D-MATH Number Theory I HS 2023
Prof. Richard Pink

Solutions 3

Dedekind rings, Fractional ideals, Lattices

1. Show that for all fractional ideals $\mathfrak{a}$ of a Dedekind ring A we have $\mathfrak{a}^{-1}\mathfrak{a} = (1)$.

   Solution: By the definition of $\mathfrak{a}^{-1}$ we have $\mathfrak{a}^{-1}\mathfrak{a} \subset (1)$. If this is a proper inclusion, there exists a maximal ideal $\mathfrak{p}$ with $\mathfrak{a}^{-1}\mathfrak{a} \subset \mathfrak{p}$. Multiplying by $\mathfrak{p}^{-1}$ we then deduce that $\mathfrak{p}^{-1}\mathfrak{a}^{-1}\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{p} \subset (1)$. By the definition of $\mathfrak{a}^{-1}$ this means that $\mathfrak{p}^{-1}\mathfrak{a}^{-1} \subset \mathfrak{a}^{-1}$. But this now contradicts Lemma 1.10.4 (b).

2. (a) Show that for all fractional ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ of a Dedekind ring A we have $(\mathfrak{a}+\mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$ and $(\mathfrak{a}\cap\mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} \cap \mathfrak{b}\mathfrak{c}$.

   (b) Do the same formulas hold for ideals of an arbitrary ring?

   Solution: (a) By definition $(\mathfrak{a}+\mathfrak{b})\mathfrak{c}$ is the fractional ideal that is generated by all elements of the form $(a+b)c$ for all $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ and $c \in \mathfrak{c}$. Taking $b = 0$ this includes all elements of the form ac, and taking $a = 0$ it includes all elements of the form bc. Thus $(\mathfrak{a}+\mathfrak{b})\mathfrak{c}$ is also generated by all elements of the form $ac + bc'$ with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ and $c, c' \in \mathfrak{c}$. But these are just the generators of $\mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$; whence the first inequality.

   Next $\mathfrak{a}\cap\mathfrak{b} \subset \mathfrak{a}$ implies that $(\mathfrak{a}\cap\mathfrak{b})\mathfrak{c} \subset \mathfrak{a}\mathfrak{c}$, and $\mathfrak{a}\cap\mathfrak{b} \subset \mathfrak{b}$ implies that $(\mathfrak{a}\cap\mathfrak{b})\mathfrak{c} \subset \mathfrak{b}\mathfrak{c}$. Together this shows that $(\mathfrak{a}\cap\mathfrak{b})\mathfrak{c} \subset \mathfrak{a}\mathfrak{c}\cap\mathfrak{b}\mathfrak{c}$. Applying this to the triple $(\mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{c}, \mathfrak{c}^{-1})$ in place of $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$ we also obtain

   $$\mathfrak{a}\mathfrak{c} \cap \mathfrak{b}\mathfrak{c} \;=\; (\mathfrak{a}\mathfrak{c} \cap \mathfrak{b}\mathfrak{c})\mathfrak{c}^{-1}\mathfrak{c} \;\subset\; (\mathfrak{a}\mathfrak{c}\mathfrak{c}^{-1} \cap \mathfrak{b}\mathfrak{c}\mathfrak{c}^{-1})\mathfrak{c} \;=\; (\mathfrak{a}\cap\mathfrak{b})\mathfrak{c}.$$

   Together we thus deduce the second equality.

   (b) The proof of the first formula in (a) works for ideals of an arbitrary ring, but not the second. Indeed that formula is false in general. For instance consider the polynomial ring $R = k[X, Y]$ in two variables over a field k and take $\mathfrak{a} := (X)$ and $\mathfrak{b} := (Y)$ and $\mathfrak{c} := (X, Y)$. Then $\mathfrak{a}\cap\mathfrak{b} = (XY)$ and hence $(\mathfrak{a}\cap\mathfrak{b})\mathfrak{c} = (X^2Y, XY^2)$, whereas $\mathfrak{a}\mathfrak{c} = (X^2, XY)$ and $\mathfrak{b}\mathfrak{c} = (XY, Y^2)$ and therefore $\mathfrak{a}\mathfrak{c} \cap \mathfrak{b}\mathfrak{c} = (XY)$.

