MODULE THEORY

ANAMITRO BISWAS

Before we begin

I am a big fan of category theoretic notation, and hence abhor a mosaic of concrete examples in the text beyond the point of clarification of the abstract ideas presented thereof. So, I have tried to make the first part of the text clean of specific known cases, except for the purpose of citing them as counterexamples. And if the reader is familiar with one or two basic examples to begin with, this, I think, will rather help him/her imagine around the abstract pillar of clouds rather than restrciting them to the dimensions of an iron pillar.

Amples examples are provided later: those that in themselves prove to be interesting enough to be worth studying.

Same goes with rigour. Ramakrishna Paramahamsa, a spiritual mystic of Bengal, was of the opinion that the *thorn of knowledge* should act as a tool to surgically remove the *thorn of ignorance*; and then both should be discarded altogether, just in the same way we do not carry along surgical instruments after we are cured. Same goes for mathematical *rigour*. It is acceptable only to the extent it does not undermine the learner's imagination, only to the purpose it helps to present a clearer idea or convince something otherwise unbelievable. So, I have kept it concise and free of such irritating rigour. However, if need be, that can be step-by-step worked out pretty much without any external help by a reader who is informed with standard undergraduate abstract algebra, and just follows the text clearly.

1. Group action

Let A be any set and G a group written here in a multiplicative way. We define a *group action* as a function $G \times A \to A;\ (g, a) \mapsto g.a \in A$ such that

(i) $g_1.\left(g_2.a\right) = \left(g_1 g_2\right).a$ for all $g_1, g_2 \in G$ and all $a \in A$;
(ii) $1_G.a = a$ for all $a \in A$.

We informally say that the group G "acts on" the set A; $G \curvearrowright A$.

For some $g \in G$, define $\sigma_g : A \to A$; $\sigma_g(A) = g.a$. Then, $\sigma_g \in S_A$, i.e., σ_g is essentially a permutation of A. This is because, we can similarly have a $\sigma_{g^{-1}}$ that acts as both left and right inverse of σ_g, making σ_g a bijective map. Indeed, $\left(\sigma_{g^{-1}} \circ \sigma_g\right)(a) = g^{-1}.(g.a) = \left(g^{-1}g\right).a = a$. Also, $\varphi : G \to S_A;\ g \mapsto \sigma_g$ is a homomorphism, i.e., $\varphi\left(g_1 g_2\right)(a) = \sigma_{g_1 g_2}(a) = \left(g_1 g_2\right).a = g_1.\left(g_2.a\right) = \sigma_{g_1}\left(\sigma_{g_2}(a)\right) = \varphi\left(g_1\right) \circ \varphi\left(g_2\right)(a)$.

2. Ring Module

A *module* M over a ring R is an action of R on M in the multiplicative way, subject to the following conditions:

(i) $(r+s)m = rm + sm$;
(ii) $(rs)m = r(sm)$;
(iii) $r(m+n) = rm + rn$;
(iv) if $1 \in R$, $1m = m$ (in this case, the module is said to be *unital*)

for all $r, s \in R$ and all $m, n \in M$. It follows that $(-r)m = -rm$ and $0m = 0$. A *submodule* is a subset that is a module in itself, and it's trivial that an equivalent condition is that $\phi \neq N \subseteq M$ is a submodule if and only if $x, y \in N \Rightarrow x + \alpha y \in N$ for all $\alpha \in R$.

2.1. Module homomorphism.

A *module homomorphism* $\varphi : M \to N$ where M and N are modules over a ring R is a mapping that keeps the module structure of $\varphi(M)$ intact, i.e.,

(i) $\varphi\left(m_1 + m_2\right) = \varphi\left(m_1\right) + \varphi\left(m_2\right)$ for all $m_1, m_2 \in M$;
(ii) $\varphi(rm) = r\varphi(m)$ where $r \in R$ and $m \in M, \varphi(m) \in N$.

