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

Solutions 2

Noetherian rings, Dedekind rings, Linearly disjoint extensions, Fractional ideals

1. Prove that the following conditions on a ring A are equivalent:

   (a) Every ideal of A is finitely generated.

   (b) Every ascending sequence of ideals of A becomes stationary.

   (c) Every non-empty set of ideals of A possesses a maximal element.

   (a′) Every submodule of a finitely generated A-module is finitely generated.

   (b′) Every ascending sequence of submodules of a finitely generated A-module becomes stationary.

   (c′) Every non-empty set of submodules of a finitely generated A-module possesses a maximal element.

   Solution: (a)⇒(b): Let $(\mathfrak{a}_n)_{n\geqslant 0}$ be an ascending sequence of ideals. Define $\mathfrak{a} := \bigcup_{n\geqslant 0}\mathfrak{a}_n$. Since each $\mathfrak{a}_n$ contains 0, so does $\mathfrak{a}$. Next consider $x, y \in \mathfrak{a}$ and $a \in A$. By definition of $\mathfrak{a}$, there exist $n_1, n_2 \geqslant 0$ such that $x \in \mathfrak{a}_{n_1}$ and $y \in \mathfrak{a}_{n_2}$. As the sequence $(\mathfrak{a}_n)_{n\geqslant 0}$ is ascending, we have $x, y \in \mathfrak{a}_{\max\{n_1,n_2\}}$. Moreover, since $\mathfrak{a}_{\max\{n_1,n_2\}}$ is an ideal, we have

   $$ax + y \in \mathfrak{a}_{\max\{n_1,n_2\}} \subset \mathfrak{a}$$

   and thus $\mathfrak{a}$ is an ideal. By (a) the ideal $\mathfrak{a}$ is finitely generated, i.e., there exist $x_1, \ldots, x_m \in A$ such that $\mathfrak{a} = (x_1, \ldots, x_m)$. By the definition of $\mathfrak{a}$ as the union of the $\mathfrak{a}_n$, for each $1 \leqslant i \leqslant m$ there exists an $n_i \geqslant 0$ such that $x_i \in \mathfrak{a}_{n_i}$. Hence, for $n := \max\{n_1, \ldots, n_m\}$, we have

   $$\mathfrak{a} = (x_1, \ldots, x_m) \subset \mathfrak{a}_n.$$

   Therefore $\mathfrak{a}_{n'} = \mathfrak{a}$ for all $n' \geqslant n$, and so the ascending sequence of ideals becomes stationary.

   (b)⇒(c): If (c) is false, there exists a non-empty set of ideals S without a maximal element. We can then recursively construct a non-terminating strictly ascending sequence of ideals contained in S, which is a contradiction to (b).

   (c)⇒(a): Let $\mathfrak{a}$ be an ideal and let S be the set of ideals generated by finitely many elements of $\mathfrak{a}$. Then S is non-empty and thus possesses a maximal element $\mathfrak{b} = (x_1, \ldots x_n)$ with $x_1, \ldots, x_n \in \mathfrak{a}$. If $\mathfrak{a} \neq (x_1, \ldots x_n)$, there exists $x_{n+1} \in \mathfrak{a} \smallsetminus \mathfrak{b}$. Then

$(x_1, \ldots, x_{n+1})$ strictly contains $\mathfrak{b}$ and is contained in S, violating the maximality of $\mathfrak{b}$. Thus we have $\mathfrak{a} = \mathfrak{b}$ and in particular, the ideal $\mathfrak{a}$ is finitely generated.

Using analogous arguments, one can show the equivalences (a′) $\iff$ (b′) $\iff$ (c′).

The implication (a′)$\Rightarrow$(a) directly follows from the fact that every ideal of A is a submodule of the A-module A.

(a)$\Rightarrow$(a′): Let M be a finitely generated A-module and suppose that it is generated by $x_1, \ldots, x_n$. Let N be a submodule of M. We shall show that N is finitely generated by induction on n. In the case $n = 0$ we have $N = M = 0$, so the assertion is obvious.

Now suppose that $n > 0$. Consider the surjective A-linear map $A \twoheadrightarrow Ax_1 \subset M$, $a \mapsto ax_1$. The preimage of N under this map is an ideal, which is finitely generated by the assumption (a). Let $z_1, \ldots, z_k$ be the images of these generators, which generate the submodule $N \cap Ax_1$. Next the factor module M/Ax_1 is generated by $n-1$ elements, so by the induction hypothesis the image $\overline{N}$ of N in M/Ax_1 is finitely generated. Choose elements $y_1, \ldots, y_m \in N$ whose images generate $\overline{N}$.