3. Consider non-zero ideals $\mathfrak{a}, \mathfrak{b}$ of a Dedekind ring A with the prime factorizations $\mathfrak{a} = \prod_{i=1}^n \mathfrak{p}_i^{\mu_i}$ and $\mathfrak{b} = \prod_{i=1}^n \mathfrak{p}_i^{\nu_i}$ for distinct maximal ideals $\mathfrak{p}_i$ and exponents $\mu_i, \nu_i \geqslant 0$.

   (a) Prove that

   $$\begin{aligned} \mathfrak{a} + \mathfrak{b} &= \textstyle\prod_{i=1}^n \mathfrak{p}_i^{\min\{\mu_i,\nu_i\}}, \\ \mathfrak{a} \cap \mathfrak{b} &= \textstyle\prod_{i=1}^n \mathfrak{p}_i^{\max\{\mu_i,\nu_i\}}, \\ \mathfrak{a} \cdot \mathfrak{b} &= \textstyle\prod_{i=1}^n \mathfrak{p}_i^{\mu_i+\nu_i}. \end{aligned}$$

(b) Explain which of these operations can be viewed as the greatest common divisor, respectively the least common multiple, of ideals.

(c) Deduce Proposition 1.11.5.

Solution:

(a) First, we show the following

Lemma: Consider non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset A$ with prime factorizations $\mathfrak{a} = \prod_{i=1}^n \mathfrak{p}_i^{\alpha_i}$ and $\mathfrak{b} = \prod_{i=1}^n \mathfrak{p}_i^{\beta_i}$ for distinct $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Then we have $\mathfrak{a} \subset \mathfrak{b}$ if and only if $\alpha_i \geqslant \beta_i$ for all i.

Proof. If $\alpha_i \geqslant \beta_i$ for all i, then $\mathfrak{p}_i^{\alpha_i} \subset \mathfrak{p}_i^{\beta_i}$ for all i and hence $\mathfrak{a} \subset \mathfrak{b}$. Conversely assume $\mathfrak{a} \subset \mathfrak{b}$ and suppose that there exists $1 \leqslant j \leqslant n$ with $\alpha_j < \beta_j$. Then multiplication by $\mathfrak{p}_j^{-\alpha_j}$ yields

$$\prod_{i \neq j} \mathfrak{p}_i^{\alpha_i} \;=\; \mathfrak{p}_j^{-\alpha_j}\mathfrak{a} \;\subset\; \mathfrak{p}_j^{-\alpha_j}\mathfrak{b} \;=\; \mathfrak{p}_j^{\beta_j - \alpha_j} \prod_{i \neq j} \mathfrak{p}_i^{\beta_i} \;\subset\; \mathfrak{p}_j.$$

As $\mathfrak{p}_j$ is a prime ideal, it follows that some factor $\mathfrak{p}_i$ for $i \neq j$ is contained in $\mathfrak{p}_j$. Since $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are maximal ideals, the inclusion $\mathfrak{p}_i \subset \mathfrak{p}_j$ must then be an equality, contradicting the assumption that $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct. Thus all $\alpha_j \geqslant \beta_j$, as desired. □

As $\mathfrak{a}, \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}$, applying the Lemma twice yields a prime factorization $\mathfrak{a}+\mathfrak{b} = \prod_{i=1}^n \mathfrak{p}_i^{\xi_i}$ with $\xi_i \leqslant \min\{\mu_i, \nu_i\}$ for all i. Moreover, the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are trivially contained in $\prod_{i=1}^n \mathfrak{p}_i^{\min\{\mu_i,\nu_i\}}$, hence their sum is too. By the Lemma, this yields $\xi_i \geqslant \min\{\mu_i, \nu_i\}$. Together, we get $\min\{\mu_i, \nu_i\} \geqslant \xi_i \geqslant \min\{\mu_i, \nu_i\}$ and thus equality.

