January 16, 2014

1 Exercises for Section 1

1.1 Let A be a ring, $A \neq 0$, and M an A-module with basis $(w_i)_{i\in I}$.

(a) Prove that there is a ring homomorphism from A to a field k, and that $\#I = \dim_k(M \otimes_A k)$.

(b) Suppose that M is a finitely generated A-module. Prove that $\#I$ is finite.

(a) Let $\mathfrak{m}$ be a maximal ideal of A. Then $k := A/\mathfrak{m}$ is a field, and the canonical map $A \longrightarrow k$ is a ring homomorphism, which gives rise to an A-action on k.

Note that $M = \bigoplus_{i\in I} Aw_i$. Define a map

$$f : M \times k \longrightarrow k^{\oplus I}$$

by setting

$$f\left(\sum_{\text{finite}} a_i w_i\,,\, x\right) = \sum_{\text{finite}} (a_i x)e_i,$$

where $(e_i)_{i\in I}$ is a basis for $k^{\oplus I}$. It is clear that f is A-bilinear. Hence f induces an A-homomorphism

$$\tilde{f} : M \otimes_A k \longrightarrow k^{\oplus I}.$$

Indeed, $\tilde{f}$ is k-linear as $f(m,\cdot)$ is a k-linear map for each $m \in M$. Now consider the k-linear map

$$g : k^{\oplus I} \longrightarrow M \otimes_A k$$

given by

$$g\left(\sum_{\text{finite}} x_i e_i\right) = \sum_{\text{finite}} e_i \otimes x_i.$$

It is easy to check that g is the inverse of $\tilde{f}$, which implies $\tilde{f}$ is a k-isomorphism. Therefore,

$$\dim_k(M \otimes_A k) = \dim_k(k^{\oplus I}) = \#I.$$

(b) Suppose $(u_n)_{n=1}^N$ is a set of A-generators of M. Since $(w_i)_{i\in I}$ is an A-basis of M, each u_n can be uniquely represented as

$$u_n = \sum_{r=1}^{l_n} \alpha_{nr} w_{nr}$$

with $\alpha_{nr} \in A - \{0\}$, $w_{nr} \in (w_i)_{i\in I}$. Let W be the collection of all such w_n^r. Then W is finite and forms a basis of M, and $M \otimes_A k$ is of dimension $\#W$. But the dimension is also equal to $\#I$. So $\#I$ coincides with $\#W$ and is thereby a finite number.

1.2 (a) Let $w_1, w_2, \cdots, w_n$ be a basis for M over A, and let

$$v_i = \sum_{j=1}^{n} a_{ij} w_j \in M \quad (1 \leq i \leq n)$$

with $a_{ij} \in A$. Prove: $v_1, v_2, \cdots, v_n$ is a basis for M over $A \Leftrightarrow \det((a_{ij})_{1 \leq i,j \leq n}) \in A^*$.

(b) The trace $\mathrm{Tr}(C)$ of an $n \times n$-matrix $C = (c_{ij})_{1 \leq i,j \leq n}$ over A is defined by $\mathrm{Tr}(C) = \sum_{i=1}^{n} c_{ii}$. Prove

$$\begin{aligned} \mathrm{Tr}(CD) &= \mathrm{Tr}(DC), \\ \mathrm{Tr}(ECE^{-1}) &= \mathrm{Tr}(C) \end{aligned}$$

for $n \times n$-matrices C, D, E over A with $\det(E) \in A^*$.

(c) Prove that the trace of an A-endomorphism of a finitely generated free module, as defined in 1.1, is independent of the choice of the basis.

(a) If $(v_i)_{i=1}^{n}$ is an A-basis for, then each w_j can be expressed as

$$w_j = \sum_{i=1}^{n} b_{ji} v_i$$

for some unique $b_{ji} \in A$. Together with the assumption that $v_i = \sum_j a_{ij} w_j$, we have

$$v_r = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{rj} b_{ji} v_i, \quad r = 1, \cdots, n.$$

Since each v_r is a basis element, by comparing the coefficients, we get

$$\sum_{j=1}^{n} a_{rj} b_{ji} = \delta_{ir}.$$

In other words, the product $[a_{ij}][b_{ij}] = \mathrm{id}_n$, and so

$$\det[a_{ij}] \cdot \det[b_{ij}] = 1.$$

This proves $\det[a_{ij}]$ is a unit of A.

Conversely, assume $\det[a_{ij}] \in A^{\times}$. Consider the equation

$$\sum_{i=1}^{n} \lambda_i v_i = 0.$$

Expressing v_i in terms of the basis $(w_j)_{j=1}^{n}$ the equation can be rewritten as

$$\sum_{j=1}^{n} \sum_{i=1}^{n} \lambda_i a_{ij} w_j = 0,$$

which yields

$$\sum_{i=1}^{n} \lambda_i a_{ij} = 0, \quad j = 1, \cdots, n.$$

These equations can be written in the matrix form

$$[\lambda_1 \quad \cdots \quad \lambda_n][a_{ij}] = [0 \quad \cdots \quad 0].$$

Hence it suffices to verify the invertibility of the matrix $[a_{ij}]$. Recall that for any $n \times n$-matrix X, we have the matrix identity

$$X \operatorname{adj}(X) = \det(X) \operatorname{id}_n,$$

in which $\operatorname{adj}(X) := [(-1)^{i+j} \det(X_{ij})]^T$ is the adjugate matrix of X, where X_{ij} is the matrix obtained from deleting the i-th row and the j-th column of X. Now $\det[a_{ij}]$ is a unit in A, by the above matrix identity, $\frac{1}{\det[a_{ij}]}\operatorname{adj}[a_{ij}]$ is an inverse of $[a_{ij}]$. This means $[a_{ij}]$ is invertible and we are done.

(b) Write $C = [c_{ij}]$ and $D = [d_{ij}]$. Then

$$CD = \left[\sum_{r=1}^{n} c_{ir} d_{rj}\right] \quad \text{and} \quad DC = \left[\sum_{r=1}^{n} d_{ir} c_{rj}\right].$$

The first identity holds since

$$\operatorname{Tr}(CD) = \sum_{i=1}^{n} \left(\sum_{r=1}^{n} c_{ir} d_{ri}\right) = \sum_{r=1}^{n} \left(\sum_{i=1}^{n} d_{ri} c_{ir}\right) = \operatorname{Tr}(DC).$$

Replacing the pair (C, D) by (EC, E^{-1}) for any invertible matrix E in the first identity, we get the second one.

(c) Let M be a finitely generated free A-module with basis $(w_i)_{i=1}^n$, and $f : M \longrightarrow M$ an A-linear map. Suppose that

$$f(w_i) = \sum_{j=1}^{n} \mu_{ij} w_l, \quad i = 1, \cdots, n.$$

By definition, the trace of f with respect to the basis $(w_i)_{i=1}^n$ is

$$\operatorname{Tr}_{(w_i)}(f) = \sum_{i=1}^{n} \mu_{ii}.$$

Assume that M has another basis $(v_i)_{i=1}^n$, and that for each i,

$$v_i = \sum_{j=1}^{n} a_{ij} w_j \quad \text{and} \quad w_i = \sum_{j=1}^{n} b_{ij} v_j,$$

where $[a_{ij}]$ and $[b_{ij}]$ are mutually inverse, as was shown in part (a). Then,

$$\begin{aligned} f(v_i) &= \sum_{j=1}^{n} a_{ij} f(w_j) = \sum_{j=1}^{n} a_{ij} \sum_{k=1}^{n} \mu_{jk} w_k = \sum_{j=1}^{n} a_{ij} \sum_{k=1}^{n} \mu_{jk} \sum_{l=1}^{n} b_{kl} v_l \\ &= \sum_{l=1}^{n} \left(\sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij} \mu_{jk} b_{kl} \right) v_l. \end{aligned}$$

So the trace of f with respect to the basis $(v_i)_{i=1}^{n}$ is

$$\begin{aligned} \mathrm{Tr}_{(v_i)}(f) &= \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij} \mu_{jk} b_{ki} = \sum_{j=1}^{n} \sum_{k=1}^{n} \left(\sum_{i=1}^{n} b_{ki} a_{ij} \right) \mu_{jk} \\ &= \sum_{j=1}^{n} \sum_{k=1}^{n} \delta_{kj} \mu_{jk} = \sum_{j=1}^{n} \mu_{jj} \\ &= \mathrm{Tr}_{(w_i)}(f). \end{aligned}$$

This proves the trace map is invariant under a change of basis.

