MA 312 Commutative Algebra / January-April 2015

(Int PhD. and Ph. D. Programmes)

Tel : +91-(0)80-2293 3212/(CSA 2239) **E-mails :** patil@math.iisc.ernet.in / dppatil@csa.iisc.ernet.in

Lectures : Monday and Thursday ; 11:00–12:30 **Venue:** MA LH-3 (**if LH-1 is not free**) / LH-1

Midterms : **Quizzes :** **(Wed-Lect)**

Final Examination :

2. Modules and Submodules

Contents

§ 2 Modules and Submodules

2.A Modules

Let A be a ring. Operations of A on abelian groups V which are compatible with the binary operations of A and V play an important roll. We begin with the following general definition :

2.A.1 Definition An *operation* of an (arbitrary) set M on an (arbitrary) set X is a map $M \times X \to X$.

An operation $A \times V \to V$ of the ring A on an abelian group $(V,+)$ is written multiplicatively, i. e., in the form $(a,x) \mapsto a \cdot x = ax, a \in A, x \in V$, since the elements a and x are of different origin there is no confusion of this notation with the multiplication in A; similarly, the addition in A and in V both are denoted by $+$. Further, the zero element of A as well as in V is denoted by the same symbol 0. Furthermore, as in ring theory we adopt the *bracket-convention* that the operation of A on V has the stronger binding that the addition in V. For $a,b \in A$ and $x,y \in V$ for example we write $ax+by$ for $(ax)+(by)$.

2.A.2 Definitions An abelian group $(V,+)$ together with a (multiplicatively written) operation of A on V is called an *A-module* if the following conditions holds for all $a,b \in A$ and for all $x,y \in V$:

(1) $1_A \cdot x = x$. (2) $a(bx) = (ab)x$. (3) $a(x+y) = ax+by$. (4) $(a+b)x = ax+bx$.

The operation of A on V is called the *scalar multiplication* of A on V and we say that it defines an *A-module structure* on the abelian group $(V,+)$. In any case without any doubt, to address the A-module structure on V it is common to use simply the term "of A-module V" or even simply "of module V". Instead of A-module one can also write *module over A*. The ring A is called the *scalar ring of V*; the elements of A are called *scalars*. When modules over a fixed ring A are considered, then the ring A is called the *ground ring* or *base ring*.

Modules over a division ring K are called *K-vector spaces*. The elements of a K-vector space are called *vectors*. A vector space over the field $\mathbb{R}$ of real numbers (respectively, the field $\mathbb{C}$ of complex numbers) is called a *real* (respectively, *complex*) *vector space*.

From the special distributive laws (3) and (4) we can deduce the following rules :

2.A.3 Rules of Scalar multiplication *Let V be an A-module. For $a\in A$ and $x\in V$, we have*:

(1) $a\cdot 0=0$ *and* $0\cdot x=0$ *for all* $a\in A$ *and all* $x\in V$.

(2) $(-a)x=a(-x)=-ax$ *for all* $a\in A$ *and all* $x\in V$.

(3) $(-a)(-x)=-((-a)x)=-(-ax)=ax$ *for all* $a\in A$ *and all* $x\in V$.

(4) (General distributive law): *For arbitrary families* $a_i\in A, i\in I$, $x_j\in V, j\in J$, *of elements such that* $a_i=0$ *for al most all* $i\in I$ *(resp.* $x_j=0$ *for al most all* $j\in J$*), we have :*

$$\Bigl(\sum_{i\in I}a_i\Bigr)\Bigl(\sum_{j\in J}x_j\Bigr)=\sum_{i,j)\in I\times J}a_ix_j$$

Proof: (1) Immediate from $a\cdot 0=a(0+0)=a\cdot 0+a\cdot 0$ and $0\cdot x=(0+0)\cdot x=0\cdot x+0\cdot x$. (2) is clear from the equations $0=0\cdot x=(a+(-a))x=ax+(-a)x$ and $0=a\cdot 0=a(x+(-x))=ax+a(-x)$. For the proof of (4) use (1), (2) and induction. □

