state: an element of G is called *p-regular* if its order is not divisible by p. A *p-regular conjugacy class* is a conjugacy class consisting of p-regular elements.

Theorem (Brauer)**.** *When K is algebraically closed of characteristic $p > 0$, the number of isomorphism classes of simple $K[G]$-modules is equal to the number of p-regular conjugacy classes in G.*

This theorem follows from Propositions 7 and 9 below. The reader who is already familiar with the basic theory of associative algebras may proceed directly to these statements and their proofs.

In what follows K will always be an algebraically closed field and all K-algebras and all their modules will be assumed to be finite dimensional vector spaces over K. Every algebra A will be assumed to have a multiplicative unit $1 \in A$. For every module M it will be assumed that 1 acts on M as the identity (such a module is called *unital*). For two A-module M and N, $\mathrm{Hom}_A(M, N)$ will denote the A-module *homomorphisms* from M to N, namely those linear maps $\phi : M \to N$ for which $\phi(am) = a\phi(m)$ for all $a \in A$ and $m \in M$. $\mathrm{End}_A(M)$ will denote the space $\mathrm{Hom}_A(M, M)$ of *endomorphisms* of M. A *submodule* of M will be a subspace M' of M such that $am' \in M'$ for every $a \in A$ and $m' \in M'$. Note that the image and kernel of and A-module homomorphism is a submodule.

Definition. M is said to be a *simple* A-module if it is non-trivial and it contains no non-trivial proper submodules.

Theorem (Schur's lemma)**.**
(1) *If M is a simple A-module, then $\mathrm{End}_A(M) \cong K$.*
(2) *If both M and N are non-isomorphic simple A-modules, then $\mathrm{Hom}_A(M, N) = 0$.*

Proof. Suppose M is simple and $\phi \in \mathrm{End}_A(M)$. Then, since K is algebraically closed, ϕ has an eigenvalue $\lambda \in K$. $\phi - \lambda I$ is singular and lies in $\mathrm{End}_A(M)$. Its kernel is a non-trivial A-submodule. By the simplicity of M, this kernel must be all of M. Therefore $\phi = \lambda I$. The proof of the second assertion is an easy exercise for the reader. □

Suppose M is a simple A-module. Pick $m \in M$ such that $m \neq 0$. The map $\phi_m : A \to M$ given by

$$\phi_m(a) = am \text{ for all } a \in A$$

is an A-module homomorphism (here A is viewed as a left A-module). Since the image of ϕ_m is a non-trivial submodule of M, it must be all of M. Therefore, ϕ_m is surjective. Its kernel is a left ideal in A.

Conclusion. *Every simple A-module is isomorphic to a quotient of A by a left ideal.*

Definition. A left ideal N of A is said to be *nilpotent* if there exists a positive integer k such that $N^k = 0$ (here N^k is the vector space spanned by products of k elements in N).

Exercise 2. Suppose that K is an algebraically closed field of characteristic p, and that $n = pm$ for some positive integer m. Show that $(t^m - 1)$ generates a nilpotent ideal in $K[t]/(t^n - 1)$.

Proposition 1. *Every nilpotent left ideal of A is contained in the kernel of ϕ_m.*

Proof. Suppose that N is a left ideal of A not contained in $\ker \phi_m$. Then Nm is a non-trivial submodule of M, hence $Nm = M$. In particular, there exists $n \in N$ such that $nm = m$. It follows that $n^k m = m$ for every positive integer k. Therefore, every power of n is non-zero. N can not, therefore, be nilpotent. □

It is not always the case that a finite dimensional A-module is a direct sum of simple modules.

Exercise 3. Take K to be any field of characteristic two. Take A to be $K[\mathbf{Z}/2\mathbf{Z}]$. Show that A has a unique non-trivial proper submodule, which is spanned by $0+1$ (here 0 and 1 are the basis vectors). Conclude that A can not be written as a direct sum of simple A-modules.