We claim that the elements $y_1, \ldots, y_m$ and $z_1, \ldots, z_k$ together generate N. To see this, take any $f \in N$ and write its image in $\overline{N}$ as the image of a linear combination $a_1y_1 + \ldots + a_my_m$. Then by construction we have $f - (a_1y_1 + \ldots + a_my_m) \in N \cap Ax_1$, which is therefore a linear combination of $z_1, \ldots, z_k$. This shows that f is a linear combination of $y_1, \ldots, y_m$ and $z_1, \ldots, z_k$, as desired. Thus N is finitely generated.

2. Let A be a Noetherian ring. Then for every multiplicative subset $S \subset A$, the ring $S^{-1}A$ is Noetherian.

   Solution: Let $\mathfrak{a} \subset A[S^{-1}]$ be an ideal. Under the condition of $\mathfrak{a}$ being prime, we prove in exercise 5 of sheet 1 that $\mathfrak{a} = S^{-1}(\mathfrak{a} \cap A)$. However, the argument presented there works for any ideal. Using this, we see that $\mathfrak{a}$ is generated by a set of generators of $\mathfrak{a} \cap A$. As A is Noetherian, then $\mathfrak{a} \cap A$ is finitely generated, so $\mathfrak{a}$ is too.

3. Prove that for any two finite field extensions $L, L'/K$ within a common overfield M the following conditions are equivalent:

   (a) L and L' are linearly disjoint over K, that is, the algebra $L \otimes_K L'$ is a field.
   (b) $[LL'/K] = [L/K] \cdot [L'/K]$
   (c) $[LL'/L] = [L'/K]$
   (d) $[LL'/L'] = [L/K]$

   Moreover, these conditions imply:

   (e) $L \cap L' = K$.

Conversely, if at least one of L/K and L'/K is galois, then (e) implies the other conditions.

Solution: First observe that since the extension L'/K is finite, it is finitely generated algebraic. Thus LL'/L is finitely generated algebraic and therefore finite. It follows that LL'/K is finite. By the multiplicativity of the degrees we thus have

$$(*) \qquad [LL'/K] \;=\; [LL'/L]\cdot[L/K] \;=\; [LL'/L']\cdot[L'/K].$$

As every factor is a positive integer, it follows that (b), (c), (d) are all equivalent.

Next the map $L\times L'\to LL'$, $(y,y')\mapsto yy'$ is K-bilinear, so by the universal property of the tensor product there is a unique K-linear map $\varphi\colon L\otimes_K L'\to LL'$ satisfying $y\otimes y'\mapsto yy'$. The image of this map is a subring which contains K and generates LL' as a field. As LL'/K is finite, this subring is already equal to LL'. Therefore φ is surjective. If $L\otimes_K L'$ is a field, then φ is also injective and hence an isomorphism. Otherwise it cannot be an isomorphism, because LL' is a field. Thus we always have $\dim_K(L\otimes_K L')\geqslant[LL'/K]$ with equality if and only $L\otimes_K L'$ is a field. Since

$$\dim_K(L\otimes_K L') \;=\; \dim_K(L)\cdot\dim_K(L') \;=\; [L/K]\cdot[L'/K],$$

this shows that (a) is equivalent to (b).

Next suppose that there exists $\ell\in(L\cap L')\smallsetminus K$. Then the element $\ell\otimes\ell^{-1}\in L\otimes L'$ satisfies $\varphi(\ell\otimes\ell^{-1})=1=\varphi(1\otimes1)$. But since $1,\ell\in L$ and $1,\ell^{-1}\in L'$ are K-linearly independent, respectively, we have $\ell\otimes\ell^{-1}\neq1\otimes1$ in $L\otimes_K L'$. Thus φ is not an isomorphism. This proves that (a) implies (e).

(*Aliter:* If $L\cap L'\neq K$ compute $[LL'/K]$ using $[L\cap L'/K]>1$.)