2.A.4 Homothecies Let V be an A-module. Then for each $a\in A$, the map $\vartheta_a:V\to V$ defined by $x\mapsto ax$ is called the homothecy or stretching by a in V. Therefore we have the map

$$\vartheta:A\to \mathrm{Maps}\,(V,V),\quad a\mapsto \vartheta_a:V\to V\,.$$

The condition (1) of the definition of an A-module structure says that $\vartheta_1=\mathrm{id}_V$ i. e., the neutral element of the multiplicative monoid of A operates as the identity on V. (Some authors drop this postulation in the definition of an A-module and say that an A-module is unitary if it holds. However, we will consider only unitary modules.) The condition (3) of the definition of A-module mean that $\vartheta_a:V\to V$ is an endomorphism of the abelian group $(V,+)$, i. e., $\vartheta_a\in\mathrm{End}\,(V,+)$. Further, by the conditions (4), (2) and (1) it follows that the map

$$\vartheta:A\to \mathrm{End}\,(V,+),\quad a\mapsto \vartheta_a:V\to V$$

is a ring homomorphism, i. e., $\vartheta_{a+b}=\vartheta_a+\vartheta_b$, $\vartheta_{ab}=\vartheta_a\circ\vartheta_b$ and $\vartheta_1=\mathrm{id}_V$.

2.A.5 Right Modules Let A be a ring. An A-module in the sense of above Definition 2.A.2 is precisely a left A-module. If the operation of A on V has the properties (1), (3) and (4) with

(2′) $a(bx)=(ba)x$ for all $ab\in A$ and all $x\in V$,

then V is called a right A-module. In this case it is convenient to write the operation of A on V on the right side. Then (2′) takes the form : $(xb)a=x(ba)$. Left and right modules are interchangeable concepts. If A^{op} denote the opposite ring of A, then the right A-modules (respectively left A-modules) are identical with the left A^{op}-modules (respectively, right A^{op}-modules). Therefore one can restrict to study only one kind of modules. Over a commutative ring the difference between left and right modules is anyway pointless.

2.A.6 Bimodules Sometimes one need to consider many module structures on the same abelian group $(V,+)$. If these module structures are compatible with each other then one use the term multi-module, in particular, bimodule when one considers two compatible module structures.

Suppose that the abelian group $(V,+)$ has a left A-module structure and also a left B-module structure. Then V is called a (A,B)-bimodule if $a(bx)=b(ax)$ for all $a\in A$, $b\in B$, $x\in V$ and in this case we use the notation $V={}_{A,B}V$.

Suppose that the abelian group $(V,+)$ has a left A-module structure and also a right B-module structure (see a) above). Then V is called a (A,B)-bimodule if $a(xb)=(ax)b$ for all $a\in A$, $b\in B$, $x\in V$ and in this case we use the notation $V={}_AV_B$.

Analogously, one can define bimodules of the type $V_{A,B}$. — A trivial example of an bimodule structure is supplied on an ordinary module V over a *commutative* ring A. With a same operation on V it is a (A,A)-bimodule of type ${}_{A,A}V$.

2.A.7 Examples Let A be a ring.

(1) The trivial group 0 is an A-module in an unique way. In fact the only scalar multiplication is $(a,0) \mapsto 0$ for all $a \in A$. This A-module is called the zero module and is also denoted by 0.

(2) Let G be an abelian group. For $x \in G$ and $m \in \mathbb{Z}$, we have $mx := x + \cdots + x$ (m-times). Then the operation $\mathbb{Z} \times G \to G$ defines a $\mathbb{Z}$-module structure on G. Conversely, on every $\mathbb{Z}$-module V the scalar multiplication is given by $(m,x) \mapsto mx := x + \cdots + x$ (m-times) in the abelian group $(V,+)$. Therefore $\mathbb{Z}$-modules are precisely abelain groups.