This can alternatively stated that $\varphi\left(m_1 + rm_2\right) = \varphi\left(m_1\right) + r\varphi\left(m_2\right)$ for all $m_1, m_2 \in M$ and all $r \in R$. The *kernel* $\ker\varphi = \{m \in M \mid \varphi(m) = 0 \in N\}$ and *image* $\varphi(M) = \{n \in N \mid \exists\, m \in M \ni n = \varphi(m)\}$ are submodules of M and N respectively. An *isomorphism* $\varphi : M \cong N$ is a homomorphism which is bijective. The set of homomorphisms from a module M to a module N is denoted by $\mathrm{Hom}_R(M, N)$. For $\varphi, \psi \in \mathrm{Hom}_R(M, N)$, we define $(\varphi + \psi)(m) = \varphi(m) + \psi(m)$ for all $m \in M$. $\mathrm{Hom}_R(M, N)$ is an abelian group with this addition. Further, if the acting ring R is commutative, we can establish $\mathrm{Hom}_R(M, N)$ as an R-module. If we let $(r\varphi)(m) = r(\varphi(m))$ for $r \in R, m \in M$, we have, for $s \in R$, $(r\varphi)(\beta m) = r(\varphi(\beta m)) = r(\beta\varphi(m)) = \beta(r\varphi)(m)$ since M is an R-module and φ is a module homomorphism. Now, if $\varphi_1 \in \mathrm{Hom}_R(L, M)$ and $\varphi_2 \in \mathrm{Hom}_R(M, N)$, we have the $\varphi_2 \circ \varphi_1 \in \mathrm{Hom}_R(L, N)$. With all these, in a special case, $\mathrm{Hom}_R(M, M)$ is a ring with multiplicative identity $I : m \mapsto m\ \forall\, m \in M$. This ring is called the *ring of endomorphisms* of M over R, denoted by $\mathrm{End}_R(M)$.

We have the natural map $f : R \to \mathrm{End}_R(M);\ r \mapsto rI$, which is not always an injective map. There might be zero divisors in the ring. But no unit belongs to $\ker f$ for sure. Otherwise, take for example, $M = \mathbb{Z}/7\mathbb{Z}, R = \mathbb{Z}$. Then $7m = 0$ for all $m \in M$. But if R is a field, this map is injective and we call $\mathrm{Im}\, f$ (the isomorphic copy of R) as the subring of scalar transformations in $\mathrm{End}_R(M)$.

Now, a module is an abelian group with some extra condition imposed with respect to a ring R. $\mathbb{Z}$ being the most primitive model of a ring (except the fact that it is an integral domain; well, the most primitive example of an integral domain), $\mathbb{Z}$-modules are just those abelian groups with no other extra condition. Thus module homomorphisms are necessarily group homomorphisms but the reverse need not be true. Also, if the underlying ring is $\mathbb{Z}$, the module homomorphisms are just the homomorphisms between abelian groups.

2.2. $M = R$. When the module is same as the ring, there is no reason to believe that the module homomorphism will be the same as the ring homomorhism.

- If $R = M = \mathbb{Z}$, $x \mapsto 2x$ is a module homomorphism, but does not take 1 to 1, and hence is not a ring homomorphism.
- If $R = M = F[x]$ for some field F, for the ring homomorphim $f : F[x] \to F[x];\ x \mapsto x^2$, $x^2 = f(x) = f(x.1) = xf(1) = x \ \rightarrow\leftarrow$ which shows that it is not a module homomorphism.

2.3. **Quotient module.** Let N be a submodule of M. As abelian groups N is a normal subgroup, and we try to impose a module structure, naturally, on the quotient group M/N by defining for $r \in R$, $r(m + N) := rm + N$. This is well-defined since if $m_1 + N = m_2 + N$, then $m_1 - m_2 \in N \Rightarrow r\left(m_1 - m_2\right) \in N \Rightarrow r\left(m_1 + N\right) = r\left(m_2 + N\right)$. In fact $\pi : M \to M/N$ is a module homomorphism, since it is a homomorphism of abelian groups anyway, and $r\pi(m) = r(m + N) = rm + N = \pi(rm)$. Futher, the kernel of the module homomorphism is the same as the kernel of the group homomorphism over the same sets with the same group operation, so $\ker\pi = N$.