1.3 Let B be an A-algebra that is finitely generated and free as an A-module, with basis $w_1, w_2, \cdots w_n$. Prove: B is separable over $A \Leftrightarrow \det(\mathrm{Tr}(w_i w_j)_{1 \le i,j \le n}) \in A^*$.

By definition, B is separable over A if and only if the A-linear map

$$\phi : B \longrightarrow \mathrm{Hom}_A(B, A),$$

given by $\phi(b)(\tilde{b}) = \mathrm{Tr}(b\tilde{b})$ for $b, \tilde{b} \in B$, is a bijection.

Let $(w_i)_{i=1}^{n}$ be a basis for B over A. Then the A-module $\mathrm{Hom}_A(B, A)$ has a corresponding basis $(\chi_i)_{i=1}^{n}$, where $\chi_i : B \longrightarrow A$ is the A-linear map so that $\chi_i(w_j) = \delta_{ij}$. Write

$$\phi(w_i) = \sum_{j=1}^{n} a_{ij} \chi_j, \quad i = 1, \cdots, n.$$

In actuality, the a_{ij} above can be expressed explicitly as

$$a_{ij} = \sum_{l=1}^{n} a_{il} \chi_l(w_j) = \phi(w_i)(w_j) = \mathrm{Tr}(w_i w_j).$$

Note that ϕ is bijective if and only if $\phi(w_1), \cdots, \phi(w_n)$ form a basis for $\mathrm{Hom}_A(B, A)$; and this is the case if and only if, by Exercise 2, the determinant $\det[\mathrm{Tr}(w_i w_j)]$ is a unit of A.

1.4 Let B be a free separable A-algebra, A' an A-algebra, and $B' = B \otimes_A A'$. Prove that B' is a free separable A'-algebra.

We will adopt the notations used in and apply the result of the previous exercise. Since the A-algebra B is free separable, $B = \bigoplus_{i=1}^n Aw_i$ as an A-module, and $\det[\mathrm{Tr}(w_i w_j)]$ is a unit in A.

To show $B' = B \otimes_A A'$ is free separable A'-algebra, first we check that B' is finitely generated and free as an A'-module. In fact, this is true since tensor products commute with direct sums:

$$B' = B \otimes_A A' = \left(\bigoplus_{i=1}^n Aw_i \right) \otimes_A A' \simeq \bigoplus_{i=1}^n (Aw_i \otimes_A A') \simeq \bigoplus_{i=1}^n A'(w_i \otimes 1).$$

This identification (about the A'-module structure) also implies that the collection $(w_i \otimes 1)_{i=1}^n$ forms an A'-basis for B'. Hence it remains to verify

$$\det[\mathrm{Tr}'(w_i \otimes 1)(w_j \otimes 1)] \in (A')^\times,$$

where Tr' stands for the trace map on $\mathrm{Hom}_{A'}(B', B')$, as well as the induced map on B'. Note that $(w_i \otimes 1)(w_j \otimes 1) = w_j w_j \otimes 1$, so what we need to be aware of is $\mathrm{Tr}'(w_i w_j \otimes 1)$. More precisely, we have to understand Tr'.

Consider the A'-module $\mathrm{Hom}_{A'}(B \otimes_A A', A \otimes_A A')$, in which we write the original A' as $A \otimes_A A'$, regarded as A'-algebra, for clarity in latter discussion. It has a natural A'-basis $(\chi_i')_{i=1}^n$, where χ_i' is the A'-linear map determined by $\chi_i'(w_j \otimes 1) = \delta_{ij}(1 \otimes 1) = \delta_{ij} \otimes 1$. Also, $\chi_i(w_j) \otimes 1 = \delta_{ij} \otimes 1$. So for any $a_j' \in A'$, $j = 1, \cdots, n$, by the linearity of χ_i', we have

$$\begin{aligned} \chi_i' \left(\sum_{j=1}^n w_j \otimes a_j' \right) &= \sum_{j=1}^n a_j' \chi_i'(w_j \otimes 1) = \sum_{j=1}^n a_j' (\chi_i(w_j) \otimes 1) \\ &= \sum_{j=1}^n \chi_i(w_j) \otimes a_j' = \chi_i \left(\sum_{j=1}^n w_j \right) \otimes a_j'; \end{aligned}$$

that is,

$$\chi_i' = \chi_i \otimes \mathrm{id}_{A'}.$$

By the definition of trace, we have $\mathrm{Tr}'(\chi_i') = 1 \otimes 1$. Together with $\mathrm{Tr}(\chi_i) = 1$, we get

$$\mathrm{Tr}'(\chi_i') = \mathrm{Tr}(\chi_i \otimes \mathrm{id}_{A'}) = \mathrm{Tr}(\chi_i) \otimes 1$$

Now, suppose that $m_{w_i w_j} = \sum_{l=1}^n a_l \chi_l$ with $a_l \in A$. Then

$$m_{w_i w_j \otimes 1} = m_{w_i w_j} \otimes \mathrm{id}_{A'} = \sum_{l=1}^n a_l \chi_l \otimes \mathrm{id}_A'.$$

Therefore,

$$\begin{aligned} \mathrm{Tr}'(w_i w_j \otimes 1) &= \mathrm{Tr}' \left(\sum_{l=1}^n a_l \chi_l \otimes \mathrm{id}_{A'} \right) \\ &= \sum_{l=1}^n a_l \mathrm{Tr}(\chi_l) \otimes 1 = \sum_{l=1}^n a_l \otimes 1 \\ &= \mathrm{Tr}(w_i w_j) \otimes 1. \end{aligned}$$

Finally, by the definition of determinant, we have

$$\det[\mathrm{Tr}'(w_i w_j \otimes 1)] = \det[\mathrm{Tr}(w_i w_j) \otimes 1] = \det[\mathrm{Tr}(w_i w_j)] \otimes 1.$$

Since $\det[\mathrm{Tr}(w_i w_j)]$ is a unit in A, we know $\det[\mathrm{Tr}(w_i w_j)] \otimes 1$ is a unit in $A \otimes_A A' = A'$ and we are done.

1.5 Let K be an algebraic number field with discriminant Δ and ring of integers A. Prove that $A[1/\Delta]$ is a free separable $\mathbb{Z}[1/\Delta]$-algebra.

Let $A' = A[1/\Delta]$ and $Z' = \mathbb{Z}[1/\Delta]$. Take an integral basis $\omega_1, \cdots, \omega_n$ of K, i.e. it is a free $\mathbb{Z}$ basis of A. Note that $\omega_1, \cdots, \omega_n$ is also a basis of K over $\mathbb{Q}$. By the definition of the discriminant of K,

$$\Delta = \mathrm{det(Tr_{K/\mathbb{Q}}(\omega_i\omega_j))}.$$

Notice that $\mathrm{Tr_{K/\mathbb{Q}}(\omega_i\omega_j)} = \mathrm{Tr_{A'/Z'}(\omega_i\omega_j)}$. Using exercise 1.3 and Δ is invertible in Z', A' is a free separable Z'-algebra.

1.6 Let A be a ring.

(a) Let $a \in A$. Prove that $A[X]/(X^2 - a)$ is a free separable A-algebra if and only if $2a \in A^*$.

(b) Let, more generally, $f \in A[X]$ be a monic polynomial. Prove that $A[X]/(f)$ is a free separable A-algebra if and only if the discriminant $\Delta(f)$ of f belongs to A^*.

