Invertible Ideals over an Integral Domain

E. L. Lady

Proposition. Let N be an ideal of a ring R containing only nilpotent elements.

(1) Let $r \in R$ be such that the image of r in R/N is invertible. Then r is invertible in R.

(2) Let $r \in R$ be such that the image of r in R/N is idempotent. Then there exists an idempotent $e \in R$ such that $e \equiv r \pmod N$.

PROOF: (1) Since r is invertible modulo N there $s \in R$ be such that $rs \equiv sr \equiv 1 \pmod N$. It now suffices to prove that rs and sr are invertible. Now let $n = 1 - rs$. Then $n \equiv 0 \pmod N$ so by hypothesis $n^k = 0$ for some k. Then

$$rs(1 + \cdots + n^{k-1}) = (1-n)(1 + \cdots + n^{k-1}) = 1 - n^k = 1.$$

(2) If $e \equiv r \pmod N$ then the image of e in R/N is idempotent, so $e^2 - e \in N$ and since all elements of N are nilpotent, $(e^2 - e)^k = 0$ for some k. Choose e so that k is as small as possible. We claim that $k = 1$. If not, note that $(2e-1)^2 = 1 + 4(e^2 - e)$ is invertible since $e^2 - e$ is nilpotent and thus $2e - 1$ is also invertible. Now $e(2e-1) = (2e-1)e$ and so $(2e-1)^{-1}e = e(2e-1)^{-1}$. Let $n = -(e^2 - e)(2e-1)^{-1}$. Then n commutes with e. It now follows that $n^k = (-1)^k(e^2-e)^k(2e-1)^{-k} = 0$. Since n commutes with e, $(e+n)^2 - (e+n) = e^2 - e + n(2e-1) + n^2 = e^2 - e - (e^2-e)(2e-1)^{-1}(2e-1) + n^2 = n^2$. Now $n^k = 0$ and if $k > 1$ then $2(k-1) = 2k - 2 \geq 2k - k = k$ so that $(n^2)^{k-1} = 0$. In other words, if $k > 1$ then $[(e+n)^2 - (e+n)]^{k-1} = 0$. Since $e + n \equiv e \equiv r \pmod N$ this contradicts the minimality of k. Thus $k = 1$ so that $e^2 - e = 0$ and e is an idempotent, as required. ☑

Lemma. Let M and N be **torsion free** modules over an integral domain D. Let $S = D \setminus \{0\}$. Identify M and N as submodules of $S^{-1}M$ and $S^{-1}N$ (which we can do since they are torsion free) and let $K = S^{-1}D$, the quotient field of D. Then $\operatorname{Hom}_D(M,N)$ can be identified with the set of K-linear transformations $\varphi_0 \colon S^{-1}M \to S^{-1}N$ such that $\varphi_0(M) \subseteq N$.

PROOF: If $\varphi_0 \colon S^{-1}M \to S^{-1}N$ is K-linear then it is a fortiori D-linear. Thus if $\varphi_0(M) \subseteq N$ then the restriction of φ_0 to M belongs to $\operatorname{Hom}_D(M,N)$.

Conversely, if $\varphi \in \operatorname{Hom}_D(M,N)$ then φ induces a K-linear map $\varphi_0 = S^{-1}\varphi \colon S^{-1}M \to S^{-1}N$ and φ is the restriction of φ_0. ☑

Theorem. Let D be a (commutative) integral domain and $\mathfrak{a}$ an ideal in D. Let K be the quotient field of D. Then the following conditions are equivalent:

(1) $\mathfrak{a}$ is projective.
(2) There exists an ideal $\mathfrak{b}$ of D such that $\mathfrak{a}\mathfrak{b}$ is principal.
(3) There exist $a_1, \dots a_n \in \mathfrak{a}$ and $b_1, \dots, b_n \in K$ such that $b_i\mathfrak{a} \subseteq D$ for all i and $\sum a_i b_i = 1$.

