21-238, Math Studies Algebra 2, Department of Mathematical Sciences, Carnegie Mellon University
Spring 2012: Monday, Wednesday, Friday, 10:30 am, Doherty Hall 1211.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

1- Monday January 16, 2012.

After basic results about algebraic structures have been shown in a first semester, one should not deduce that algebra is such a small country that most of the interesting places have been described. Any course in mathematics is a choice of a path inside a "known" territory, although it may contain the description of conjectures, which are about what one may find behind the borders of that area (which expands with time because of research and development). Using geographical analogies may not always be relevant, but a country may have flat regions where it is easy to wander around, and hilly parts going to a mountainous area where it is harder to travel, although training in this region is worth the effort since it gives access to some places with a beautiful panoramic view; from there one may have a glimpse of a much further mountain range, which requires a different equipment, like for crossing a river, or a glacier, but if a large expanse has to be crossed, the exploration of a new area lying beyond it may force to postpone research for practicing development, so that many may easily arrive at the border of the territory to be explored. Similarly, there are easy results in algebra and more difficult ones, and there are areas where algebra is mixed with analysis, possibly for problems in geometry, with applications in various areas of science or engineering. I have noticed that some areas which were considered "pure mathematics" when I was a student have found applications since, but before boasting that mathematics is very useful for applications I suggest to check how much of algebra or any other part of mathematics is really used in each particular application.[1]

Although I shall be mostly interested in those applications of algebra which are used outside mathematics, it is useful to know a few definitions corresponding to generalizations which will not be studied here, like the general properties of modules. However, the case where the ring is a field corresponds to vector spaces, whose subject is called linear algebra,[2] which we have already encountered, but much more will be said about it, since it is extremely important for applications.

Definition 1.1: If R is a ring, a *left R-module* is an Abelian group $(M,+)$ equipped with a *scalar multiplication* $(r,m)\mapsto r\,m$ from $R\times M$ into M, such that $r\,(m_1+m_2)=r\,m_1+r\,m_2$, $(r_1+r_2)\,m=r_1m+r_2m$, $r_1(r_2m)=(r_1r_2)\,m$, so that $0\,m=0$ for all $r,r_1,r_2\in R$, and all $m,m_1,m_2\in M$. A left R-module M is *unital* if R is unital and $1\,m=m$ for all $m\in M$ ($m\,1=m$ for a right R-module). Similarly for a *right R-module*. A *two-sided R-module* is an Abelian group $(M,+)$ with both a left and a right module structure, satisfying the supplementary relation $r_1(m\,r_2)=(r_1m)\,r_2$ for all $r_1,r_2\in R$ and all $m\in M$.

Example 1.2: A ring R is a two-sided R-module. An Abelian group is a two-sided $\mathbb{Z}$-module.

Definition 1.3: If N is a left R-module, then $M\subset N$ is a *submodule* of N if M is an additive subgroup of N and $R\,M\subset M$, where $R\,M=\{r\,m\mid r\in R, m\in M\}$. M inherits a structure of left R-module, and one writes $M\le N$.

If M is a left R-module, and $X\subset M$, then a *linear combination* of elements of X has the form $\sum_{i=1}^m r_ix_i$, with $r_1,\ldots,r_m\in R$ and $x_1,\ldots,x_m\in X$. A subset of M is a submodule if and only if it is stable by linear combinations. The set of linear combinations of elements of X is denoted $\langle X\rangle$, and it is the smallest submodule containing X (for vector spaces, i.e. if R is a field, one calls it the span of X). A left R-module

[1] It is for this reason that in the first semester I avoided teaching the whole Galois theory, in order to check how much of it is needed for deducing the basic results on finite fields, in view of using them for coding theory: only the results on splitting field extensions were used, and it was not necessary to understand much about the Galois correspondence (between intermediate fields and subgroups of the Galois group).

[2] In many applications of linear algebra, the field used is $\mathbb{R}$ or $\mathbb{C}$, so that one often encounters questions from analysis: solving a linear system $A\,x=y$ can be done in a purely algebraic way, although implementing a particular algorithm when the field is $\mathbb{R}$ or $\mathbb{C}$ forces to observe that computers do not store real numbers but discrete approximations of them, and the propagation of (truncation) errors in algorithms then becomes useful; it then is natural to compute approximations of a solution by iterating schemes, whose convergence to the exact solution becomes a question of analysis.