(a) Let $B = A[X]/(X^2 - a)$ and $[b] = b + (X^2 - a)$. It is easy to check that $\{[1], [x]\}$ is a A-basis of B and thus $\mathrm{rank}_A(B) = 2$. By the definition of $m_{[x]}$, we have $m_{[x]}([1]) = [x]$ and $m_{[x]}([x]) = [x]^2 = [a]$. Then $\mathrm{Tr}([x]) = \mathrm{Tr}(m_{[x]}) = 0$. Clearly, $\mathrm{Tr}([a]) = \mathrm{rank}_A(B) \cdot a = 2a$. Using Exercise 1.3, B is a free separable A-algebra if and only if

$$4a = \det \begin{pmatrix} \mathrm{Tr}([1]) & \mathrm{Tr}([x]) \\ \mathrm{Tr}([x]) & \mathrm{Tr}([x]^2) \end{pmatrix} \in A^*.$$

(b) Let $B = A[X]/(f)$, $[b] = b + (f)$ and $n = \deg(f)$. It is easy to check that $\{[1], [x], \cdots, [x]^{n-1}\}$ is a A-basis of B and thus $\mathrm{rank}_A(B) = n$. Write

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

A element t_m in A ($m \in \mathbb{Z}_{\geqslant 0}$) is defined by using a recursive relations

$$t_m + a_{n-1}t_{m-1} + \cdots + a_{n+m+1}t_1 + m a_{n-m} = 0$$

for $1 \leqslant m \leqslant n$,

$$t_m + a_{n-1}t_{m-1} + \cdots + a_0 t_{m-n} = 0$$

for $m > n$ and set $t_0 = n$. (Note that this is Newton identities. Originally it give relations between power sums and elementary symmetric polynomials.) Also, we define the discriminant $\Delta(f)$ by

$$\Delta(f) = \det \begin{pmatrix} t_0 & t_1 & \cdots & t_{n-1} \\ t_1 & t_2 & \cdots & t_n \\ \vdots & \vdots & \ddots & \vdots \\ t_{n-1} & t_n & \cdots & t_{2n-2} \end{pmatrix} \in A.$$

By an induction on m, the definition of $\mathrm{Tr}_{B/A}(m_{[x]^m})$ and the recursive relations between t_i and a_i, we get $\mathrm{Tr}(m_{[x]^m}) = t_m$ for all $m \geqslant 0$. Using Exercise 1.3, B is a free separable A-algebra if and only if

$$\Delta(f) = \det \begin{pmatrix} \mathrm{Tr}([1]) & \mathrm{Tr}([x]) & \cdots & \mathrm{Tr}([x]^{n-1}) \\ \mathrm{Tr}([x]) & \mathrm{Tr}([x]^2) & \cdots & \mathrm{Tr}([x]^n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}([x]^{n-1}) & \mathrm{Tr}([x]^n) & \cdots & \mathrm{Tr}([x]^{2n-2}) \end{pmatrix} \in A^*.$$

1.7 Suppose that the scheme X is the disjoint union of two schemes X', X''. Prove that the category $\mathbf{FEt}_X$ is equivalent to a suitably defined "product category" $\mathbf{FEt}_{X'} \times \mathbf{FEt}_{X''}$.

Let $\phi : Z \to X = X' \amalg X''$ be a finite étale covering. Consider $Z' = \phi^{-1}(X')$ and $Z'' = \phi^{-1}(X'')$. Then, $Z' \to X'$ and $Z'' \to X''$ are flat and unramified because these are local properties. And they are finitely presented if we consider affine coverings of X' and X'' induced from the affine covering of X. Thus, by 6.9, they are finite étale coverings. Conversely, given finite étale coverings $\phi_1 : Z' \to X'$ and $\phi_2 : Z'' \to X''$, we consider $Z = Z' \amalg Z'' \to X$. It is finite étale due to the similar reason as above. Consider $F : \mathbf{FET}_{X'} \times \mathbf{FET}_{X''} \to \mathbf{FET}_X$ is the functor sends objects as discussion. It sends morphisms in the natural way. It remains to show F is fully faithful. Its induced map on morphisms is injective clearly. Since

$$\begin{tikzcd} Z_1 \amalg Z_2 \arrow[rr] \arrow[dr] & & W_1 \amalg W_2 \arrow[dl] \\ & X_1 \amalg X_2 & \end{tikzcd}$$

is commutative, surjectivity is assured.

1.8 Let $S = \varprojlim S_i$ be a projective limit as in 1.7, and define for each $j \in I$ the projection map $f_j : S \longrightarrow S_j$ by $f_j((x_i)_{i \in I}) = x_j$. Prove that the system $(S, (f_j)_{j \in I})$ has the following "universal property":

(i) $f_{ij} \circ f_i = f_j$ for all $i, j \in I$ with $i \geq j$;

(ii) if T is a set and $(g_j : T \longrightarrow S_j)_{j \in I}$ is a collection of maps satisfying $f_{ij} \circ g_i = g_j$ (for all $i, j \in I$ with $i \geq j$), then there is a unique map $g : T \longrightarrow S$ such that $g_j = f_j \circ g$ for all $j \in I$.

Prove further that this universal property characterizes $(S, (f_j)_{j\in I})$ in the following sense: if S' is a set and $(f'_j : S' \longrightarrow S_j)_{j\in I}$ a collection of maps satisfying the analogues of (i), (ii), then there is a unique bijection $f' : S' \longrightarrow S$ such that $f'_j = f_j \circ f'$ for all $j \in I$.

Recall that the projective limit

$$S = \left\{ (x_k)_{k\in I} \in \prod_{k\in I} S_k : f_{ij}(x_i) = x_j \text{ for all } i, j \in I \text{ with } i \geq j \right\}.$$

For any $(x_k)_{k\in I} \in S$ and any $i, j \in I$ with $i \geq j$, we have

$$f_{ij} \circ f_i((x_k)_{k\in I}) = f_{ij}(x_i) = x_j = f_j((x_k)_{k\in I}).$$

This proves (i). Let $(g_j : T \longrightarrow S_j)_{j\in I}$ be a collection of maps with the property $f_{ij} \circ g_i = g_j$ for all $i, j \in I$ with $i \geq j$. If there is a map $g : T \longrightarrow S$ such that $g_j(t) = f_j(g(t))$ for all $t \in T$ and $j \in I$, then we will have

$$g(t) = (g_j(t))_{j\in I},$$

in which $(g_j(t))_{j\in I}$ indeed belongs to S because of the the property of $(g_j)_{j\in I}$. Now define the map $g : T \longrightarrow S$ by the above formula. Then we obtain both the existence and uniqueness of g that satisfies the required equations.

The second part that the universal property characterizes projective limits is just a consequence of the standard formal argument.

1.9 Let the notations be as in 1.7, and $S = \varprojlim S_i$

(a) Suppose that all sets S_i are endowed with a compact Hausdorff topology, that all S_i are non-empty, and that all maps f_{ij} are continuous. Prove that S is non-empty and compact. [*Hint:* Apply Tikhonovs theorem.]

(b) Suppose that all sets S_i are *finite* and *non-empty*. Prove that $S \neq \emptyset$.

(c) Suppose that I is countable, that all S_i are non-empty, and that all f_{ij} are surjective. Prove that $S \neq \emptyset$.

(d) Let I be the collection of all finite subsets of $\mathbb{R}$, and let I be partially ordered by inclusion. For each $i \in I$, let S_i be the set of *injection* maps $\phi : i \to \mathbb{Z}$, and let $f_{ij} : S_i \to S_j$ (for $j \subset i$) map ϕ to its restriction $\phi|j$. Prove that this defines a projective system in which all S_i are non-empty and that all f_{ij} are surjective, but that the projective limit S is empty.