Definition. An A-module M is said to be *semisimple* if it can be written as a direct sum of simple modules. A is called a *semisimple algebra* if, as an A-module, A is semisimple. A is called a *simple algebra* if it has no proper two-sided ideals.

Exercise 4. Suppose that K is a algebraically closed and that the characteristic of K does not divide n. Show that the equation $t^n - 1 = 0$ has n distinct roots.

Exercise 5. Assume that K is as in Exercise 4. Show that $K[\mathbf{Z}/n\mathbf{Z}]$ is semisimple (Hint: use Exercises 1 and 4).

Example. *Maschke's theorem* (see, e.g., [Art94, p. 316]) states that $K[G]$ is semisimple when the characteristic of K does not divide the order of G.

Exercise 6. (see [Lan99, p. 656]) Show that the algebra $M_n(K)$ of $n\times n$ matrices is simple (for example, by showing that the two-sided ideal generated by any non-zero matrix is all of $M_n(K)$). Show that every simple module is isomorphic to K^n (which can be thought of as the space of column vectors on which $M_n(K)$ acts on the left by multiplication).

Proposition 2. *Every semisimple algebra is a direct sum of simple algebras.*

Proof. Let A_1 be a minimal two-sided ideal of A. Let A' be a complement of A_1 (as a left A-module), so that $A = A_1 \oplus A'$. Suppose that the decomposition of 1 under the above direct sum decomposition is $1 = \epsilon_1 + \epsilon'$. The decomposition of $a \in A$ is given by $a = a\epsilon_1 + a\epsilon'$. In particular, $\epsilon_1 = \epsilon_1 1 = \epsilon_1(\epsilon_1 + \epsilon') = \epsilon_1^2 + \epsilon_1\epsilon'$. Therefore, $\epsilon_1^2 = \epsilon_1$ and $\epsilon_1\epsilon' = 0$. Similarly, $\epsilon'\epsilon_1 = 0$. We can also write $A = \epsilon_1 A \oplus \epsilon' A$, where the decomposition of $a \in A$ is given by $a = \epsilon_1 a + \epsilon' a$. If $a_1 \in A_1$, then comparing its two decompositions shows that $a_1 = a_1\epsilon_1 = \epsilon_1 a_1$. More generally, if $a \in A$, then $a\epsilon_1 = a\epsilon_1^2 = (a\epsilon_1)\epsilon_1$. But $a\epsilon_1 \in A_1$. Therefore, $(a\epsilon_1)\epsilon_1 = \epsilon_1(a\epsilon_1)$. A similar argument can be used to show that $\epsilon_1 a = (\epsilon_1 a)\epsilon_1$. Therefore $a\epsilon_1 = \epsilon_1 a$. Since $\epsilon' = 1 - \epsilon_1$, it also follows that $\epsilon' a = a\epsilon'$ for every $a \in A$. Therefore, $A' = A\epsilon' = \epsilon' A$, so that A' is also a two sided ideal. Now repeat this argument replacing A by A'. Continuing in this manner, one obtains that $A = A_1 \oplus \cdots \oplus A_s$ for some s, where the summands are minimal two-sided ideals, hence simple algebras. □

We now discuss another characterization of semisimple algebras. Firstly note that

Lemma 3. *The sum of two nilpotent left ideals is nilpotent.*

Proof. Suppose that N_1 and N_2 are two nilpotent left ideals. Take k such that $N_1^k = N_2^k = 0$. Every element of $(N_1 + N_2)^{2k}$ is a product of $2k$ terms of the form $(n_1 + n_2)$, where $n_1 \in N_1$ and $n_2 \in N_2$. In each term of the expansion of this product, either elements of N_1, or elements of N_2 occur at least k times, so that the term is either in N_1^k or N_2^k, and is therefore 0. □

Exercise 7. Show that $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ are nilpotent elements in $M_2(K)$, but their sum is not nilpotent. Why does this example not contradict Lemma 3?