M is *simple* if its only submodules are $\{0\}$ and M. A left R-module M is *finitely generated* if $M = \langle X \rangle$ for a finite set X, and it is *cyclic* if it is generated by one element m.

Example 1.4: Unlike for vector spaces, a module M can be finitely generated and nevertheless contain a submodule which is not finitely generated, as the following example (with M cyclic) shows. Let $R = \mathbb{Z}[x_1, x_2, \ldots]$ be the (unital) ring of all polynomials in infinitely many variables and with integer coefficients, so that R is cyclic (since it is generated by 1). Let I be the (two-sided) ideal generated by $\{x_1, x_2, \ldots\}$, which is a submodule of R which is not finitely generated. Indeed, if it was generated by $\{P_1, \ldots, P_k\}$ it would be generated by $\{x_1, \ldots, x_m\}$ if the variables appearing in $P_1, \ldots, P_k$ have an index $\leq m$, but all polynomials in $\langle x_1, \ldots, x_m \rangle$ give the value 0 if one evaluates them at $x_1 = \ldots = x_m = 0$ and $x_{m+1} = 1$, so that $x_{m+1} \notin \langle x_1, \ldots, x_m \rangle$.

Definition 1.5: A left R-module is *Noetherian* if and only if every increasing sequence of submodules is eventually constant; it is *Artinian* if and only if every decreasing sequence of submodules is eventually constant. The ring R is *left Noetherian* if it is Noetherian as a left R-module, i.e. if every increasing sequence of left ideals is eventually constant.

Remark 1.6: If R is a field F, one talks about F-vector spaces V; a vector space V is finitely generated if and only it has finite dimension, in which case it is both Noetherian and Artinian; a non-trivial vector space V is simple if and only if it has dimension 1; a field F is a Noetherian ring, since its only left ideals are $\{0\}$ and F.

Since submodules of $\mathbb{Z}$ coincide with its subgroups and have the form $a\,\mathbb{Z}$, and for $a, b \neq 0$, $a\,\mathbb{Z} \subset b\,\mathbb{Z}$ means $b \mid a$ (i.e. b divides a), one deduces that $\mathbb{Z}$ is Noetherian but not Artinian. It can be shown that the Noetherian $\mathbb{Z}$-modules are precisely the finitely generated Abelian groups.

Similarly to a result proved for Noetherian rings, if M is a left R-module, then M is Noetherian if and only if all its submodules are finitely generated.

Definition 1.7: A *module homomorphism* ψ of a left R-module M_1 into a left R-module M_2 is an homomorphism of groups (i.e. $\psi(a + b) = \psi(a) + \psi(b)$ for all $a, b \in M_1$), which satisfies $\psi(r\,m) = r\,\psi(m)$ for all $r \in R$ and all $m \in M$ (in the case of vector spaces, it is called a linear mapping). The *kernel* of ψ (i.e. $ker(\psi) = \{m \in M_1 \mid \psi(m) = 0\}$) is a submodule of M_1, and the *image* of ψ (i.e. $im(\psi) = \{\psi(m) \mid m \in M_1\}$) is a submodule of M_2.

If N is a left R-module and $M \leq N$, then the *quotient module* N/M has elements $n + M$, as for a quotient of Abelian groups, and $r\,(n + M)$ is defined as $r\,n + M$,[3] so that N/M is a left R-module, and the quotient map $n \mapsto n + M$ is an homomorphism.

Remark 1.8: One checks easily the first isomorphism theorem, that if ψ is a module homomorphism of a left R-module M_1 into a left R-module M_2, then $M_1/ker(\varphi) \simeq im(\varphi)$, by the bijection $m + ker(\varphi) \mapsto \varphi(m)$.

The natural mappings for rings are the ring-homomorphisms, whose kernels are exactly the two-sided ideals, so that the structure of left module on a ring R is exactly what is needed so that the kernels of the natural mappings (from R into left R-modules) are exactly the left ideals of R.