Theorem 1 (First Isomorphism Theorem)**.** *If $\varphi : M \to N$ is a module homomorphism, the $M/\ker\varphi \cong Im\ \varphi$.*

Theorem 2 (Second Isomorphism Theorem)**.** *Define $A + B := \{a + b \mid a \in A, b \in B\}$ for modules A and B. This is the smallest module, containing both A and B as submodules. Also, $A \cap B$ is a submodule of both A and B. Then, $(A + B)/A \cong A/(A \cap B)$.*

Theorem 3 (Third Isomorphism Theorem)**.** *If A and B are submodules of M such that $B \subseteq A$, then $(M/A)/(B/A) \cong M/B$.*

These results follow from the corresponding theorems for abelian groups, with additional checking for the action by ring elements.

2.4. **Annihilator.**

2.4.1. *Annihilator of module.* If we have an ideal I of R such that $rm = 0$ for all $r \in I$ and $m \in M$, then I is called an *annihilator* of M. In that case we can visualize M as a ring module over the quotient ring R/I where $(r + I).m := rm$ where $r \in R,\ m \in M$. In particular, if I is maximal, then R/I is a field and hence M shall be a vector space.

If M and N are modules over ring R that is annihilated by ideal I, then any R-module homomorphism $M \to N$ is also an R/I-module homomorphism.

Take for example a $\mathbb{Z}$-module G. This means that for some element x in the module, $nx \in G$. Thus G consists of distinct cycles of finite or infinite length and so is an abelian group. On the other hand, any abelian group is a $\mathbb{Z}$-module. The action of a ring element from $\mathbb{Z}$ is absorbed into addition of elements within the module, because $rm = \underbrace{m, \ldots, m}_{r}$ for $r \in \mathbb{Z}, m \in G$. Now, if there exists some $m \in \mathbb{N}$ such that $mx = 0$ for all $x \in G$, then $m\mathbb{Z}$ is an annihilator of G. Even otherwise, simply G is a $\mathbb{Z}/m\mathbb{Z}$-module. In particular for $m = p \in \mathbb{P}$ a prime, $\mathbb{Z}/m\mathbb{Z}$ has the structure of $\mathbb{F}_p$ and so G is a vector space over $\mathbb{F}_p$. If A is such an additive group, then an $\mathbb{Z}$-module homomorphism

$A \to A$ is also a $\mathbb{Z}/p\mathbb{Z}$-module homomorphim, i.e., a linear transformation with underlying fielf $\mathbb{F}_p$. In particular, the group of all invertible linear transformations $A \to A$ is the *general linear group* $\mathrm{GL}(A)$.

2.4.2. *Annihilator of ideal.* We shall denote by $\mathrm{Ann}_M(I)$ the annihilator of right ideal I of R in module M as $\mathrm{Ann}_M(I) := \{m \in M \mid am = 0 \,\forall\;\, a \in I\}$. One can see that $\mathrm{Ann}_M(I)$ is a submodule of M, because if $m_1, m_2 \in \mathrm{Ann}_M(I)$, then $m_1 + \alpha m_2 \in \mathrm{Ann}_M(I)$ for all $\alpha \in R$. This submodule may be proper, as in $R = \mathbb{Z}, M = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, I = 4\mathbb{Z}$.

2.4.3. *Annihilator of submodule.* On the other hand, for a submodule N of M, the *annihilator* of N in R consists of those $r \in R$ for which $rn = 0$ for all $n \in N$, denoted by $\mathrm{Ann}_R(N)$. One can see that this is a two-sided ideal of R as it absorbs any other element r_1 of R this way: $r_1 rn = r_1 0 = 0$, or $rr_1 n = rn_1$ for some $n_1 \in N$ and $rn_1 = 0$ for $r \in \mathrm{Ann}_R(N)$. The annihilator of a submodule of M is contained in M, and might be a proper subset as well, e.g., $R = \mathbb{Z}, M = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, N = \mathbb{Z}/2\mathbb{Z} \times \{0\}$.