(3) Let A be a ring. The left multiplication $\lambda_a : A \to A$, $x \mapsto ax$ by elements $a \in A$ defines an A-module structure on A (whereas the right multiplication $\rho_a : A \to A$, $x \mapsto xa$ defines a right A-module structure on A. Then with these operations A is a bimodiule ${}_AA_A$).

(4) Let $R \subseteq A$ be a subring. The restriction of the multiplication $A \times A \to A$ in the ring A to the subring R, i. e., restriction to $R \times A$ (respectively, to $A \times R$) defines a left R-module (respectively, right R-module) structure on A. For example, the chain $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ of fields define a natural $\mathbb{R}$-vector space structure on $\mathbb{C}$ and natural $\mathbb{Q}$-vector space structures on $\mathbb{R}$ and on $\mathbb{C}$. More generally, the restriction of the scalar multiplication $A \times V \to V$ of the A-module V to $R \times V$ defines an R-module structure on V. In future an A-module V will be considered as an k-module with this natural R-module structure, unless otherwise specified.

(5) (Direct products and Direct sums) Let $V_i, i \in I$, be a family of A-modules. On the abelian groups direct product $\prod_{I \in I} V_i$ and the direct sum $\oplus_{i \in I} V_i$ we define the scalar multiplication of an element $a \in A$ on the I-tuple $(x_i)_{i \in I}$ by $a(x_i)_{i \in I} := (ax_i)_{i \in I}$ (componentwise scaler multiplication). These A-modules are called the direct product and the direct sum of the family $V_i, i \in I$. If all V_i are equal to the same A-module V, then the I-fold direct product of V is the set V^I of all maps from I into V. The common notation $V^{(I)}$ is used for the I-fold direct sum of V. If I is a finite set then $V^I = V^{(I)}$. Moreover, if $I = \{1, \ldots, n\}$, then we just denote $V^I = V^{(I)}$ by V^n. Note that $V^{\emptyset} = 0$ is the zero module.

2.B Submodules

Let A be a ring and let V be an A-module. A subset $W \subseteq V$ is called an A-submodule of V (or simply a submodule of V) if W is a subgroup of the abelian group V and if the scalar multiplication $A \times V \to V$ of A on V restricts to a scalar multiplication $A \times W \to W$ on W, i. e., for all $a \in A$ and $x \in W$ we have $ax \in W$.

An A-submodule W of an A-module V is therefore closed under the multiplication of all scalars $a \in A$. The restriction of the A-module structure on V to W defines an A-module structure on W. In this sense every A-submodule itself is an A-module. In case of vector spaces over a division ring K, K-submodules are also called K-subvector spaces or just K-subspaces.

2.B.1 Examples Let A be a ring.

(1) In every A-module V, the zero module 0 and V itself are A-submodules of V; these are called trivial submodules of V.

(2) In an abelian group , the Z-modules are precisely the subgroups.

(3) In any ring A, the A-submodule of the left A-module A (respectively, the right A-module A) are precisely the left-deals (respectively, right-ideals) in A.

(4) Let $V_i, i \in I$ be a family of A-modules. Then the direct sum $\oplus_{i \in I} V_i$ is an A-submodule of the direct product $\prod_{i \in I} V_i$. In particular, the I-fold direct sum $V^{(I)}$ of V is an A-submodule of the I-fold direct product V^I of V. Moreover, if I is infinite then $V^{(I)}$ is a proper submodule of V^I.

2.B.2 Criterion for submodule *Let A be a ring and let V be an A-module. A subset $W \subseteq V$ is an A-submodule of V if and only if the following three conditions are satisfied*: (1) $W \neq \emptyset$. (2) *For all $x \in W$ and all $y \in W$ we have $x + y \in W$.* (3) *For all $a \in A$ and all $x \in W$ we have $ax \in W$.*

Proof: □

We can combine the conditions (2) and (3) in the above criterion in the following condition : for all $a, b \in A$ and for all $x, y \in V$, $ax + by \in W$.