Next $\prod_{i=1}^n \mathfrak{p}_i^{\max\{\mu_i,\nu_i\}}$ is trivially contained in $\mathfrak{a} \cap \mathfrak{b}$, so applying the Lemma yields a prime factorization $\mathfrak{a} \cap \mathfrak{b} = \prod_{i=1}^n \mathfrak{p}_i^{\eta_i}$ with $\eta_i \leqslant \max\{\mu_i, \nu_i\}$ for all i. Moreover, we have $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}, \mathfrak{b}$, so applying the Lemma twice, we obtain $\eta_i \geqslant \nu_i, \mu_i$. Thus $\eta_i = \max\{\nu_i, \mu_i\}$.

Finally, the formula for the product follows directly from the multiplication rules of ideals.

Aliter: The formula for the product follows directly from the multiplication rules of ideals. For the other two formulas set $\lambda_i := \min\{\mu_i, \nu_i\}$, so that $\mu_i = \lambda_i + \mu_i'$ and $\nu_i = \lambda_i + \nu_i'$ with integers $\mu_i', \nu_i' \geqslant 0$, and set $\mathfrak{c} := \prod_{i=1}^n \mathfrak{p}_i^{\lambda_i}$, so that $\mathfrak{a} = \mathfrak{a}'\mathfrak{c}$ with $\mathfrak{a}' := \prod_{i=1}^n \mathfrak{p}_i^{\mu_i'}$ and $\mathfrak{b} = \mathfrak{b}'\mathfrak{c}$ with $\mathfrak{b}' := \prod_{i=1}^n \mathfrak{p}_i^{\nu_i'}$. Then by the formulas in Exercise 2 it suffices to prove the two equalities for $(\mathfrak{a}', \mathfrak{b}')$ in place of $(\mathfrak{a}, \mathfrak{b})$.
In that case we must prove that $\mathfrak{a}' + \mathfrak{b}' = (1)$. Suppose that this were not the case. Then $\mathfrak{a}' + \mathfrak{b}'$ is contained in some maximal ideal $\mathfrak{p}$. But then $\mathfrak{a}' \subset \mathfrak{p}$

and Proposition 1.11.3 implies that $\mathfrak{a}' = \mathfrak{a}''\mathfrak{p}$ for some ideal $\mathfrak{a}''$, and then the prime factorization of $\mathfrak{a}''$ multiplied by $\mathfrak{p}$ must be the prime factorization of $\mathfrak{a}'$. Therefore $\mathfrak{p}$ must appear in the prime factorization of $\mathfrak{a}'$. Thus for some i we have $\mathfrak{p} = \mathfrak{p}_i$ and $\mu_i' > 0$. But by the same argument with $\mathfrak{b}'$ in place of $\mathfrak{a}'$ we deduce that $\nu_i' > 0$. This contradicts the construction. Therefore $\mathfrak{a}' + \mathfrak{b}' = (1)$, as desired.

Thus $\mathfrak{a}'$ and $\mathfrak{b}'$ are coprime. Observe that $\mathfrak{a}' \cap \mathfrak{b}'$ is the kernel of the homomorphism $A \to (A/\mathfrak{a}') \times (A/\mathfrak{b}')$, $x \mapsto (x + \mathfrak{a}', x + \mathfrak{b}')$. But by the Chinese Remainder Theorem this is also equal to $\mathfrak{a}'\mathfrak{b}'$. Thus $\mathfrak{a}' \cap \mathfrak{b}' = \mathfrak{a}'\mathfrak{b}'$, which by the formula for the product is $\prod_{i=1}^n \mathfrak{p}_i^{\mu_i'+\nu_i'} = \prod_{i=1}^n \mathfrak{p}_i^{\max\{\mu_i',\nu_i'\}}$, as desired.

(b) We say that an ideal $\mathfrak{b}$ *divides* $\mathfrak{a}$ if and only if $\mathfrak{a} \subset \mathfrak{b}$. Thus an ideal $\mathfrak{c}$ is a common divisor of $\mathfrak{a}$ and $\mathfrak{b}$ if and only if $\mathfrak{a} \subset \mathfrak{c}$ and $\mathfrak{b} \subset \mathfrak{c}$, or equivalently $\mathfrak{a} + \mathfrak{b} \subset \mathfrak{c}$. Therefore we can view $\mathfrak{a} + \mathfrak{b}$ as the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$.