2.5. **Field.** If the ring is actually a field (i.e., commutative and without any zero divisors), then the module is essentially a vector space over the field. For commutaive rings a right module is also a left module. Now, if V is a vector space over a field F, then V is also a module over the polynomial ring $F[x]$. We can assign a linear operator (field-module homomorphism) $T : V \to V$ and with respect to that define for $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$,

$$p(x).v = a_n T^n v + a_{n-1} T^{n-1} v + \ldots a_1 T v + a_0 v$$

which is consistent with its restriction on F, where $v \mapsto a_0 v$. Note that this extended action depends upon the linear operator T chosen. If T is identically 0, we have the same module structure with no more information about the elements other than those of F. On the other hand, if T is the shift operator, $(v_1, \ldots, v_r) \mapsto (v_2, v_3, \ldots, v_r, 0)$, we get a different $F[x]$-module structure of V.

Thus, essentially we arrive at a bijection

$$\left\{ \begin{array}{r} \text{a module structure of} \\ V \text{ over } F[x] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{r} \text{a vector space } V \text{ over } F \\ \text{and a linear operator } T : V \to V \end{array} \right\}$$

Now we call a subspace W of V, *T-invariant* or *T-stable* for a linear operator $T : V \to V$ if $T(W) \subseteq W$. Thus, for W to be a submodule of V with respect to $F[x]$ we need, necessarily and sufficiently, W to be *T-stable* in V, because for W to be T-stable means W to be T^k-stable for $k \in \mathbb{N}$ and closed with respect to sums as a module (abelian group). An example might be the shift operator mentioned earlier, where $T^k e_i = \begin{cases} e^{i-k} \text{ if } k < i; \\ 0 \text{ else.} \end{cases}$ for $e_i = \underbrace{(0, 0, \ldots, 0, 1, 0, \ldots, 0)}_{r}$ with 1 in the i^{th} position. Thus if $W = \{(v_1, \ldots, v_t, 0, \ldots 0)\}$ be a t-dimensional subspace of V, then $T^k\,(v_1, \ldots, v_\ell, 0, \ldots, 0) \in W$ for all $\ell \leq t$ and so W is T-stable, i.e., submodule.

2.6. **Module homomorphism over $\mathbb{Z}$.** Let A be a $\mathbb{Z}$-module, $a \in A$ and $n \in \mathbb{N}$. Now, the module homomorphism $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$; $\overline{k} \mapsto ka$ is well-defined if and only if $na = 0$, otherwise $\overline{k} \mapsto k$ is not a function.

Also, the number of such homormorphisms is bijectively determined by the number of possible mappings of $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ to A and these can only be those elements of A such that $na = 0$. The set of such elements, A_n, is in other words the annihilator of the ideal $n\mathbb{Z}$ in $\mathbb{Z}$. Thus, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$. To show that this is an abelian group homomorphism, for $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$, $\varphi\left(\overline{k_1} + \overline{k_2}\right) = \left(k_1 + k_2\right) a = k_1 a + k_2 a = \varphi\left(\overline{k_1}\right) + \varphi\left(\overline{k_2}\right)$.

3. Direct product

Let $M_1, M_2, \ldots M_k$ be R-modules. Their *direct product* $M_1 \times \cdots \times M_k$ is defined as the collection of $(m_1, \ldots, m_k)$ where $m_i \in M_i$, and addition and multiplication by element from R is componentwise. If $N_1, \ldots, N_k$ are submodules of a module M, then the following are equivalent:

(1) We have an isomorphism $\pi : N_1 \times \cdots \times N_k \cong N_1 + \cdots + N_k$; $(n_1, \ldots, n_k) \mapsto n_1 + \cdots + n_k$;

(2) For any $j \in \{1, \ldots, k\}$, $N_j \cap \left(\sum_{i \in \{1, \ldots, k\} \setminus \{j\}} N_i \right) = \{0\}$;

(3) Every $n \in N_1 + \cdots + N_k$ can be written uniquely as a sum $n_1 + \cdots + n_k$ where $n_i \in N_i$ $(i = 1, \ldots, k)$.