2.B.3 Example (Torsion modules) Let A be a commutative ring and let V be an A-module. An element $x \in V$ is called torsion if there exists a non-zero divisor $a \in A$ with $ax = 0$.The zero element $0 \in V$ is a torsion element, since $1 \cdot 0 = 0$. If $x \in V$ is a torsion element and if $c \in A$ is arbitrary, then cx is also torsion element (since $ax = 0$ for some non-zero divisor in A, we also have $a(cx) = c(ax) = 0$.). Further, if $y \in V$ is another torsion element, i. e., if $by = 0$ for some non-zero divisor in $b \in A$, then ab is a non-zero divisor in A with $ab(x+y) = bax + aby = 0$ and so $x + y$ is also a torsion element. Therefore by the above criterion *the set of all torsion elements in* V $\mathrm{t}(V) = \mathrm{t}_A(V) = \{x \in V \mid x$ *is a torsion element*$\}$ *is an* A*-submodule of* V. This submodule is called the torsion-submodule of V. An A-module V is called torsion-free if $\mathrm{t}(V) = 0$. If every element of V is torsion, i.e., if $\mathrm{t}(V) = V$ then V is called torsion-module.

(a) Direct sum of torsion-modules is again a torsion-module. A submodule of a torsion-module is a torsion-module.

(b) Direct product of torsion-free modules is again a torsion-free module. A submodule of a torsion-free module is a torsion-free module.

(c) The A-module A is always torsion-free. In an abelian group (in any $\mathbb{Z}$-module) torsion-elements are precisely the set of elements of positive order. The $\mathbb{Z}$-module $\mathbb{Q}$ is torsion-free. Every finite abelian group if a $\mathbb{Z}$-torsion module. For $n \in \mathbb{N}^*$, let Z_n denote a cyclic group of order n. Then the direct product $\prod_{n \in \mathbb{N}^*} \mathrm{Z}_n$ of the $\mathbb{Z}$-torsion modules Z_n, $|, n \in \mathbb{N}^*$, is not $\mathbb{Z}$-torsion module.

2.B.4 Intersection of submodules *Let* A *be a ring,* V *be an* A*-module and let* $W_i, i \in I$*, be a family of* A*-submodules of* V*. Then the intersection* $\bigcap_{i \in I} W_i$ *is also an* A*-submodule of* V*.*

Proof: Follows immediately from 2.B.2. □

If x_i, $i \in I$, is a family of element in an A-module V, then by 2.B.4 there exists a smallest (with respect to the inclusion) submodule of V which contain all the elements x_i, $i \in I$, namely, the intersection of the family of all submodules which contain x_i, $i \in I$ and this family is non-empty, since V is one of them.

2.B.5 Definition Let A be a ring and let V be an A-module. For a family x_i, $i \in I$, of elements of V, the smallest A-submodule of V containing x_i, $i \in I$, is precisely the subset $\{\sum_{i \in I} a_i x_i \mid (a_i)_{i \in I} \in A^{(I)}\}$ of V. Therefore this A-submodule is denoted by $\sum_{i \in I} A x_i$ and we say that it is the A-submodule of V generated by the family x_i, $i \in I$. If W is an A-submodule of V and if $W = \sum_{i \in I} A x_i$ for some family x_i, $i \in I$ in V, then we say that x_i, $i \in I$ is a generating system for W. If $X \subseteq V$, then A-submodule of V generated by X is denoted by AX.

For example, the zero A-submodule of V is generated by the $\emptyset \subseteq V$, but it is also generated by $\{0\} \subseteq V$. Every A-module has a generating system, for example the set of all of its elements. An A-submodule with generating system consisting of a single element x is called a cyclic A-submodule generated by x and is denoted by Ax. Every element of Ax is of the form ax with $a \in A$, but a need not be unique, i. e., $ax = bx$ for some $a, b \in A$, but $a \neq b$. — The cyclic $\mathbb{Z}$-modules are precisely the cyclic groups.