(a) Define $S_{ij} := \{(s_i)_{i\in I} \in \prod_{i\in I} S_i \,|\, f_{ij}(s_i) = s_j\}$. We have $S = \cap_{i\geq j} S_{ij}$. Since each S_{ij} is closed in $\prod_{i\in I} S_i$, by Tikhonov's theorem, $\prod_{i\in I} S_i$ is compact, and hence S_{ij} is compact.

For all $\bar{I} = \{i_1, ..., i_n\}$ and $\bar{J} = \{j_1, ..., j_m\}$, by I is a projective system, there is an $i_0 \in I$ such that $S_{i_0} \to S_i$ via $f_{i_0,i}$ and $S_{i_0} \to S_j$ via $f_{i_0,j}$, respectively. Hence $\cap_{i\in\bar{I}, j\in\bar{J}} S_{ij} \neq \emptyset$. So $S = \cap_{i,j} S_{ij} \neq \emptyset$ by the finite intersection property. (Recall: X is compact Hausdorff space and $\{F_i\}$ a family of closed subsets in X. If for all finite indes set $J \subset I$, we have $X \cap (\cap_{i\in J} F_i) \neq \emptyset$, then $X \cap (\cap_{i\in I} F_i) \neq \emptyset$.) So $S \subset \prod_{i\in I} S_i$ is closed, hence compact.

(b) Given discrete topology on each S_i; then apply (a).

(c) ...

(d)

$$I := \{ \ i \text{ is a finite subset in } \mathbb{R} \ \}, \ i \geq j \Leftrightarrow i \supseteq j$$
$$S_i := \{\phi : i \hookrightarrow \mathbb{Z}\}$$

$$\begin{array}{rcl} f_{ij} : S_i & \to & S_j \\ \phi & \mapsto & \phi|_j \end{array}$$

(i) For each $i, j \in I$, set $k := i \cup j$. Then $k \geq i, j$

(ii) $f_{ii} = \text{id}$ is clear.

(iii) $f_{ik} = f_{jk} f_{ij}$ is the compose of restriction map. Hence $(i \in I, S_i)$ is a projective system. $S \neq \emptyset$ is clear and f_{ij} is surjective since we can freely extend all $\psi : j \to \mathbb{Z}$ to $\psi_{ext} : i \to \mathbb{Z}$ if $i \supset j$.

To prove $\varprojlim S_i$ is empty, suppose $(\phi_i)_{i\in I}$ is an element in $\varprojlim S_i$. By definition, $\phi_i : i \to \mathbb{Z}$ such that $\phi_i|_j = \phi_j$ for $j \subset i$. In particular, all ϕ_i have the same restriction on all singleton $\{x\} \subset \mathbb{R}$. This says we have an injection $\mathbb{R} \hookrightarrow \mathbb{Z}$, a contradiction.

1.10 Prove: if π_j is a profinite group for each j in a set J, then $\prod_{j\in J} \pi_j$ is a profinite group.

1.13 Let p be a prime number, and $\mathbb{Z}_p$ the ring of p-adic integers. Prove:

(a) $\mathbb{Z}_p^* = \mathbb{Z}_p - p\mathbb{Z}_p$;

(b) each $a \in \mathbb{Z}_p - \{0\}$ can be uniquely written in the form $a = up^n$ with $u \in \mathbb{Z}_p^*$, $n \in \mathbb{Z}, n \geq 0$;

(c) $\mathbb{Z}_p$ is a local domain with residue class field $\mathbb{F}_p$.

First, we prove that, for each $n \geqslant 1$, there is an exact sequence of abelian groups

$$0 \to \mathbb{Z}_p \xrightarrow{\cdot p^n} \mathbb{Z}_p \xrightarrow{\pi_n} \mathbb{Z}/p^n\mathbb{Z} \to 0,$$

where π_n sends $((a_m))$ to a_n.

Clearly, π_n is surjective. If $a = (a_m)$ belongs to $\ker(\pi_n)$, then $a_m \equiv 0 \pmod{p^n}$ for all $m \geqslant n$. This means that, under the isomorphism $\mathbb{Z}/p^{m-n}\mathbb{Z} \to p^n\mathbb{Z}/p^m\mathbb{Z}$, there is a element b_{m-n} of $\mathbb{Z}/p^{m-n}\mathbb{Z}$ such its image in $\mathbb{Z}/p^m\mathbb{Z}$ satisfies $a_m = p^n b_{m-n}$. The b_l define an element b of $\mathbb{Z}_p$ such that $p^n b = a$. Obversely, the kernel of π_n contains $p^n\mathbb{Z}_p$ and thus the above sequence is exact at the middle term. Similarly, the multiplicative map $\cdot p^n$ is injective.

(a) By the above exact sequence for $n = 1$, we know that $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to the field $\mathbb{F}_p$. This implies that $\mathbb{Z}_p^* \subseteq \mathbb{Z}_p \setminus p\mathbb{Z}_p$. On the other hand, if $a \in \mathbb{Z}/p^n\mathbb{Z}$ which is not divided by p, then its image in $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is nonzero thus invertible. Hence there are $b, c \in \mathbb{Z}/p^n\mathbb{Z}$ such that $ab = 1 - pc$. Then

$$ab(1-pc)^{-1} = ab(1 + pc + \cdots + p^{n-1}c^{n-1}) = 1$$

in $\mathbb{Z}/p^n\mathbb{Z}$ which proves $a \in (\mathbb{Z}/p^n\mathbb{Z})^*$. In general, for $a = (a_n) \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, we have $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ which is not divided by p and thus a_n has the inverse in $\mathbb{Z}/p^n\mathbb{Z}$. By the uniqueness of inverse elements, we get $(a_n^{-1}) \in \mathbb{Z}_p$ and hence $a \in \mathbb{Z}_p^*$.

(b) For each nonzero $a = (a_n) \in \mathbb{Z}_p$, there is the largest n such that $a_i = 0$ for all $1 \leqslant i \leqslant n$. Since $\pi_n(a) = 0$, we have $a = p^n u$. By the choice of n, $u \notin p\mathbb{Z}_p$ i.e. $u \in \mathbb{Z}_p^*$. The uniqueness of the decomposition is obvious.

(c) Use (b), we can define the p-adic valuation for $\mathbb{Z}_p$:

$$v_p(a) = \begin{cases} +\infty & \text{if } a = 0, \\ n & \text{if } a = p^n u, u \in \mathbb{Z}_p^*. \end{cases}$$

Then $\mathbb{Z}_p$ is a discrete valuation ring, i.e.

$$v_p(ab) = v_p(a) + v_p(b),\ v_p(a+b) \geqslant \min\{v_p(a), v_p(b)\}$$

and $v_p(a) = +\infty$ if and only if $a = 0$. Hence $\mathbb{Z}_p$ is a local domain with the maximal ideal $\{a \in \mathbb{Z}_p \,|\, v_p(a) \geqslant 1\} = p\mathbb{Z}_p$.

1.14 Prove that there is an isomorphism $\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p$ of topological rings (definition obvious).

Recall that $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ for any prime p. For any positive integer m, which admit the prime factorization $p_1^{n_1} \cdots p_k^{n_k}$, the Chinese remainder theorem gives

$$\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}.$$

Through this isomorphism we have a natural map $\prod_{p \text{ prime}} \mathbb{Z}_p \longrightarrow \mathbb{Z}/m\mathbb{Z}$ for every $m \in \mathbb{N}$, which induces a unique homomorphism of topological rings

$$f : \prod_{p \text{ prime}} \mathbb{Z}_p \longrightarrow \hat{\mathbb{Z}}$$

such that the natural maps mentioned above are factorized over f. On the other hand, for each prime number p the collection of canonical maps $(\hat{\mathbb{Z}} \longrightarrow \mathbb{Z}/p^n\mathbb{Z})_{n \in \mathbb{N}}$ induces a unique homomorphism

$$\hat{\mathbb{Z}} \longrightarrow \mathbb{Z}_p$$

over which the canonical maps just mentioned are factorized. This gives rise to the homomorphism

$$g : \hat{\mathbb{Z}} \longrightarrow \prod_{p \text{ prime}} \mathbb{Z}_p.$$

Note for any $m \in \mathbb{N}$ that the natural map $\hat{\mathbb{Z}} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ is factorized over g with the help of the isomorphism at the beginning. An argument concerning the uniqueness of f and g subject to their characterizing properties shows that both $f \circ g$ and $g \circ f$ are identities. Thus f and g are isomorphisms.