Proof. **(1) ⇒ (2).** Let there exist $n \in N_j \cap \left(\sum_{i\in\{1,\dots,k\}\setminus\{j\}} N_i\right)$. Then $n = n_j = \sum_{i\in\{1,\dots,k\}\setminus\{j\}} n_i$ where $n_i \in N_i$ $(i = 1,\dots,j-1,j+1,\dots,k)$, $n_j \in N_j$. Then $\sum_{i=1}^{j-1} n_i - n_j + \sum_{i=j+1}^{k} n_i = 0$, i.e., $(0,\dots,0) \neq \left(n_1,\dots,n_{j-1},-n_j,n_{j+1},\dots,n_k\right) \in \ker\pi \rightarrow\leftarrow$.

(2) ⇒ (3). Let it can be written in two different ways: $n = n_1 + \cdots + n_k = n'_1 + \cdots + n'_k$. By induction we see, $n_j - n'_j = \sum_{i=1}^{j-1} \left(n_i - n'_i\right) \in N_j \cap \sum_{i=1}^{j-1} N_i$ Thus, $n_i = n'_i$ for $i = 1,\dots j-1$ and $n_j = n'_j$. For $j - 1 = 1$ it holds anyway.

(3) ⇒ (1)

□

If $N_1,\dots,N_k$ are submodules of M such that $M = \sum_{i=1}^{k} N_i$ and we have an isomorphism $\pi : N_1 \times \cdots \times N_k \cong N_1 + \cdots + N_k;\ \left(n_1,\dots,n_k\right) \mapsto n_1 + \cdots + n_k$, then $M = N_1 \oplus \cdots \oplus N_k$ is called the internal direct sum of $N_1,\dots N_k$. While the direct product is the external direct sum, we see that in the finite case with the above condition (2), both are the same thing.

4. Free module

4.1. **Generator.** If A is a subset of a module M, then $RA = \left\{\sum_{i=1}^{m} r_1 a_i \mid r_i \in R, a_i \in A, m \in \mathbb{Z}^+\right\}$ is the submodule *generated by* A and the least submodule of M containing A. If $|A| < \infty$ we say that RA is finitely generated, and Ra is a cyclic submodule. If N is a submodule, it can have multiple generating sets, but if it is finitely gerenated there should be a minimum $d \in \mathbb{Z}^+$ such that N has a generating set consisting of d elements, and each such set is called the *minimal set of generators for* N. If $N_1, N_2, \dots, N_k$ be submodules of M, then the module $N_1 + \cdots + N_k := \left\{a_1 + \dots a_n \mid a_i \in N_i\right\}$, which is the smallest module containing all the N_i's. This is actually the submodule generated by $N_1 \cup \cdots \cup N_k$. If A_i is the set of generators of N_i for $i \in \{1,\dots,k\}$, then $A_1 \cup \cdots \cup A_k$ is the minimal set of generators for $N_1 + \cdots + N_k$.

4.2. **Free module.** An R-module F is called*free* on a subset A of F if every element $m \in M$ can be written *uniquely* as $\sum_{i=1}^{n} r_i a_i$ where $r_i \in R, a_i \in A$ and $n \in \mathbb{N}$. Note the difference with direct sum, and that this condition is stricter, i.e., $\bigoplus_{i=1}^{n} N_i$ is not necesarily free over $\bigcup_{i=1}^{n} N_i$. Take for example, $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ which is not free over $2\mathbb{Z}$ since though we can find unique $a_i \in 2\mathbb{Z}$, $(2k+1)a_i$ are equal for all $k \in \mathbb{Z}$ which does not give us unique acting elements from the ring.

4.3. **Universal property.** Given any set A and a mapping φ from A to some R-module M, there is the free module $F(A)$ over A and a unique module homomorphism Φ from $F(A)$ to R such that the following diagram is commutative:

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\Phi"] \\
& M
\end{tikzcd}$$