Similarly both $\mathfrak{a}$ and $\mathfrak{b}$ divide of $\mathfrak{c}$ if and only if $\mathfrak{c} \subset \mathfrak{a}$ and $\mathfrak{c} \subset \mathfrak{b}$, or equivalently $\mathfrak{c} \subset \mathfrak{a} \cap \mathfrak{b}$. Therefore we can view $\mathfrak{a} \cap \mathfrak{b}$ as the least common multiple of $\mathfrak{a}$ and $\mathfrak{b}$.

(c) By (a) we have $\mathfrak{a} + \mathfrak{b} = (1)$ if and only if $\min\{\mu_i, \nu_i\} = 0$ for all i, which means that their factorizations in maximal ideals do not have a common factor. Moreover, we have $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$ if and only if $\mu_i + \nu_i = \max\{\mu_i, \nu_i\}$. As the μ_i and ν_i are non-negative integers, the second condition means that for each i we have $\mu_i = 0$ or $\nu_i = 0$, which implies that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime.

4. Prove that a Dedekind ring is factorial if and only if it is a principal ideal domain.

Solution: As principal ideal domains are factorial, it suffices to show the other implication. Let A be a factorial Dedekind ring and consider a non-zero prime ideal $\mathfrak{p}$. Let a be a non-zero element of $\mathfrak{p}$. Then by assumption we can write $a = up_1 \cdots p_n$ with a unit u and prime elements p_i. Since $\mathfrak{p}$ is prime, it must contain at least one factor of this product, and it cannot contain the unit u. Thus some $p_i \in \mathfrak{p}$. Then $(p_i) \subset \mathfrak{p}$ is an inclusion of two non-zero prime ideals. As A has Krull dimension 1, this must be an equality. All this shows that every non-zero prime ideal of A is principal. As every non-zero ideal can be written as the product of non-prime ideals, it is principal as well.

5. Consider the number field $K := \mathbb{Q}(\sqrt{-5})$ and its ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.

(a) Show that $(3) = \mathfrak{p}\mathfrak{p}'$ with prime ideals $\mathfrak{p} := (3, 1+\sqrt{-5})$ and $\mathfrak{p}' := (3, 1-\sqrt{-5})$.

(b) Determine the structure of the ring $\mathcal{O}_K/(3)$.

(c) Determine the inverse of $\mathfrak{p}$ as a fractional ideal.

(d) Which powers of the ideal $\mathfrak{p}$ are principal?

(e) Compute the factorization of (2) into prime ideals.

(f) Compute the factorization of (5) into prime ideals.

(g) Compute the factorization of (11) into prime ideals.

Solution:

(a) By definition the ideal $\mathfrak{p}\mathfrak{p}'$ is generated by $3 \cdot 3 = 9$ and $3 \cdot (1 \pm \sqrt{-5})$ and $(1+\sqrt{-5}) \cdot (1-\sqrt{-5}) = 6$. Thus it contains $9-6=3$, which in turn divides all other generators; hence $\mathfrak{p}\mathfrak{p}' = (3)$.

Since $1 \pm \sqrt{-5} \notin (3)$, both $\mathfrak{p}$ and $\mathfrak{p}'$ properly contain (3). Thus the formula $\mathfrak{p}\mathfrak{p}' = (3)$ also implies that both $\mathfrak{p}$ and $\mathfrak{p}'$ are properly contained in $\mathcal{O}_K$.

Next observe that $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} \cdot \sqrt{-5}$; hence $(3) = 3\mathcal{O}_K = 3\mathbb{Z} \oplus 3\mathbb{Z} \cdot \sqrt{-5}$ has index 9 in $\mathcal{O}_K$. As the inclusions $(3) \subset \mathfrak{p} \subset \mathcal{O}_K$ and $(3) \subset \mathfrak{p}' \subset \mathcal{O}_K$ are all proper, it follows that $\mathfrak{p}, \mathfrak{p}' \subset \mathcal{O}_K$ have index 3. Thus the factor rings $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_K/\mathfrak{p}'$ have order 3. But any ring of order 3 is isomorphic to $\mathbb{F}_3$ and hence a field; which implies that $\mathfrak{p}$ and $\mathfrak{p}'$ are prime ideals.