2.B.6 Sum of submodules *Let* A *be a ring ,* V *be an* A*-module and let* W_i $i \in I$ *be a family of* A*-submodules of* V*. Then the* A*-submodule* W *of* V *generated by the union* $\bigcup_{i \in I} W_i$ *is precisely*

$$\{\sum_{i \in I} x_i \mid x_i \in W_i \text{ for all } i \in I \text{ and } x_i = 0 \text{ for almost all } i \in I\}$$

Proof: □

The A-submodule of V constructed in 2.B.6 is called the sum of submodules W_i, $i \in I$, and is denoted by $\sum_{i \in I} W_i$. For $I = \{1, \ldots, n\}$ it is also denoted by $W_1 + \cdots + W_n$ or $\sum_{i=1}^n W_i$. It is

$$W_1 + \cdots + W_n = \{x_1 + \cdots + x_n \mid x_i \in W_i, i = 1, \ldots, n\}$$

2.B.7 Definition An element $x \in V$ is called a linear combination of the family $x_i \in V$, $i \in I$ (with coefficients in A), if there is family a_i, $i \in I$, of elements in A, such that almost all a_i are zero, i. e., there exists an element $(a_i)_{i\in I} \in A^{(I)}$ such that $x = \sum_{i\in I} a_i x_i$; in this case the elements a_i, $i \in I$ are called the coefficients of the linear combination. In general these coefficients are not uniquely determined by the element x.

For calculation with linear combinations we note the two rules : two linear combinations can also be added by adding the coefficients and a linear combination can be multiplied by a scalar $a \in A$ by multiplying the coefficients by a, i. e, if $x_i \in V$, $(a_i)_{i\in I}$, $(b_i)_{i\in I} \in A^{(I)}$ and $a \in A$, then :

$$\sum_{i\in I} a_i x_i + \sum_{i\in I} b_i x_i = \sum_{i\in I} (a_i + b_i) x_i \qquad \text{and} \qquad a \sum_{i\in I} a_i x_i = \sum_{i\in I} (a a_i) x_i .$$

With this definition : *The A-submodule generated by the system x_i, $i \in I$ is precisely the set of all linear combinations of the family x_i, $i \in I$.*

2.B.8 Definition An A-module V is called finitely generated or a finite A-module if there is generating system for V consisting finitely many elements.

2.B.9 Remark Note that a finite module V need not mean that V has only finitely many elements. For example, the Z-module $\mathbb{Z}$ has infinitely many elements but it is a finite $\mathbb{Z}$-module, in fact a cyclic $\mathbb{Z}$-module (generated by the element 1). Note also the contrast: in group theory finite group mean group with finitely many elements. The abelian group $\mathbb{Z}$ is not a finite group but it is a finite $\mathbb{Z}$-module.

2.B.10 Proposition *Let A be a ring and let V be an A-module. If V is a finitely generated A-module, then every generating system of V contains a finite generating system.*

Proof: Let $y_1, \ldots, y_n \in V$ be a given finite generating system for V, i. e., $V = Ay_1 + \cdots + Ay_n$ and let x_i, $i \in I$ be a generating system for V. Then for each $j = 1, \ldots, n$, $y_j = \sum_{i\in E(j)} a_{ij} x_i$ with $a_{ij} \in A$ and finite subsets $E(j) \subseteq I$. Then $E := \cup_{j=1}^n E(j)$ is a finite subset of I and the submodule generated by x_i, $i \in E$ contain all the elements $y_1, \ldots, y_n$ and hence $V = Ay_1 + \cdots + Ay_n \subseteq \sum_{i\in E} Ax_i \subseteq V$. Therefore $V = \sum_{i\in E} Ax_i$, i. e., V is generated by the finite subfamily x_i, $i \in E$. □

2.B.11 Definition Let A be a ring and let V be an A-module. A generating system X of an A–module V is called minimal generating system for V if it is minimal (with respect to the natural inclusion) in the set $\{Y \mid Y \subseteq \text{ is a generating system for } V\}$. — If V is finite A-module, then

$$\mu_A(V) := \min\{|X| \mid X \subseteq V \text{ is a generating system for } V\}$$

is called the minimal number of generators for V.