1.15 Let $\mathbb{Z}_{10} = \varprojlim_{n\geq 1} \mathbb{Z}/10^n\mathbb{Z}$.

(a) Prove that each $a \in \mathbb{Z}_{10}$ has a unique representation $a = \sum_{n=0}^{\infty} c_n 10^n$ with $c_n \in \{0, \cdots, 9\}$.

(b) Prove that there exits a unique continuous function $v : \mathbb{Z}_{10} \to \mathbb{R}$ such that $v(a) = (\text{number of factors 2 in } a)^{-1}$ for each positive integer a.

(c) Let $(a_n)_{n=0}^{\infty}$ be a sequence of positive integers not divisible by 10 such that the number of factors 2 in a_n tends to infinity for $n \to \infty$. Prove that the sum of the digits of a_n in the decimal system tends to infinity for $n \to \infty$.

For any $a \in \mathbb{Z}_{10}$, we may write $a = (b_n)_{n=1}^{\infty}$ in the product coordinates. Let $\sum_{m=0}^{n-1} c_m^n 10^m$ be the decimal expansion of b_n. Note that c_m^n stable as $n \to \infty$. Let c_m be the stable value. Then the representation $\sum_{m=0}^{\infty} c_m 10^m$ is what we are looking for and it is unique.

For the statement (b), the image of $\mathbb{Z}_{>0}$ in $\mathbb{Z}_{10}$ is dense. (The proof is similar to 1.12) The behavior of a continuous function is totally determined by its value on a dense subset. So (b) follows.

For (c). Suppose there exists such a sequence $\{a_n\}_{n=1}^{\infty}$ such that the conditions hold but the sum of digits of a_n does not go to infinity. Let $s(a_n)$ denote the sum of digits of a_n. Then by assumption, $\limsup_{n\to\infty} s(a_n) = M < \infty$.

Take a sequence $\{a_n\}_{n=1}^{\infty}$ so that $\limsup_{n\to\infty} s(a_n)$ is minimum. Firstly, observe that $a_n \to \infty$. Let b_n be the number obtained by removing the first digits from a_n. Then b_n also satisfying the condition since $a_n - b_n = k_n \cdot 10^{r(n)}$. So the number b_n must divisible by 2 sufficiently. And the number b_n is non-zero. But $\limsup_{n\to\infty} s(b_n) \leq \limsup_{n\to\infty} s(a_n) - 1$.

Therefore, such sequence $\{a_n\}_{n=1}^{\infty}$ does not exist.

1.16 (a) Prove that each $a \in \hat{\mathbb{Z}}$ has a unique representation $a = \sum_{n=1}^{\infty} c_n n!$ with $c_n \in \{0, 1, \ldots, n\}$.

(b) Let $b \in \mathbb{Z}, b \geq 0$, and define the sequence $(a_n)_{n=0}^{\infty}$ of non-negative integers by $a_0 = b, a_{n+1} = 2^{a_n}$. Prove that $(a_n)_{n=0}^{\infty}$ converges in $\hat{\mathbb{Z}}$, and that $\lim\limits_{n\to\infty} a_n \in \hat{\mathbb{Z}}$ is independent of b.

(c) Let $a = \lim\limits_{n\to\infty} a_n$ as in (b), and write $a = \sum_{n=1}^{\infty} c_n n!$ as in (a). Compute c_n for $1 \leq n \leq 10$.

Throughout the proof we adopt the fact in Problem 1.17(c) that

$$\hat{\mathbb{Z}} \simeq \varprojlim_{m>0} \mathbb{Z}/m!\mathbb{Z}.$$

(a) Let S be the collection of formal series $\sum_{n=1}^{\infty} c_n n!$ with $0 \leq c_n \leq n$. We will show that there is a bijection between $\hat{\mathbb{Z}}$ and S. Define for each m a map $S \longrightarrow \mathbb{Z}/m!\mathbb{Z}$ that sends $\sum_{n=1}^{\infty} c_n n!$ to $\sum_{n=1}^{m-1} c_n n! \pmod{m!}$. Indeed, these maps form a projective system; and we have $0 \leq \sum_{n=1}^{m-1} c_n n! < m!$ due to the constraint on c_n. Now we prove the induced map $\phi : S \longrightarrow \hat{\mathbb{Z}}$ is bijective by constructing its inverse. Observing that

$$c_m = \frac{1}{m!}\left(\sum_{n=1}^{m} c_n n! - \sum_{n=1}^{m-1} c_n n!\right),$$

we define a map $\psi : \hat{\mathbb{Z}} \longrightarrow S$ sending each $(b_m \pmod{m!})_{m>0}$, where $0 \leq b_m < m!$, to the formal series $\sum_{n=1}^{\infty}(\frac{1}{n!}(b_{n+1} - b_n))n!$. It is well-defined since $b_{n+1} \equiv b_n \pmod{n!}$, i.e. $b_{n+1} - b_n \in n!\mathbb{Z}$, according to the property of projective limits; and because of the bounds of b_{n+1} and b_n, we know $\frac{1}{n!}(b_{n+1} - b_n) \in \{0, 1, \cdots, n\}$. Clearly, ϕ and ψ are mutually inverse and we are done.

(b) It suffices to show that for each $N \in \mathbb{N}$, $(a_n \pmod{N})_{n \geq N}$ is stable and independent of b. We prove this by an induction argument on N. The statement is trivial for $N = 1$. For an $N > 1$, we suppose the statement holds up to $N - 1$. Now consider $a_n \pmod{N}$. Write $N = 2^k N'$ with N' odd. By Chinese remainder theorem, it is sufficient to verify that $(a_n \pmod{2^k})_{n \geq N}$ and $(a_n \pmod{N'})_{n \geq N}$ stabilize and does not depends on b. In fact, when $n \geq N > k$, we have $a_n \equiv 0 \pmod{2^k}$; also, we have $n - 1 \geq N - 1 \geq \varphi(N) \geq \varphi(N')$, where φ is the Euler function, implying that $(a_{n-1} \pmod{\varphi(N')})_{n \geq N}$ is stable and independent of b due to the induction hypothesis. It follows by Euler's theorem that $(a_n \pmod{N'})_{n \geq N}$ is stable and independent of b.

(c) According to the correspondence ψ constructed in (a), we first compute $a \pmod{n!}$ for $n = 1, \cdots, 11$. Other than Chinese remainder theorem and the fact that $a = 2^a$, in the calculation we will also need the congruence

$$2^{p^r(p-1)} \equiv 1 \pmod{p^{r+1}},$$

where p is a prime and r is a nonnegative integer. We prove this by induction on r. If $r = 0$, then it is just the Euler's theorem. Assume the congruence is true up to $r - 1$ for some r and a fixed prime p. Then we have $2^{p^{r-1}(p-1)} = 1 + \alpha p^r$ for some integer α. Hence

$$\begin{aligned} 2^{p^r(p-1)} &= (1 + \alpha p^r)^p \\ &= 1 + \binom{p}{1}\alpha p^r + \binom{p}{2}\alpha^2 p^{2r} + \cdots + \binom{p}{p}\alpha^p p^{rp} \\ &\equiv 1 \pmod{p^{r+1}}. \end{aligned}$$

Thus the congruence holds for every nonnegative r. Now we turn to the calculation:

- $a \equiv 0 \pmod{1!}$; $a \equiv 0 \pmod{2!}$.

- $a \equiv 4 \pmod{3!}$, where $3! = 2 \times 3$.