Definition 1.9: If M is a left R-module and $m \in M$, the *annihilator of* m is $Ann(m) = \{r \in R \mid r\,m = 0\}$, which is a left ideal of R, while the *annihilator of* M is $Ann(M) = \{r \in R \mid r\,m = 0 \text{ for all } m \in M\}$, which is a two-sided ideal of R.[4]

Definition 1.10: If G is a group and R is a ring, the *group ring* $R\,G$ is the set of functions from G into R which are non-zero only on a finite set, and one writes $\sum_i r_i g_i$ for the function taking the value r_i at g_i:

[3] For $r \in R$ and $n \in N$, the set $\{r\,(n + m) \mid m \in M\}$ is included in $r\,n + M$, and the inclusion may be strict with $r \neq 0$: if $N = \mathbb{Z}_8[x]$ is a left $\mathbb{Z}_8$-module, and one obtains a submodule $M \leq N$ by considering polynomials $P = \sum_n a_n x^n$ with $a_n \in \{0, 2, 4, 6\}$ for all n (i.e. $a_n = 0 \pmod 2$), then $2P = \sum_n b_n x^n$ with $b_n \in \{0, 4\}$ for all n.

[4] If $r \in Ann(m)$ and $s \in R$, one has $(s\,r)\,m = s\,(r\,m) = 0$, so that $s\,r \in Ann(m)$, showing that $Ann(m)$ is a left ideal, but without R being commutative, one cannot decide if $(r\,s)\,m$ is 0; however, if $r \in Ann(M)$, then $r \in Ann(s\,m)$ and $(r\,s)\,m = r\,(s\,m) = 0$, so that $r\,s \in Ann(M)$, showing that $Ann(M)$ is a two-sided ideal.

addition is pointwise and multiplication is $\left(\sum_i r_i g_i\right) \cdot \left(\sum_j r'_j g'_j\right) = \sum_{i,j} (r_i r'_j)\,(g_i g'_j)$. It is a left R-module, and if R is a field it is an R-vector space with G as a basis.

Definition 1.11: If G is a group, if F is a field and V is an F-vector space, a *representation of* G *on* V is an homomorphism ψ from G into $GL(V)$. The representation is *irreducible* if there is no non-trivial subspace $W \neq V$ invariant by all the $\psi(g), g \in G$.

Example 1.12: There is a representation of the symmetric group S_n (hence of every group G of order n since it is isomorphic to a subgroup of S_n) on F^n, by associating to $\sigma \in S_n$ the linear mapping $A_\sigma \in GL(F^n)$ defined by $A_\sigma e_i = e_{\sigma(i)}$ for $i = 1, \ldots, n$ (once a basis $e_1, \ldots, e_n$ has been chosen).

If $n \geq 2$, this representation is not irreducible, since the subspace $V = \{\sum_i x_i e_i \mid \sum_i x_i = 0\}$ is invariant by all the permutation matrices (because $\sum_i e_i$ is an eigenvector for A_σ^T for all σ, with eigenvalue 1).

Remark 1.13: Representations of groups play a role in physics, but I am not really sure what Wigner meant when he said that "elementary particles" are irreducible representations of the group of rotations $S\mathbb{O}(3)$.[5]

Example 1.14: If G is a group, if K is a field, and ψ is a representation of G on a K-vector space V, then V has a structure of left KG-module by defining $\left(\sum_i k_i g_i\right) v = \sum_i k_i \psi(g_i)(v)$.

Additional footnotes: Goeppert-Mayer,[5] Jensen J.H.D..[6]

[5] Jenõ Pál (Eugene Paul) Wigner, Hungarian-born physicist, 1902–1995. He shared the Nobel Prize in Physics in 1963, for his contributions to the theory of the atomic nucleus and the elementary particles, particularly through the discovery and application of fundamental symmetry principles, jointly with Maria Goeppert-Mayer and J. Hans D. Jensen, for their discoveries concerning nuclear shell structure. He emigrated to United States in 1933, and he worked at Princeton University, Princeton, NJ.

[5] Maria Goeppert-Mayer, German-born physicist, 1906–1972. She received the Nobel Prize in Physics in 1963, with J. Hans D. Jensen, for their discoveries concerning nuclear shell structure, jointly with Eugene P. Wigner. She worked in Chicago, IL, and at USCD (University of California San Diego), La Jolla, CA.

[6] J. Hans D. Jensen, German physicist, 1907–1963. He received the Nobel Prize in Physics in 1963, with Maria Goeppert-Mayer, for their discoveries concerning nuclear shell structure, jointly with Eugene P. Wigner. He worked in Hannover, and in Heidelberg, Germany.