Ideal in a Dedekind domain is generated by at most two elements.

Joachim Jelisiejew, December 11, 2019

Facts that we proved before the faulty proof:

1. If two ideal $I, J \subset A$ satisfy $IA_{\mathfrak{m}} = JA_{\mathfrak{m}}$ for every $\mathfrak{m} \subset A$ maximal then $I = J$.

2. If A is an Artinian ring then $\mathrm{Spec}(A) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_s\}$ is finite, consists of maximal ideals and
$$A \simeq A_{\mathfrak{m}_1} \times A_{\mathfrak{m}_2} \times \ldots \times A_{\mathfrak{m}_s}.$$

Theorem 1. *Let A be a Dedekind domain and $I \subset A$ be a non-zero ideal. Let $0 \neq f \in I$ be any element. Then there exists $g \in I$ such that $(f, g) = I$.*

Proof. The closed set $V(f) \subset \mathrm{Spec}(A)$ is homeomorphic to $\mathrm{Spec}(A/(f))$ hence is a Noetherian topological space and so contains only finitely many elements. Since $f \neq 0$, every element of $V(f)$ is a maximal ideal, so every element of $V(f)$ is minimal with respect to inclusion in $V(f)$. Hence $V(f)$ is finite, say $V(f) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

The ring $A/(f)$ is Noetherian and zero-dimensional, hence Artinian, so using the fact above
$$\frac{A}{(f)} = \prod_{i=1}^{r} \left(\frac{A}{(f)}\right)_{\mathfrak{p}_i} = \prod_{i=1}^{r} \frac{A_{\mathfrak{p}_i}}{fA_{\mathfrak{p}_i}}. \qquad (1)$$

Recall that $IA_{\mathfrak{p}_i} = \mathfrak{p}_i^{e_i} A_{\mathfrak{p}_i}$, so the ideal $I/(f)$ corresponds on the right hand side to the ideal
$$\prod_{i=1}^{r} \frac{\mathfrak{p}_i^{e_i} A_{\mathfrak{p}_i}}{fA_{\mathfrak{p}_i}}.$$

For every $i = 1, 2, \ldots, r$ pick $t_i \in A$ such that $t_i A_{\mathfrak{p}_i} = \mathfrak{p}_i A_{\mathfrak{p}_i}$ is a local parameter. Then the ideal $\prod_{i=1}^{r} \frac{\mathfrak{p}_i^{e_i} A_{\mathfrak{p}_i}}{fA_{\mathfrak{p}_i}}$ in $\prod_{i=1}^{r} \frac{A_{\mathfrak{p}_i}}{fA_{\mathfrak{p}_i}}$ is actually generated by the single element $(t_1^{e_1}, \ldots, t_r^{e_r})$. Let $\bar{g} \in A/(f)$ correspond to this element in the isomorphism (1). Then $(\bar{g} + (f))/(f) = I/(f)$. Let $g \in A$ be any preimage of $\bar{g}$. Then we have an equality of ideals
$$\frac{(g) + (f)}{(f)} = \frac{I}{(f)}.$$

It follows that $I + (f) = (g) + (f)$ as ideals of A. Since $f \in I$, the left hand side is just I, so $I = (g, f)$. ∎

Remark 2. On the lecture I wrongly tried to take g equal to $t_1^{e_1} \ldots t_r^{e_r}$. This particular choice of g was elegant but incorrect, because we had no guarantee that $gA_{\mathfrak{p}_i} = \mathfrak{p}_i^{e_i} A_{\mathfrak{p}_i}$: we might have chosen for example $t_1 \in \mathfrak{p}_1 \cap \mathfrak{p}_2$ and then $gA_{\mathfrak{p}_2}$ is divisible by $t_2^{e_1+e_2}$. To make g work we need to choose $t_i \in \mathfrak{p}_i \setminus \bigcup_{j \neq i} \mathfrak{p}_j$. This can be done by the Chinese remainder theorem, see below.