By Proposition 2.B.10 every minimal generating system of a finite A-module is finite. More generally, a generating system x_i, $i \in I$ of an A-module V is called minimal if there is no proper subset $J \neq I$ of I such that x_j, $j \in J$, generate V.

For a minimal system of generators x_i, $i \in I$ of V, the index map $I \to V$, $i \mapsto x_i$, is injective. Therefore this definition is not essentially more general than the previous one. A minimal generating system never contains the zero element. If V is finitely generated, then by Proposition 2.B.10 every generating system contains a finite generating system and hence also contain a minimal generating system.

An arbitrary module need not have a minimal generating system. For example, the $\mathbb{Z}$-module $\mathbb{Q}$ does not have minimal generating system, see Exercise 2.2.

2.B.12 Example A minimal generating system of a finite A-module V has at least $\mu_A(V)$ elements and need not have the cardinality $\mu_A(V)$. For example, $\{1\}, \{2,3\}, \{p,q \mid \gcd(p,q) = 1\}$ are minimal generating systems for the $\mathbb{Z}$-module $\mathbb{Z}$ and $\mu_{\mathbb{Z}}(\mathbb{Z}) = 1$. Moreover, for every natural number $m \in \mathbb{N}^*$, there is a minimal generating system for the $\mathbb{Z}$-module $\mathbb{Z}$ with cardinality m, namely, $x_1, \ldots, x_m$, where $x_i := \prod_{j=1, j\neq i}^m p_j$ and $p_1, \ldots, p_m$ are distinct prime numbers.

2.B.13 Theorem *Let A be a ring, V be an A-module and let $Y \subseteq V$ be an infinite generating system for V. Then every generating system x_i, $i \in I$, of V contains a generating system x_j, $j \in J$, $J \subseteq I$ with $|J| \leq |Y|$.*

Proof: For every $y \in Y$, there exists a finite subset $E(y)$ of I such that $y \in \sum_{i \in E(y)} Ax_i$. Then x_j, $j \in J := \cup_{y \in Y} E(y)$ is a generating system for V, since $V = \sum_{y \in Y} Ay \subseteq \sum_{j \in J} Ax_j \subseteq V$. Note that since Y is infinite, for $I = Y$ and $E_y = E(y)$, $y \in Y$, the assumptions in Corollary 2 below are satisfied and hence $|J| = |\cup_{y \in Y} E(y)| \leq |Y|$ by Corollary 2[1]. □

2.B.14 Corollary *Let A be a ring and let V be an A-module If V has countable generating system, then every generating system of V contains a countable generating system.*

Proof: If V is a finite A-module, then the assertion follows directly from Proposition 2.B.10 and if V is not finite, then it follows from Theorem 2.B.13. Moreover, the cardinality argument in the proof of 2.B.13 in this special case in simple: A countable union of countable sets is again countable. □

2.B.15 Let A be a ring, $\mathfrak{a}$ be a left-ideal in A and let V be an A-module. The set of linear combinations of elements of V with coefficients from the ideal $\mathfrak{a}$ form a submodule of V. This submodule is generated by ax, $a \in \mathfrak{a}, x \in V$ and is denoted by $\mathfrak{a}V$.

The following rules are easy to verify : For left-ideals $\mathfrak{a}, \mathfrak{b}$ in A and A-submodules W, U of V we have : (a) $(\mathfrak{a} + \mathfrak{b})V = \mathfrak{a}V + \mathfrak{b}V$. (b) $\mathfrak{a}(\mathfrak{b}V) = (\mathfrak{a}\mathfrak{b})V$. (c) $\mathfrak{a}(W + U) = \mathfrak{a}W + \mathfrak{a}U$.