Furthermore, in this case the elements $a_1, \dots, a_n$ generate $\mathfrak{a}$. In practicular, $\mathfrak{a}$ is finitely generated. Also $\mathfrak{b} \approx \mathrm{Hom}_D(\mathfrak{a}, D)$ (as D-modules).

PROOF: (1) $\Leftrightarrow$ (3): Let $\{a_i\}_{i\in i}$ be a set of generators for $\mathfrak{a}$ and let F be a free D-module with a basis $\{e_i\}_{i\in I}$. Then there exists a surjection $\varphi\colon F \to \mathfrak{a}$ with $\varphi(e_i) = a_i$. And $\mathfrak{a}$ is projective if and only if φ splits. (If $\sum_I d_i e_i \in F$ then $\varphi(\sum_I d_i e_i) = \sum_I d_i a_i \in \mathfrak{a}$.)

Let $S = D \setminus \{0\}$ and let $K = S^{-1}D$. Then $S^{-1}\mathfrak{a}$ is a non-trivial Ksubspace of the one-dimensional vector space K so $S^{-1}\mathfrak{a} = K$. Now φ splits if and only if there exists $\sigma\colon \mathfrak{a} \to F$ such that $\varphi\sigma = 1_{\mathfrak{a}}$. By the preceding Lemma, such a σ exists if and only if there is a K-linear map $\sigma_0\colon S^{-1}\mathfrak{a} = K \to S^{-1}F$ such that $S^{-1}\varphi\,\sigma_0 = 1_K$ and $\sigma_0(\mathfrak{a}) \subseteq F$.

But if $\sigma_0\colon K \to F$ is K-linear then σ_0 is determined by $\sigma_0(1) = \sum b_i e_i$ where $b_i \in K$ and almost all b_i are zero. Suppose, say, that $b_1, \dots, b_t \neq 0$ and $b_i = 0$ otherwise. Then for $x \in \mathfrak{a}$, $\sigma_0(x) = \sum_1^t b_i x e_i \in F$ if and only if $b_i x \in D$ for $i = 1, \dots, t$. Thus $\sigma_0(\mathfrak{a}) \subseteq F$ if and only if $b_i\mathfrak{a} \subseteq D$ for $i = 1, \dots, t$. And $S^{-1}\varphi\,\sigma_0 = 1_K$ if and only if $1 = S^{-1}\varphi\,\sigma_0(1) = S^{-1}\varphi\,(\sum b_i e_i) = \sum_1^t b_i a_i$.

Thus $\mathfrak{a}$ is projective if and only if φ splits, and this occurs if and only if there exist $b_1, \dots, b_t \in K$ such that $b_i\mathfrak{a} \subseteq D$ for all i and $\sum a_i b_i = 1$.

Note further that if this is the case then for $a \in \mathfrak{a}$, $b_i a \in D$ for all i and $a = 1a = \sum_1^t a_i b_i a$. This shows that $a_1, \dots, a_t$ generate $\mathfrak{a}$.

(3) $\Rightarrow$ (2): Let $d \in D$ be a common denominator for $b_1, \dots, b_n$, i.e. $db_i \in D$ for all i. Let $\mathfrak{b}$ be the ideal generated by $db_1, \dots, db_n$. Then $\mathfrak{a}\mathfrak{b} = \sum db_i\mathfrak{a} \subseteq (d)$ since $b_i\mathfrak{a} \subseteq D$, and conversely $d = d\sum a_i b_i = \sum a_i db_i \in \mathfrak{a}\mathfrak{b}$ so $(d) \subseteq \mathfrak{a}\mathfrak{b}$. Thus $\mathfrak{a}\mathfrak{b}$ is principal.

(2) $\Rightarrow$ (3): Easy. ☑

Definition. If an ideal $\mathfrak{a}$ in an integral domain D satisfies the preceding conditions, we say that $\mathfrak{a}$ is **invertible**.