Suppose that N is a nilpotent left ideal of A. If N is not maximal, then there exists a nilpotent ideal N' that is not contained in N. By Lemma 3, $N + N'$ is a nilpotent ideal, which strictly larger than N. From the finite dimensionality of A, it now follows that A has a unique maximal nilpotent left ideal, which is called the *radical* of A, denoted $\mathrm{Rad}A$. By Proposition 1, $\mathrm{Rad}A \subset \ker \phi_m$. Now $(\mathrm{Rad}A)A$ is a two-sided ideal. It is nilpotent because

$$[(\mathrm{Rad}A)A]^2 \subset (\mathrm{Rad}A)^2 A,\ [(\mathrm{Rad}A)A]^3 \subset (\mathrm{Rad}A)^3 A, \dots.$$

It follows that $(\mathrm{Rad}A)A \subset \mathrm{Rad}A$, and so $\mathrm{Rad}A$ is a two-sided ideal.

Exercise 8. If I is a two-sided ideal in A, show that the formulas $(a + I) + (b + I) = a + b + I$ and $(a + I)(b + I) = ab + I$ give rise to a well-defined algebra structure on the quotient space $\frac{A}{I}$.

This allows one to make sense of the quotient $\frac{A}{\mathrm{Rad}A}$ as an algebra.

Proposition 4. *A is semisimple if and only if* $\mathrm{Rad}A = 0$.

Proof. Suppose that A is semisimple. Then A, as a left A-module, can be written as a sum of simple A-modules:

$$A = M_1 \oplus \cdots \oplus M_k.$$

Suppose that $1 = e_1 + \cdots + e_k$ is the decomposition of 1. Then the identity map of A (which is right multiplication by 1) can be written as $\phi_{e_1} + \cdots + \phi_{e_m}$. By Proposition 1, $\mathrm{Rad}A \subset \cap_{i=1}^k \ker \phi_{e_i}$. On the other hand

$$\cap_{i=1}^k \ker \phi_{e_i} = \ker(\phi_{e_1} + \cdots + \phi_{e_k}) = 0.$$

Therefore, $\mathrm{Rad}A = 0$.

Conversely, suppose that $\mathrm{Rad}A = 0$. Then A has no non-trivial nilpotent left ideals. Let N be a minimal non-zero left ideal of A (as an A-module, N is simple). Then N^2 is a left ideal contained in N. Since $N^2 \neq 0$, $N^2 = N$. Therefore, there exists $a \in N$ such that $Na \neq 0$. But Na itself is a left ideal contained in N. Therefore, $Na = N$. It follows that $B = \{b \in N \mid ba \neq 0\}$ is a left ideal properly contained in N. Therefore $B = 0$. Moreover, since $Na = N$, $a = ca$ for some $c \in N$. Also $ca = c^2 a$, so that $(c - c^2)a = 0$. In other words, $c - c^2 \in B$. Therefore $c - c^2 = 0$. Therefore c is a non-zero idempotent in N. By the minimality of N, $Ac = N$. Moreover, $A = Ac \oplus A(1 - c)$. If $A(1 - c)$ is not simple, then take a minimal left ideal in $A(1 - c)$ and repeat the above process. Since A is a finite dimensional vector space, this process will end after a finite number of steps, resulting in a decomposition of A into a direct sum of simple modules. Therefore A is semisimple. ∎

Corollary 5. $\frac{A}{\mathrm{Rad}A}$ *is semisimple.*

Proof. Since Rad$A$ is a maximal nilpotent ideal, $\frac{A}{\mathrm{Rad}A}$ has no nilpotent ideals. By Proposition 4, $\frac{A}{\mathrm{Rad}A}$ is semisimple. $\square$

Exercise 9. Suppose that K has characteristic p, and let $n = pm$ for some positive integer m. Show that $K[\mathbf{Z}/n\mathbf{Z}]$ is not semisimple (Hint: use Exercises 1 and 2).