2.B.16 Example For a left ideal $\mathfrak{a}$ is a ring A and a natural number $n \in \mathbb{N}$ recursively define the powers of $\mathfrak{a}$ by : $\mathfrak{a}^0 := \mathbb{A}, \mathfrak{a}^{n+1} := \mathfrak{a}\mathfrak{a}^n$. Then we have a descending chain of left ideals in A:

$$A = \mathfrak{a}^0 \supseteq \mathfrak{a} \supseteq \mathfrak{a}^2 \supseteq \cdots \supseteq \mathfrak{a}^n \supseteq \mathfrak{a}^{n+1} \supseteq \cdots .$$

— The elements of the power $\mathfrak{a}^n$ of a left-ideal $\mathfrak{a}$ are precisely the finite sums of products $a_1 \cdots a_n$ with $a_i \in \mathfrak{a}$, $i = 1, \ldots, n$. Further, $\mathfrak{a}^m \mathfrak{a}^n = \mathfrak{a}^{m+n}$ for all $m, n \in \mathbb{N}$.

A left-, right-, or two-sided ideal $\mathfrak{a}$ is called n i l p o t e n t if there exists $m \in \mathbb{N}$ such that $\mathfrak{a}^m = 0$. Clearly, if $\mathfrak{a}^m = 0$, then $a_1 \cdots a_m = 0$ for all $a_1, \ldots, a_m \in \mathfrak{a}$. Moreover, we have the following very useful special case of Nakayama's lemma :

2.B.17 Lemma *Let A be a ring and let $\mathfrak{a}$ be a nilpotent left-ideal in A. Let V be an A-module and let $W \subseteq V$ be an A-submodule of V. If $W + \mathfrak{a}V = V$, then $W = V$.*

Proof: It is enough to prove that $W = W + \mathfrak{a}^n V$ for every $n \in \mathbb{N}$. We show this by induction on n. For $n = 0$ the assertion is trivial. By induction hypothesis we have the equalities : $V = W + \mathfrak{a}^n V = W + \mathfrak{a}^n(W + \mathfrak{a}V) = W + \mathfrak{a}^n W + \mathfrak{a}^n(\mathfrak{a}V) = W + \mathfrak{a}^{n+1} V$. □

---

[1] The Corollary 2 is an an easy consequence of the following theorem from set theory :

Theorem *For any infinite set Y, we have $|Y \times Y| = |Y|$.* (For the proof of this one need to use Zorn's Lemma.) From this we deduce :

Corollary 1 *For any two non-empty sets I, Y with one of them infinite, we have $|I \times Y| = \sup\{|I|, |Y|\}$.* (We may assume that $|I| \leq |Y|$. Then Y is infinite and $|Y| \leq |I \times Y| \leq |Y \times Y| = |Y|$ by the above theorem and hence $|I \times Y| = |Y|$ by Schröder-Berstein theorem.)

Corollary 2 *Let Y be an infinite set and let E_i, $i \in I$, be a family of sets with $|I| \leq |Y|$ and $|E_i| \leq |Y|$ for all $i \in I$. Then $|\cup_{i \in I} E_i| \leq |Y|$.* (We may assume that $E_i \neq \emptyset$ for all $i \in I$. Since $|E_i| \leq |Y|$, there is a surjective map $g_i : Y \to E_i$ for each $i \in I$. Then the map $I \times Y \to \cup_{i \in I} E_i$ with $(i, y) \mapsto g_i(y)$ is also surjective and hence $|\cup_{i \in I} E_i| \leq |I \times Y| = \sup\{|I|, |Y|\} = |Y|$ by Corollary 1.)

2.B.18 Maximal ideals Let A be a ring. The set of left-ideals in A is ordered by the natural inclusion $\subseteq$. Its biggest element if the unit ideal A. A maximal element in the set of left-ideal different from A is called a maximal left-ideal. Analogously one can define maximal right-ideals. In commutative ring one simply calls them maximal ideals. Therefore : *A ring is a division ring if and only if its zero ideal is a maximal left-ideal.*