  Since $2^2 \equiv 1 \pmod 3$, we have $a \equiv 2^{a \bmod 2} \equiv 1 \pmod 3$. Together with the fact that $a \equiv 0 \pmod 2$, the result follows.

- $a \equiv 16 \pmod{4!}$, where $4! = 2^3 \times 3$.

  This follows from $a \equiv 0 \pmod{2^3}$ and $a \equiv 1 \pmod 3$.

- $a \equiv 16 \pmod{5!}$, where $5! = 2^3 \times 3 \times 5$.

  Since $2^4 \equiv 1 \pmod 5$, we have $a \equiv 2^{a \bmod 4} \equiv 1 \pmod 5$. Then combining with $a \equiv 16 \pmod{4!}$ we get the result.

- $a \equiv 16 \pmod{6!}$, where $6! = 2^4 \times 3^2 \times 5$.

Since $2^{3\times 2} = 2^6 \equiv 1 \pmod{3^2}$, we have $a \equiv 2^{a \bmod 6} \equiv 2^4 \equiv 7 \pmod 9$. Also, we have $a \equiv 0 \pmod{2^4}$ and $a \equiv 16 \pmod{5!}$. Combining the conditions together gives us the result.

- $a \equiv 16 \pmod{7!}$, where $7! = 2^4 \times 3^2 \times 5 \times 7$.

  Since $2^6 \equiv 1 \pmod 7$, we have $a \equiv 2^{a \bmod 6} \equiv 2^4 \equiv 2 \pmod 7$. And by $a \equiv 16 \pmod{6!}$ we get the result.

- $a \equiv 25,216 \pmod{8!}$, where $8! = 2^7 \times 3^2 \times 5 \times 7$.

  This follows from $a \equiv 0 \pmod{2^7}$ and $a \equiv 16 \pmod{7!}$.

- $a \equiv 186,496 \pmod{9!}$, where $9! = 2^7 \times 3^4 \times 5 \times 7$.

  Since $2^{3^3\times 2} = 2^{54} \equiv 1 \pmod{3^4}$, we have $a \equiv 2^{a \bmod 54} \pmod{3^4}$. To find $a \bmod 54$, first note that $2^{3^2\times 2} = 2^{18} \equiv 1 \pmod{3^3}$, and that $a \equiv 16 \pmod{18}$ because $a \equiv 7 \pmod 9$ and $a \equiv 0 \pmod 2$. It follows that $a \equiv 2^{a \bmod 18} \equiv 2^{16} \equiv 7 \pmod{3^3}$. Together with $a \equiv 0 \pmod 2$ we obtain $a \equiv 34 \pmod{54}$. Therefore $a \equiv 2^{a \bmod 54} \equiv 2^{34} \equiv 34 \pmod{3^4}$. Combining this with $a \equiv 25,216 \pmod{8!}$ leads us to the result.

- $a \equiv 1,275,136 \pmod{10!}$, where $10! = 2^8 \times 3^4 \times 5^2 \times 7$.

  Since $2^{5\times 4} = 2^{20} \pmod{5^2}$, we have $a \equiv 2^{a \bmod 20} \pmod{5^2}$. Note that $a \equiv 16 \pmod{20}$ because $a \equiv 0 \pmod 4$ and $a \equiv 1 \pmod 5$. Hence $a \equiv 2^{16} \equiv 11 \pmod{5^2}$. Together with $a \equiv 0 \pmod{2^8}$ and $a \equiv 186,496 \pmod{9!}$ we get the result.

- $a \equiv 26,676,736 \pmod{11!}$, where $11! = 2^8 \times 3^4 \times 5^2 \times 7 \times 11$.

  Since $2^{10} \equiv 1 \pmod{11}$, we have $a \equiv 2^{a \bmod 10} \pmod{11}$. But $a \equiv 6 \pmod{10}$ since $a \equiv 0 \pmod 2$ and $a \equiv 1 \pmod 5$, so $a \equiv 2^6 \equiv 9 \pmod{11}$. Together with $a \equiv 1,275,136 \pmod{10!}$ the result follows.

Then, set $b_m := a \bmod m!$ so that $a = (b_m \pmod{m!})_{m>0}$. While converting $(b_m \pmod{m!})_{m>0}$ into the form $\sum_{n=1}^{\infty} c_n n!$, we have been aware from part (a) that $c_n = (b_{n+1} - b_n)/n!$. Applying this formula, we know $c_1, \cdots, c_{10}$ are 0, 2, 2, 0, 0, 0, 5, 4, 3, 7, respectively.

1.17 A subset J of a partially ordered set I is called *cofinal* if $\forall i \in I : \exists j \in J$ such that $j \geq i$.

(a) Prove: if J is a cofinal subset of a direct partially ordered set, then J is directed.

(b) Let the notation be as in 1.7, and let $J \subset I$ be a cofinal subset. Prove that there is a canonical bijection $\varprojlim_{j\in J} S_j \cong \varprojlim_{i \in I} S_i$.

(c) Prove: $\hat{\mathbb{Z}} \cong \varprojlim_{n>0} \mathbb{Z}/n!\mathbb{Z}$.

For (a), let $i, j \in J \subset I$. I is direct implies $\exists k \in I$ such that $k \geq i$ and $k \geq j$. By cofinality, there exists an $l \in J$ so that $l \geq k$. Hence $l \geq i$ and $l \geq j$. This proves J is also a direct set.

It now makes sense to talk about the inverse limit $\varprojlim_{j \in J} S_j$. There are canonical projections $\varprojlim_{i \in I} S_i \to S_j$ for all $j \in J$. The morphisms clearly commute with the morphisms in the projective system $\{S_j : j \in J\}$. The universal property says that there exists a morphism $\theta : \varprojlim_{i \in I} S_i \to \varprojlim_{j \in J} S_j$.

Firstly, this map is canonical by construction. For the surjectivity, let $x = (s_j)_{j \in J} \in \varprojlim_{j \in J} S_j$. For each $i \in I$, we choose $j \geq i$ by cofinality and define $s_i := f_{ji}(s_j)$. This is well-defined. Indeed, if there exists another $k \in J$ with $k \geq i$. Pick $l \in J$ so that l dominates j and k.

$$f_{ji}(s_j) = f_{ji} \circ f_{lj}(s_l) = f_{ki} \circ f_{lk}(s_l) = f_{ki}(s_k).$$

By construction, $(s_i)_{i \in I} \in \varprojlim_{i \in I} S_I$ and $\theta((s_i)_{i \in I}) = x$. The injectivity is obvious. These prove (b).

For the last one, put $J = \{n! : n \in \mathbb{N}\}$ and $I = \mathbb{N}$ with the usual ordering. Using (b), we obtain (c).

1.19 Let π be a profinite group acting on a set E. Prove that the action is continuous if and only if for each $e \in E$ the *stabilizer* $\pi_e = \{\sigma \in \pi : \sigma e = e\}$ is open in π, and for finite E if and only if the *kernel* $\pi' = \{\sigma \in \pi : \sigma e = e, \quad \forall e \in E\}$ of the action is open in π.

Let $\theta : \pi \times E \to E$ be the action. For each $e \in E$, consider the composition $\pi \times \{e\} \to \pi \times E \to E$. Suppose the later one is continuous. Then the pre-image of $\{e\}$, which is equal to π_e, is clearly an open set. Conversely, it suffices to show that for any $e \in E$ the pre-image of $\{e\}$ is an open set in $\pi \times E$. Now $\theta^{-1}(\{e\}) = \{(\sigma, x) \in \pi \times E : \sigma x = e\}$. Let $\mathcal{O}(e)$ be the set of G-orbit of e. For any $m \in E$, there exists a g_m so that $g_m m = e$. We may write

$$\theta^{-1}(\{e\}) = \coprod_{m \in \mathcal{O}(e)} (g_m \pi_m \times \{m\}).$$

Hence it is open.

From now on suppose E is finite. Note that we have $\pi' = \bigcap_{e \in E} \pi_e$. Being an intersection of finitely many open sets, π' is clearly open. Conversely, assume that π' is open. $\pi' \leq \pi_e$ for any $e \in E$. π_e is open in π.