Remark 3. The ring $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain but not a PID, for example the ideal $(2, 1 + \sqrt{-5})$ is not principal. Hence one cannot hope for all ideals to be generated by one element.

Remark 4. The big picture is that Dedekind domains correspond to smooth one-dimensional objects (Dedekind domains that are finitely generated $\mathbb{k}$-algebras are exactly affine *algebraic curves*). In the above argument we repeatedly use the trick: reduce to a closed subset of curve (=finitely many points) and then look locally at each point separately.

Second proof – bonus. The closed set $V(f) \subset \operatorname{Spec}(A)$ is homeomorphic to $\operatorname{Spec}(A/(f))$ hence is a Noetherian topological space and so contains only finitely many elements. But $f \neq 0$ so every element of $V(f)$ is a maximal ideal, so every element of $V(f)$ is minimal. Hence $V(f)$ is finite, say $V(f) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

Let $t_i \in A$ be an element such that $t_i A_{\mathfrak{p}_i} = \mathfrak{p}_i A_{\mathfrak{p}_i}$ for $i = 1, \ldots, r$. Let $e_i = \nu_{\mathfrak{p}_i}(I)$ be defined as

$$IA_{\mathfrak{p}_i} = \mathfrak{p}^{e_i} A_{\mathfrak{p}_i}.$$

Then $IA_{\mathfrak{p}_i} = t_i^{e_i} A_{\mathfrak{p}_i}$ and $(f)A_{\mathfrak{p}_i} = t_i^{e_i'} A_{\mathfrak{p}_i}$ for some $e_i, e_i' \mathbb{Z}_{\geq 0}$. Since $f \in I$ we have $e_i' \geq e_i$.

The maximal ideals $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are coprime for every pair $i \neq j$, so also $\mathfrak{p}_i^{e_i+1}$ and $\mathfrak{p}_j^{e_j+1}$ are coprime and by the Chinese Remainder theorem (see [Problem 4, Set 10, Exercises]), there exists an element $g \in A$ such that

$$g \equiv t_i^{e_i} \mod \mathfrak{p}_i^{e_i+1}$$

for $i = 1, 2, \ldots, r$. Then $gA_{\mathfrak{p}_i} + \mathfrak{p}_i^{e_i+1} A_{\mathfrak{p}_i} = t_i^{e_i} A_{\mathfrak{p}_i} + \mathfrak{p}^{e_i+1} A_{\mathfrak{p}_i} = \mathfrak{p}_i^{e_i} A_{\mathfrak{p}_i}$ so by local version of Nakayama we have $gA_{\mathfrak{p}_i} = \mathfrak{p}_i^{e_i} A_{\mathfrak{p}_i}$. Then we also have

$$gA_{\mathfrak{p}_i} = \mathfrak{p}_i^{e_i} A_{\mathfrak{p}_i} = t_i^{e_i} A_{\mathfrak{p}_i} = IA_{\mathfrak{p}_i}.$$

Consider the ideal $J = (f, g)$ and a maximal ideal $\mathfrak{q} \subset A$. If $\mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ then $f \notin \mathfrak{q}$, so f is invertible in $A_{\mathfrak{q}}$ and $JA_{\mathfrak{q}} = A_{\mathfrak{q}} = IA_{\mathfrak{q}}$. If $\mathfrak{q} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ say $\mathfrak{q} = \mathfrak{p}_i$, then

$$JA_{\mathfrak{p}_i} = (f)A_{\mathfrak{p}_i} + (g)A_{\mathfrak{p}_i} = \mathfrak{p}_i^{e_i'} A_{\mathfrak{p}_i} + \mathfrak{p}_i^{e_i} A_{\mathfrak{p}_i} = \mathfrak{p}_i^{e_i} A_{\mathfrak{p}_i} = IA_{\mathfrak{p}_i}$$

since $e_i' \geq e_i$. We have proven that $JA_{\mathfrak{q}} = IA_{\mathfrak{q}}$ for all maximal $\mathfrak{q}$, hence $J = I$ by the fact above. $\square$