Define $F(A)$ to be the set of those functions on A to R that takes non-zero values only for a finite number of elements of A. Identify the element $a \in A$ with $f_a \in F(A)$ which takes a to $1 \in R$ and other elements of A to 0. Thus each element of $F(A)$ looks like $\left[\text{with the “basis” } \left\{f_a \mid a \in A\right\}\right] \sum_{i=1}^{n} r_i f_{a_i} \longleftrightarrow \sum_{i=1}^{n} r_i a_i$. This shows F(A) to be a free module on A, for which, of course we have to define addition $\left(f_{a_1} + f_{a_2}\right)(x) = f_{a_1}(x) + f_{a_2}(x)$ for $a_1, a_2 \in A$, $x \in F(A)$ and $\left(r f_a\right)(x) = r\left(f_a(x)\right)$ for $a \in A, r \in R$. Now we come to the function Φ assigning to each element of $F(A)$,

$$\sum_{i=1}^{n} r_i f_{a_i} \mapsto \sum_{i=1}^{n} r_i \varphi\left(a_i\right).$$

It is easy to see that $\Phi|_A = \varphi$ and that Φ is a module homomorphism. Since the values on $F(A)$ are uniquely determined by the values on A, Φ is the unique extension of ϕ.

This means that if $|A| < \infty$ and $A = \left\{a_1, \dots, a_n\right\}$ then $F(A) = \sum_{i=1}^{n} Ra_i \cong R^n$. Additionally, any two free modules over a set are isomorphic to each other as modules, and for any set A, $F\left(F(A)\right) = F(A)$. When $R = \mathbb{Z}$, free module on any set A is called the *free abelian group on A*. If $|A| = n$, it's the free abelian group of *rank n*, isomorphic to $\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n}$. The free module structure enables us to define something for the basis elements, and *extend by linearity* for the rest.

5. Irreducibility

An R-module M is called *irreducible* if its only submodules are 0 and M, which should be distinct.

Let there be some nozero element $m \in M$ which does not generate the whole of M. Then Rm is a submodule of M distinct from both 0 and M, which would contradict the fact that M is irreducible. Thus each element of a nonzero irreducible module acts as its generator, and hence M is cyclic. It is easy to see that a nonzero cyclic module whose each element is a generator, is irreducible. Thus the condition is 'if and only if'.

Therefore, all irreducible $\mathbb{Z}$-modules are cyclic groups of prime order, $\mathbb{Z}/p\mathbb{Z},\ p \in \mathbb{P}$.

For commutative R, the R-module M s irreducible if and only if $M \cong R/I$ (as R-modules). Of course, if M is irreducible, there is this natural map $\varphi : R \to M,\ r \mapsto rm$ where $m \neq 0$ is a fixed element of M. Consider the subset I of R such that $\rho m = 0$ for all $\rho \in I$. For $\rho_1, \rho_2 \in I$, $\left(\rho_1 - \rho_2\right) m = \rho_1 m - \rho_2 m = 0$ and for $r \in R$, $\left(r\rho_1\right) m = r\left(\rho_1 m\right) = r0 = 0$, which means that I is a subring of R which also absorbs multiplication by other elements of R. Thus $I = \ker \varphi$ is an ideal of R. So, $\varphi' : R/I \to M,\ (r + I) \mapsto (r + I)\, m \coloneqq rm$ is an isomorphism. This being an isomorphism also proves conversely that M is a nonzero cyclic module generated by each of its elements, i.e., is irreducible. It remains to show that I is maximal; but that is true since I is an annihilator of the whole of M any ideal $\neq M$ containing I should be an annihilator of a submodule of M, but the only submodules of M are 0 and M.

If M_1 and M_2 are irreducible R-modules and $\varphi : M_1 \to M_2$ is a homomorphism, then $\ker \varphi$, which is a submodule of M_1, can either be 0 or be M_1: in the latter case the homomorphism is trivial and in the former case it is an isomorphism.

Schur's lemma. Now let $\varphi \in \mathrm{End}_R(M)$ where M is irreducible. φ being an isomorphism, there exists $\varphi^{-1} : M \overset{\sim}{\longrightarrow} M$ such that $\varphi\varphi^{-1} = \varphi^{-1}\varphi = 1$, i.e., $\mathrm{End}_R(M)$ is a division ring.

Coming up...

- Tensor product
- Modules over principal ideal domains

Further reading:

[A] M. Artin, *Algebra*, Prentice Hall of India (1994).
[DF] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice Hall ed. 2 (1991).
[H] I. N. Herstein, *Topics in Algebra* ed. 2, Wiley (2019).