(b) Since $2 \cdot (1+\sqrt{-5}) + 2 \cdot (1-\sqrt{-5}) - 3 = 1$ lies in $\mathfrak{p} + \mathfrak{p}'$, the ideals $\mathfrak{p}$ and $\mathfrak{p}'$ are coprime. By part (a) and the Chinese Remainder Theorem it follows that $\mathcal{O}_K/(3) \cong \mathcal{O}_K/\mathfrak{p} \times \mathcal{O}_K/\mathfrak{p}' \cong \mathbb{F}_3 \times \mathbb{F}_3$.

(c) The inverse fractional ideal of (3) is $(\frac{1}{3})$; hence (a) implies that $\mathfrak{p}^{-1} = (\frac{1}{3}) \cdot \mathfrak{p}' = (1, \frac{1-\sqrt{-5}}{3})$.

(d) For any principal ideal $\mathfrak{a} = (a + b\sqrt{-5}) \subseteq \mathcal{O}_K$ we have $[\mathcal{O}_K : \mathfrak{a}] = \mathrm{Norm}(\mathfrak{a}) = |\mathrm{Norm}_{K/\mathbb{Q}}(a + b\sqrt{-5})| = a^2 + 5b^2$. For all $a, b \in \mathbb{Z}$ this number is $\neq 3$. Since $[\mathcal{O}_K : \mathfrak{p}] = 3$, it follows that $\mathfrak{p}$ is not principal.

Next, the ideal $\mathfrak{p}^2$ is generated by the elements $3 \cdot 3 = 9$ and $3 \cdot (1+\sqrt{-5})$ and $(1+\sqrt{-5})^2 = -4 + 2\sqrt{-5}$. Thus it also contains the smaller element

$$9 - 3 \cdot (1+\sqrt{-5}) + (-4 + 2\sqrt{-5}) \;=\; 2 - \sqrt{-5}.$$

This obviously divides the third generator, and since $\mathrm{Norm}_{K/\mathbb{Q}}(2-\sqrt{-5}) = (2-\sqrt{-5}) \cdot (2+\sqrt{-5}) = 2^2 + 5 = 9$, it also divides the first generator. Since $3 \cdot (1+\sqrt{-5}) + 3 \cdot (2-\sqrt{-5}) = 9$, it therefore also divides the second generator; hence $\mathfrak{p}^2 = (2-\sqrt{-5})$ is principal.

Together this shows that the ideal class of $\mathfrak{p}$ in the class group $\mathrm{Cl}(\mathcal{O}_K)$ has order 2. Therefore $\mathfrak{p}^n$ is principal if and only if n is even.

(e) Since $\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2+5)$ with $\sqrt{-5}$ corresponding to the residue class of X, we have $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2+5)$. Since $X^2 + 5 = (1+X)^2$ in $\mathbb{F}_2[X]$, it follows that $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(1+X)^2$. This ring has the unique maximal ideal $(1+X)/(1+X)^2$, and the factor ring is $\mathbb{F}_2 \cong \mathbb{F}_2[X]/(1+X) \cong \mathcal{O}_K/\mathfrak{q}$ for $\mathfrak{q} := (2, 1+\sqrt{-5})$. Thus $\mathfrak{q}$ is a prime ideal. The isomorphism $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(1+X)^2$ also shows that $\mathfrak{q}^2$ maps to zero in $\mathcal{O}_K/(2)$; hence $\mathfrak{q}^2 \subseteq (2)$. Since $[\mathcal{O}_K : \mathfrak{q}^2] = [\mathcal{O}_K : \mathfrak{q}]^2 = 2^2 = [\mathcal{O}_K : (2)]$, it follows that $\mathfrak{q}^2 = (2)$.

Note: In the same way as in (d) one can show that $\mathfrak{q}$ is not a principal ideal.