1.20 Let G be a group with profinite completion $\hat{G}$. Prove that the category *finite* G-sets is equivalence to the category of $\hat{G}$-**sets**.

Let $\mathcal{C}$ be the category of finite G-sets. Let X be an object in $\hat{G}$-sets. This means that X is a finite set with a continuous $\hat{G}$-action. There exists a natural group homomorphism $G \to \hat{G}$. Hence X can be viewed as a finite G-set. And $\hat{G}$-morphism also can be regarded as a G-morphism in this way. So we have defined a functor F from $\hat{G}$-sets to $\mathcal{C}$. It suffices to show that F is essentially surjective and fully faithful.

Let Y be an object in $\mathcal{C}$, i.e., there is an action of G on Y. Now consider the stabilizer of Y, denoted by H. Then H is normal and $[G:H] < \infty$. Let $\hat{G} \to G/H$ be the natural projection. This induces an action of $\hat{G}$ on Y. And by construction, the action is continuous. This proves F is essentially surjective.

We are going to show that F is fully faithful. Given two objects X and Y in $\hat{G}$, F induces a set-theoretic map

$$\mathrm{Hom}_{\hat{G}}(X,Y) \to \mathrm{Hom}_{\mathcal{C}}(F(X),F(Y)).$$

This map is injective by our construction. Given $f \in \mathrm{Hom}_{\mathcal{C}}(F(X),F(Y))$. f is a G-equivariant map from X to Y. By construction, the map f can also be viewed as a $\hat{G}$ equivariant map, say f'. Then we have $F(f') = f$. This shows F is fully faithful.

1.21 (a) Prove that the cateogry $\hat{\mathbb{Z}}$**-sets** is equivalent to the category whose objects are pairs (E,σ), with E a finite set and σ a permutation of E, a morphism from (E,σ) to (E',σ') being a map $f: E \to E'$ satisfying $f\sigma = \sigma' f$.

(b) Construct a profinite group π containing $\hat{\mathbb{Z}}$ as a closed normal subgroup of index 2, such that the category π**-sets** is equivalent to the category whose objects are triples (E,σ,τ), with E a finite set and σ and τ permutations of E for which $\sigma^2 = \tau^2 = \mathrm{id}_E$, a morphism from (E,σ,τ) to (E',σ',τ') being a map $f: E \to E'$ satisfying $f\sigma = \sigma' f$ and $f\tau = \tau' f$.

(a) By Exercise 1.20, the category of $\hat{\mathbb{Z}}$**-sets** is equivalent to the category of finite $\mathbb{Z}$-sets. Since $\mathbb{Z}$ is generated by 1, it suffices to consider how 1 acts on E, which should be a one-to-one map since (-1) acts reversely, and thus bijective as E is a finite set. So, 1 corresponds to some permutation $\sigma \in S^n$ if $|E| = n$. And the condition for morphisms is exactly the same condition for morphisms on finite $\mathbb{Z}$-sets.

(b) Construct π as follows: consider the category S consisting of objects (E,σ,τ), where E is a finite set and $\sigma^2 = \tau^2 = 1$. Also any morphism $f(E) = E'$ should satisfy $f\sigma = \sigma' f$, $f\tau = \tau' f$. Then, S can be regarded as the category finite P-sets, where P is a noncommutative group generating by s and t with $s^2 = t^2 = 1$. Suppose $\psi : S \to \hat{\mathbb{Z}}-$**sets** defined by $\psi(E,\sigma,\tau) = (E,\sigma\tau)$. We should check ψ is surjective to claim st is of infinite order. If it is the case, then by Exercise 1.20, the category finite P-sets is equivalent to π**-sets**, where $\pi = \hat{P}$. π hence contains $\hat{\mathbb{Z}}$, which is of index 2 since $\mathbb{Z} \cong \langle st \rangle$ is a normal subgroup of P of index 2. And $\hat{\mathbb{Z}}$ is necessary closed followed from Exercise 1.11 (b).

To show all permutations can be the product of two order 2 permutations, simply notice that

$$(1\,2\,\cdots\,m) = \left(\prod_{p<q}^{p+q=m+2}(p\,q)\right)\left(\prod_{p<q}^{p+q=m+1}(p\,q)\right),$$

and the two factors satisfy the equation $x^2 = 1$ in the permutation group.

1.24 Let it given that under the equivalence of categories in 1.14 finite coverings and finite sets correspond to each other. Deduce from this and Exercise 1.20 that the profinite group $\hat{\pi}(X)$ occuring in 1.15 is the profinite completion of the group $\pi(X)$ occuring in 1.14, if X is as in 1.14.

By 1.14 and *finite correspondence* mentioned above, given X satisfying the conditions in 1.14, category of finite coverings of X is equivalent to the category of finite $\pi(X)$-sets. And by Exercise 1.20, thus equivalent to the category of $\widehat{\pi(X)}$**-sets**. Since $\hat{\pi}(X)$ is determined uniquely up to isomorphism, $\widehat{\pi(X)} \cong \hat{\pi}(X)$.

1.25 Let X be the topological space $\{0, 1, 2, 3\}$, the open sets being $\emptyset$, $\{0\}$, $\{2\}$, $\{0, 2\}$, $\{0, 1, 2\}$, $\{0, 3, 2\}$, X. Prove: $\hat{\pi}(X) \cong \hat{\mathbb{Z}}$.

1.26 (a) Let π be a profinite group such that $x^2 = 1$ for all $x \in \pi$. Prove that π is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\mathbf{n}}$ for a uniquely determined cardinal number $\mathbf{n}$, which is equal to the $\mathbb{Z}/2\mathbb{Z}$-dimension of the group of continuous group homomorphisms $\pi \to \mathbb{Z}/2\mathbb{Z}$.

(b) Let G be the additive group of a $\mathbb{Z}/2\mathbb{Z}$-vector space of dimension $\mathbf{k}$, where $\mathbf{k}$ is an infinite cardinal. Prove: $\hat{G} \cong (\mathbb{Z}/2\mathbb{Z})^{2^{\mathbf{k}}}$ as profinite groups.

(c) Construct a profinite group that is not isomorphic to the profintie completion of any abstract group

(a) G consists only of involutions and thus G is Abelian. Given any open normal subgroup N, $G/N \cong (\mathbb{Z}/2\mathbb{Z})^n$ for some positive integer n. Let $N_1 \cdots N_n$ be open normal subgroups with index 2 such that $G/N \cong G/N_1 \times \cdots \times G/N_n$ and $N = \bigcap_{i=1}^n N_i$. Consider the group of all continuous group homomorphism in the form $G \to \mathbb{Z}/2\mathbb{Z}$, and this group naturally has $\mathbb{Z}/2\mathbb{Z}$-vector space structure. Fix a basis of the vector space, call it Σ. Then the canonical homomorphisms $\pi_i : G \to G/N_i \cong \mathbb{Z}/2\mathbb{Z}$ have decompositions: $\pi_i = \sum_{j=1}^{m_i} f_{ij}$ where $f_{ij} \in \Sigma$. Then $\bigcap_{i,j} \ker f_{ij} \subset \bigcap_{i=1}^n N_i = N$. So, finite intersections of $\ker(f_i)$ where $f_i \in \Sigma$ form a cofinal subset of all open normal subgroups of G. On the other-hand, we have canonical projections $p_f : (\mathbb{Z}/2\mathbb{Z})^\Sigma \to \mathbb{Z}/2\mathbb{Z}$ (f denoted as an element of Σ), and similarly the finite intersections of kernel of p_f also form a cofinal subset of all open normal subgroups of $(\mathbb{Z}/2\mathbb{Z})^\Sigma$. Given $f_1 \cdots f_n \in \Sigma$, $(\mathbb{Z}/2\mathbb{Z})^\Sigma / \bigcap_{i=1}^n \ker(f_i) \cong (\mathbb{Z}/2\mathbb{Z})^n$ and $[G : \bigcap_{i=1}^n \ker(f_i)] = 2^m$ (where $m \leq n$). Let us verify that $m = n$. Suppose not, let $v_1 \cdots v_m$ be a basis of $G/\bigcap_{i=1}^n \ker(f_i)$. Define $A \in M_{m\times n}(\mathbb{Z}/2\mathbb{Z})$ by $A_{i,j} = f_j(v_i)$. Because $m < n$, there exists a nonzero vector $x \in \mathbb{Z}/2\mathbb{Z}^n$ such that $A \cdot x = (0)_{m\times 1}$. But $f_1 \cdots f_n$ are $\mathbb{Z}/2\mathbb{Z}$-linearly independent, there exists $g \in G$ such that $\sum_{i=1}^n x_i f_i(g) = 1$, where $x = (x_1, \cdots, x_n)^t$. Say $g = \sum_{i=1}^m a_i v_i$ in $G/\bigcap_{i=1}^n \ker(f_i)$. This then implies $(a_1, \cdots, a_m) \cdot A \cdot x = 1$, contradiction. Also we have a canonical injective group homomorphism $G/\bigcap_{i=1}^n \ker(f_i) \to (\mathbb{Z}/2\mathbb{Z})^n$ by $g \mapsto (f_1(g), \cdots, f_n(g))$. But as $\mathbb{Z}/2\mathbb{Z}$-vector space, they have same dimension; therefore, above mapping is actually isomorphic. Such isomorphisms are compatible with restriction maps; therefore, $G \cong (\mathbb{Z}/2\mathbb{Z})^\Sigma$.