2.B.19 Example In the ring $\mathbb{Z}$ every ideal is of the form $\mathbb{Z}a$ with a uniquely determined natural number $a \in \mathbb{N}$. For $ab \in \mathbb{N}$ the inclusion $\mathbb{Z}a \subseteq \mathbb{Z}b$ is equivalent with $a \in \mathbb{Z}b$ or with an existence of $c \in \mathbb{N}$ such that $a = cb$ and so with the divisibility condition "b divides a". Therefore $\mathbb{Z}a$ is maximal ideal in $\mathbb{Z}$ if and only if $a \neq 1$ and a has no divisors other than 1 and a. But this condition exactly characterize the prime numbers. Therefore it shows that : *$\mathbb{Z}a$ for $a \in \mathbb{N}$ is a maximal ideal in the ring $\mathbb{Z}$ if and only if a is a prime number.* If $a \in \mathbb{N}, a \neq 1$, then a has a prime divisor.

In the zero ring there are no maximal ideals. On the contrary if $A \neq 0$, then it has enough maximal left- and right-ideals by Krull's theorem. Below we will prove more general result than this.

2.B.20 Maximal submodules Let V be an A-module. Then maximal elements (with respect to the natural inclusion) in the set $\mathscr{S}_A(V)$ of all A–submodules of V are called maximal A-submodules of V. Maximal A- submodules of the A-module A are precisely are maximal ideals in A. Let W be a maximal A-submodule of V and let $x \in V, x \notin W$. Then $W \neq W + Ax$ and by the maximality of W, we have the equality $W + Ax = V$. Therefore W is a cofinite A-submodule in the sense of the following definition.

2.B.21 Definition An A- submodule W of V is called cofinite if there exists finitely many elements $x_1, \ldots, x_n \in V$ such that $V = W + Ax_1 + \cdots + Ax_n$. Equivalently, the quotient A-module V/W is finitely generated.

If W is a cofinite A-submodule of V, then every A-submodule W' with $W \subseteq W' \subseteq V$ is also cofinite. Every A-submodule of a finite A-module is cofinite.

Below we prove the converse of the above remark that *in any A-module V cofinite A-submodules different from V exists if V has maximal submodules.*

2.B.22 Theorem *Let W be a cofinite A-submodule of an A-module V with $W \neq V$. Then there exists a maximal A-submodule of V which contain W. In particular, in a finite non-zero A-module V there are maximal A-submodules.*

Proof: Let $V = W + Ax_1 + \cdots + Ax_n$. Let r be the number such that $W_r := W + Ax_1 + \cdots + Ax_{r-1} \neq V$, but $W_r + Ax_r = V$. Then it is enough to prove the theorem for W_r instead of W. We may therefore assume that $W \neq V$ and $W + Ax = V$ for some $x \in V$. Let $\mathfrak{M} := \{W' \mid W' \text{ is a submodule of } V \text{ with } W \subseteq W' \subsetneq V\}$. Then $W \in \mathfrak{M}$ and $\mathfrak{m}$ is a non-empty set ordered by the natural inclusion. We note that $\mathfrak{M}$ is inductively ordered. For, if $\mathfrak{C} \subseteq \mathfrak{M}$ is a non-empty chain in $\mathfrak{M}$, then $U' := \cup_{U \in \mathfrak{C}} U$ is an upper bound of $\mathfrak{C}$ in $\mathfrak{M}$: Clearly U' is a submodule of V, $W \subseteq U'$, since $\mathfrak{C} \neq \emptyset$. Further, since $x \neq U$ for all $U \in \mathfrak{C}$, we have $x \neq U'$ and so $U' \neq V$. Now by Zorn's Lemma there exists a maximal element in $\mathfrak{M}$ and this is a maximal submodule of V which contain W. □

2.B.23 Corollary *In a finite module $|, V \neq 0$, there are maximal submodules.*

By specializing the above corollary to the finite module $V = A = A \cdot 1$, we note the following:

2.B.24 Corollary (Krull's Theorem) *Let A be a ring and let $\mathfrak{a}$ be an ideal in A with $\mathfrak{a} \neq A$. Then there exists a maximal ideal $\mathfrak{m}$ in A with $\mathfrak{a} \subseteq \mathfrak{m} \subsetneq A$. In particular, in every non-zero ring, there are maximal left-ideals.*