Corollary. *Every simple algebra is semisimple.*

Proof. Since Rad$A$ is a proper two-sided ideal, the simplicity of A implies that Rad$A = 0$. Therefore A is semisimple. $\square$

Theorem (Wedderburn)**.** *Every simple algebra is isomorphic to $M_n(K)$ for some positive integer n.*

Proof. Since A is semisimple, A (viewed as a left A-module) can be decomposed into a direct sum of simple A-modules. Let

$$A = M_1^{\oplus m_1} \oplus \cdots \oplus M_k^{\oplus m_k} \tag{6}$$

be such a decomposition where $M_1, \ldots, M_k$ are pairwise non-isomorphic. For each $a \in A$, the map $\phi_a : A \to A$ defined by $\phi_a(x) = xa$ is an A-module homomorphism $A \to A$. Moreover, $\phi_a \circ \phi_b = \phi_{ba}$. Conversely, every A-module homomorphism $\phi : A \to A$ is of the form ϕ_a, where $a = \phi(1)$. Therefore the A-module homomorphisms $A \to A$ form an algebra A^* whose elements are the same as those of A, but multiplication is reversed. A two-sided ideal of A is also a two sided ideal of this A^*. Therefore A^* is also simple. Schur's lemma can be used to show that $A^* = M_{m_1}(K) \oplus \cdots \oplus M_{m_k}(K)$. $M_{m_1}(K)$ is proper two-sided ideal of A^*. Therefore, by the simplicity A^* we must have $k = 1$ in (6) and $A^* = M_{m_1}(K)$. $\square$

Proposition 7. *Let A be a finite dimensional algebra over an algebraically closed field K of characteristic $p > 0$. Let*

$$S = \text{Span } \{ab - ba \mid a, b \in A\},$$
$$T = \{r \in A \mid r^q \in S \textit{ for some power } q \textit{ of } p\}.$$

Then T is a subspace of A, and the number of isomorphism classes of simple A-modules is $\dim_K(A/T)$.

Proof. In the expansion

$$(a + b)^p = \sum_{\epsilon_i \in \{a,b\}} \epsilon_1 \cdots \epsilon_p,$$

all the terms except a^p and b^p can be grouped into sets of p summands of the form

$$\epsilon_1 \cdots \epsilon_p + \epsilon_2 \cdots \epsilon_p \epsilon_1 + \cdots + \epsilon_p \epsilon_1 \cdots \epsilon_{p-1}.$$

All the terms in the above expansion are congruent modulo S, and so their sum vanishes modulo S. Therefore,

$$(a+b)^p \equiv a^p + b^p \mod S. \tag{8}$$

It follows T is closed under addition. It is clear that T is closed under multiplication by scalars in K. Hence T is a subspace of A.

Now take $u, v \in A$, and let $w = v(uv)^{p-1}$. Then

$$(uv - vu)^p \equiv (uv)^p - (vu)^p \equiv uw - wu \equiv 0 \mod S.$$

Therefore, the pth power of an element of S is again in S. Hence $S \subset T$.

Suppose now, that A is *simple*. By Wedderburn's theorem, A is isomorphic to $M_n(K)$ for some positive integer n. Claearly, for $A = M_n(K)$, every matrix in S has trace zero. The converse of this statement is also true: every matrix with trace zero lies in S. To see this for $n = 2$, note that

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \left[\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right],$$
$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right],$$
$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \left[\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right].$$

In the above equations, $ab - ba$ has been denoted $[a, b]$, which is customary. Similar identities can be used to obtain the result for arbitrary n. Since S consists of trace zero matrices, $\dim(A/S) = 1$, and since $S \subset T$, $\dim(A/T)$ must be 0 or 1. The matrix E_{11} for which the entry in the first row and first column is 1 and all other entries are 0 is never in T. Therefore T is a proper subspace of A. One must therefore have that $\dim(A/T) = 1$. On the other hand $M_n(K)$, being simple, has a unique simple module up to isomorphism. Therefore, Proposition 7 holds when A is simple.