Finally, assume that one of L/K and L'/K is galois and that $L\cap L'=K$. After exchanging L and L' if necessary, we may assume that L/K is galois. By the primitive element theorem there then exists $d\in L$ with $L=K(d)$. This implies that $LL'=L'(d)$. Let $f\in K[X]$ be the minimal polynomial of d over K. Since L/K is normal, this splits into linear factors over L. Now let $g\in L'[X]$ be the minimal polynomial of d over L'. Since $f(d)=0$, we then have $g|f$ in $L'[X]$. It follows that all zeros of g lie in L; hence we have $g\in L[X]$. Therefore $g\in(L\cap L')[X]=K[X]$. As f is already irreducible in $K[X]$, this shows that $g=f$. In particular we have

$$[LL'/L'] \;=\; [L'(d)/L'] \;=\; \deg(g) \;=\; \deg(f) \;=\; [L/K].$$

Therefore (e) implies (b) in this case, as desired.

4. Prove that any two finite field extensions $L, L'/K$ with $[L/K]$ and $[L'/K]$ coprime are linearly disjoint over K.

   Solution: After embedding L and L' into an algebraic closure of K, we may assume that they are contained in a common overfield M. Then the subfield $LL' \subset M$ always satisfies $[LL'/K] \leqslant [L/K] \cdot [L'/K]$ by the solution of Exercise 3. On the other hand, by the multiplicativity of degrees $(*)$ above both $[L/K]$ and $[L'/K]$ divide $[LL'/K]$. As these numbers are coprime by assumption, it follows that $[L/K] \cdot [L'/K]$ divides $[LL'/K]$. Thus we must have $[L/K] \cdot [L'/K] = [LL'/K]$.

5. Which of the following field extensions are linearly disjoint?

   (a) $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$

   (b) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ and $\mathbb{Q}(i\sqrt[4]{2})/\mathbb{Q}$

   (c) $\mathbb{Q}(\sqrt[5]{2})\mathbb{Q}$ and $\mathbb{Q}(e^{2\pi i/5}\sqrt[5]{2})/\mathbb{Q}$

   Solution:

   (a) As the degrees of the field extensions are 5 and 6 respectively, they are linearly disjoint by Exercise 4.

   (b) The element $\sqrt{2}$ is contained in $\mathbb{Q}(\sqrt[4]{2}) \cap \mathbb{Q}(i\sqrt[4]{2})$, hence the field extensions are not linearly disjoint over $\mathbb{Q}$ by condition (e) of Exercise 3.

   (c) Both field extension have degree 5, but together they generate the field extension

   $$\mathbb{Q}\big(\sqrt[5]{2}, e^{2\pi i/5}\sqrt[5]{2}\big) = \mathbb{Q}\big(\sqrt[5]{2}, e^{2\pi i/5}\big)$$

   with

   $$\big[\mathbb{Q}\big(\sqrt[5]{2}, e^{2\pi i/5}\big)/\mathbb{Q}\big] = \big[\mathbb{Q}(\sqrt[5]{2}, e^{2\pi i/5})/\mathbb{Q}(e^{2\pi i/5})\big] \cdot \big[\mathbb{Q}(e^{2\pi i/5})/\mathbb{Q}\big] \leqslant 5 \cdot 4$$

   By Exercise 3 the extensions are therefore not linearly disjoint.

6. (a) Consider the polynomial ring $A = k[Y, Z]$ over a field k together with the ideal $\mathfrak{a} = (Y, Z)$. Determine the A-submodules

   $$\mathfrak{a}^{-1} := \{x \in \mathrm{Quot}(A) \mid x \cdot \mathfrak{a} \subset A\}.$$

   and $\mathfrak{a}\mathfrak{a}^{-1} \subset A$.

   (b) Repeat this for $A = \mathbb{Z}[Y]$ and $\mathfrak{a} = (2, Y)$.

   Solutions:

   (a) Since $\mathfrak{a} \subset A$ is an ideal, we have $A \subset \mathfrak{a}^{-1}$. Conversely consider any element $x \in \mathfrak{a}^{-1}$. Since A is a unique factorization domain, we can write $x = b/c$ with coprime $b, c \in A$. Then $x \in \mathfrak{a}^{-1}$ implies that $xY \in A$ or again that $bY \in (c)$. Thus c divides bY within A. As b and c are coprime, this shows that $c|Y$.

The same argument with Z in place of Y shows that $c|Z$. As Y and Z are coprime, this implies $c \in A^\times$. Thus $x = b/c \in A$.

Together this shows that $\mathfrak{a}^{-1} = A$ and therefore $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}$.

(b) The same argument as in (a) shows that $\mathfrak{a}^{-1} = A$ and $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}$.

**7. Which of the properties of Dedekind rings hold for the ring $\mathcal{O}(\mathbb{C})$ of entire functions $\mathbb{C} \to \mathbb{C}$?