Aliter (using divisibility only): Trial computation shows that $(1+\sqrt{-5})^2 = 2(2-\sqrt{-5})$ is divisible by 2. Thus $1+\sqrt{-5}$ must be divisible by some prime ideal dividing (2), i.e., containing 2, and so the ideal $\mathfrak{q} := (2, 1+\sqrt{-5})$ is also divisible by that prime ideal. On the other hand we have $1+\sqrt{-5} \notin 2\mathbb{Z} \oplus 2\mathbb{Z}\sqrt{-5} = (2)$. Together this implies that $(2) \subsetneq \mathfrak{q} \subsetneq \mathcal{O}_K$. Since $[\mathcal{O}_K : (2)] = 4$, it follows that $[\mathcal{O}_K : \mathfrak{q}] = 2$ and that $\mathfrak{q}$ is a maximal ideal. In particular $\mathfrak{q}$ is a prime ideal. Finally, the ideal $\mathfrak{q}^2$ is generated by the elements $2 \cdot 2 = 4$ and $2 \cdot (1+\sqrt{-5})$ and $(1+\sqrt{-5})^2 = -4 + 2\sqrt{-5}$. Thus it also contains the element $-4 + 2 \cdot (1+\sqrt{-5}) - (-4+2\sqrt{-5}) = 2$. Since that in turn divides all other generators, it follows that $\mathfrak{q}^2 = (2)$.

(f) Since $\sqrt{-5}^2 = -5$, we have $(\sqrt{-5}) = \mathbb{Z}\sqrt{-5} \oplus \mathbb{Z}5$ and so $\mathcal{O}_K/(\sqrt{-5}) \cong \mathbb{F}_5$. As that is a field, the ideal $(\sqrt{-5})$ is a prime ideal. Moreover $(\sqrt{-5})^2 = (-5) = (5)$, and we are done.

(g) Since $\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2+5)$, we have $\mathcal{O}_K/(11) \cong \mathbb{F}_{11}[X]/(X^2+5)$. Since the only squares in $\mathbb{F}_{11}$ are the residue classes $0, 1, 4, 9, 5, 3$, the polynomial $X^2 + 5 = X^2 - 6$ has no zero in $\mathbb{F}_{11}$ and is therefore irreducible. Thus the factor ring $\mathcal{O}_K/(11)$ is a finite field of order 11^2; hence (11) is already a prime ideal.

6. Show that a subgroup Γ of a finite-dimensional $\mathbb{R}$-vector space V is a complete lattice if and only if Γ is discrete and V/Γ is compact.

Solution: Suppose that Γ is a complete lattice, i.e., that $\Gamma = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$ for an $\mathbb{R}$-basis $v_1, \ldots, v_n$ of V. Then we can identify V with $\mathbb{R}^n$ such that $\Gamma = \mathbb{Z}^n$. Then Γ is discrete and we get homeomorphisms $V/\Gamma \cong \mathbb{R}^n/\mathbb{Z}^n \cong (\mathbb{R}/\mathbb{Z})^n \cong (S^1)^n$, which is compact (and Hausdorff).

Aliter: Then Γ is discrete by definition of the topology of V. Next we have $V = \Phi + \Gamma$ for $\Phi := \{\sum x_i v_i \mid \forall i : 0 \leqslant x_i \leqslant 1\}$. Thus we obtain a continuous surjective map $\Phi \twoheadrightarrow V/\Gamma$. Since Φ is bounded and closed, it is compact; hence its image V/Γ is compact, too.

Conversely, suppose that Γ is discrete and V/Γ is compact. By a proposition from the lecture, the first condition implies that $\Gamma = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_m$ for $\mathbb{R}$-linearly independent $v_1, \ldots, v_m \in V$. Let $V_1 := \operatorname{span}(v_1, \ldots, v_m)$ and write $V = V_1 \oplus V_2$ for some subspace $V_2 \subseteq V$. Then we obtain a homeomorphism $V/\Gamma \cong V_1/\Gamma \times V_2$, and it follows that $\dim V_2 = 0$, because V/Γ is compact. In conclusion, the lattice Γ is complete.