For the general case, note that every nilpotent element of A is in T. Therefore, $\mathrm{Rad}A \subset T$. It follows from Proposition 7 that $\mathrm{Rad}A$ acts trivially on every simple A-module and that the number of isomorphism classes of simple modules is the same for A and $\frac{A}{\mathrm{Rad}A}$. $\frac{A}{\mathrm{Rad}A}$ is a direct sum $A_1 \oplus \cdots \oplus A_r$ of simple algebras by Corollary 5 and Proposition 2. A simple module for A_i becomes a simple module for $A_1 \oplus \cdots \oplus A_r$ when the other summands act trivially. Moreover, every simple module is obtained in this way. Therefore, $A_1 \oplus \cdots \oplus A_r$ (and hence A) has r isomorphism classes of simple modules. On the other hand, define T_i for A_i just as T was defined for A. Then A/T is a direct sum of the A_i/T_i's. Therefore, applying Proposition 7 in the simple case to A_i, we see that $\dim A/T = r$. □

Proposition 9. *Let K be an algebraically closed field of characteristic $p > 0$ and let $A = K[G]$. Then, the number of p-regular conjugacy classes in G is the same as* $\dim A/T$.

Proof. Every $x \in G$ can be written as $x = st$, where s is p-regular and the order of t is a power of p, for if the order of x is $n = n'p^e$, where n' is not divisible by p, then there exist integers a and b such that $ap^e + bn' = 1$, and one may take $s = x^{ap^e}$ and $t = x^{bn'}$. By (8),

$$(st - s)^p \equiv s^p t^p - s^p \mod S.$$

Consequently, if q is the order of t,

$$(st - s)^q \equiv s^q t^q - s^q \equiv 0 \mod S.$$

Therefore, $st - s \in T$, or $st \equiv s \mod T$. Therefore, every element of G (thought of as an element of $K[G]$) is congruent modulo T to a p-regular element. Furthermore, since T contains S, all elements in the same conjugacy class are equivalent modulo T. Therefore, the number of p-regular conjugacy classes in G is an upper bound for $\dim A/T$.

Suppose $R \subset G$ is a set of representatives of p-regular conjugacy classes. It remains to show that R is a linearly independent set in A/T. Suppose that $\sum a_r r \in T$ for some $a_r \in K$, $r \in R$. There exists a power q of p such that $r^q = r$ for every $r \in R$ (because p is a unit in $\mathbf{Z}/n'\mathbf{Z}$, where n' is the order of r), and such that $(\sum a_r r)^q \in S$. Therefore,

$$\left(\sum a_r r\right)^q \equiv \sum a_r^q r^q \equiv \sum a_r^q r \mod S,$$

and consequently, $\sum a_r^q r \in S$. But S consists of those elements of $K[G]$ with the property that the sum the coefficients of all the elements in each conjugacy class of G is zero (prove this). Therefore, a_r^q, and hence a_r is zero for every $r \in R$. It follows that R is linearly independent in A/T. □

Acknowledgements. The author is grateful to S. Ponnusamy and K. N. Ragahavan for helpful comments on preliminary drafts of this article. He thanks the students of TIFR for inviting him to give the lecture on which this article is based.

References

[Art94] Michael Artin. *Algebra*. Prentice Hall of India Private Limited, New Delhi, 1994.

[Ben91a] D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1991. Basic representation theory of finite groups and associative algebras.

[Ben91b] D. J. Benson. *Representations and cohomology. II*, volume 31 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1991. Cohomology of groups and modules.

[CR62] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[Cur99] Charles W. Curtis. *Pioneers of representation theory: Frobenius, Burnside, Schur, and Brauer*, volume 15 of *History of Mathematics*. American Mathematical Society, Providence, RI, 1999.

[Fei82] Walter Feit. *The representation theory of finite groups*, volume 25 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, 1982.

[Lan99] Serge Lang. *Algebra*. Addison-Wesley (International Student Edition), third edition, 1999.

E-mail address: `amri@imsc.res.in`
URL: `http://www.imsc.res.in/~amri`

The Institute of Mathematical Sciences, CIT campus, Taramani, Chennai 600113.