(b) Let us estimate the dimension of Γ, the $\mathbb{Z}/2\mathbb{Z}$ vector space of all continuous group homomorphism $\hat{G} \to \mathbb{Z}/2\mathbb{Z}$, and then apply (a).

Since the image of the canonical injective group homomorphism $G \to \hat{G}$ is dense in $\hat{G}$, a continuous group homomorphism $\hat{G} \to \mathbb{Z}/2\mathbb{Z}$ is determined by a group homomorphism $G \to \mathbb{Z}/2\mathbb{Z}$. Thus the case is reduced to compute the dimension of the dual space of G, which is 2^k. This means $\hat{G} \cong (\mathbb{Z}/2\mathbb{Z})^{2^k}$.

(c) From (b), the cardinality of completions of such abstract groups are either finite or greater than or equal to the cardinality of $\mathbb{R}$. Therefore, $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{Q}}$ is not completion of any abstract group.

1.27 Let X be an infinite topological space whose closed sets are exactly the finite subsets and X itself.

(a) Prove that every covering of X is trivial (see the Introduction), that X is connected, and that the group $\hat{\pi}(X)$ from 1.15 is trivial.

(b) Suppose that X is countable. Prove that X is not pathwise connected.

(c) Suppose that $\#X \geq \#\mathbb{R}$. Prove that X is locally pathwise connected and semilocally simply connected, and that $\pi(X)$ is trivial.

(a) Since obviously X is irreducible, use [1.28].

(b) Suppose not. Then given any two distinct points p, q, there exists continuous function $f : [0,1] \to X$ such that $f(0) = p, f(1) = q$. Then $\mathrm{im}(f)$ is a finite subset or a countably infinite subset of X. It suffices to consider that $\mathrm{im}(f)$ is of countably infinite. Say $\mathrm{im}(f) = \bigcup_{i=1}^{\infty} p_i$. Then $[0,1] = \bigcup_{i=1}^{\infty} f^{-1}(p_i)$, which is a countably infinite union of closed disjoint intervals, which is disconnected. Contradiction.

(c) Assume the axiom of choice is true. Recall the definition of locally path connected and semi-locally simply connected:

Locally path connected: for every point p and open set U containing p, there exist open path connected V such that $p \in V \subset U$.

Semi-locally simply connected: Every point in X has a neighborhood U with the property that every loop in U can be contracted to a single point.

Proof of locally path connected: Since cardinality of X is greater than $\mathbb{R}$, there exists a surjective map $F : X \to \mathbb{R}$. Let open subset U containing p, since $X \setminus U$ is a finite set, $\Sigma := \mathbb{R} \setminus F(U)$ is a set of finitely many points. Because cardinality of U is greater than $\mathbb{R}$, $F|_U$ is not injective. We can always manually adjust $F|_U$ so that $F|_U : U \to \mathbb{R}$ is surjective. Now, we may assume $F : U \to \mathbb{R}$ is surjective. Let p, q be distinct points in U, and $F(p) < F(q)$. By axiom of choice, we can define a function $f : [F(p), F(q)] \to U$ by defining $f(F(p)) := p$, and $f(F(q)) := q$ and for $y \in (F(p), F(q))$, let $f(y)$ be an element of $F^{-1}(y)$. Given any closed subset of $\mathrm{im}(f)$, that is, a finite subset of $\mathrm{im}(f)$, the pre-image is a set of finitely points in $[F(p), F(q)]$, which is closed. Therefore, f is continuous. Suppose $F(p) = F(q)$. Then adjust F by: picking any $x \in \mathbb{R}$ such that $x \neq F(q)$ and redefine the value of q, $F(q) := x$. Then we can apply similar argument. Therefore, U is path connected, and actually X is a path connected space.

Proof of semi-locally simply connected: Let $f : [0,1] \to X$ be a loop, ...

1.28 Let X be an irreducible topological space. Prove that the group $\hat{\pi}(X)$ from 1.15 is trivial.

Let $f : Y \to X$ be any covering where Y is a connected topological space. Then construct a function by sub-covering $g : Z \subset Y \to X$ by: Pick any point $p \in X$ and an open neighborhood N of p such that $f|_{f^{-1}(N)}$ is a trivial covering. Fix a piece of $f^{-1}(N)$, $\hat{N}$. Then for any other points of X, $z \notin N$, and any trivial neighborhood N_z, $N_z \cap N \neq \emptyset$ and $N_z \cap N \neq \emptyset$ is also a trivial neighborhood. Then there exists exactly one piece of $f^{-1}(N_z)$ whose intersection with $\hat{N}$ is nonempty. Let $Z := \bigcup_{z \notin N} \hat{N}_z \cup N$. Then f restricted to Z is a homeomorphism to X, but Y is connected. This implies $Y = Z$ and Y is a trivial covering.

1.29 Put $A = \mathbb{Z}[\sqrt{-3}]$, $B = \mathbb{Z}[X]/(X^4 + X^2 + 1)$ and $\beta = (X \mod X^4 + X^2 + 1) \in B$. View B as an A-algebra via the ring homomorphism $A \to B$ mapping $\sqrt{-3}$ to $\beta - \beta^{-1}$. Prove that B is a free separable A-algebra.

First, we check that B is a free A-module with a basis $\{1, \beta\}$. Note that the inverse of β is $-\beta(\beta^2 + 1)$. Clearly, the A-module B is generated by $1, \beta, \beta^2, \beta^3$. By a direct computation, we have $\beta^2 = 1 + \sqrt{-3}\beta$, $\beta^3 = \sqrt{-3} - 2\beta$ and $\beta^4 = -2 + \sqrt{-3}\beta$. Also, $1, \beta$ are linearly independent over A by comparing the degree in $\mathbb{Z}[X]$. Hence B is a free A-module of rank 2.

Under the basis $\{1, \beta\}$, we have

$$[m_\beta] = \begin{pmatrix} 0 & 1 \\ 1 & \sqrt{-3} \end{pmatrix}, \ [m_{\beta^2}] = \begin{pmatrix} 1 & \sqrt{-3} \\ \sqrt{-3} & -2 \end{pmatrix}.$$

Then

$$\det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\beta) \\ \mathrm{Tr}(\beta) & \mathrm{Tr}(\beta^2) \end{pmatrix} = \det \begin{pmatrix} 2 & \sqrt{-3} \\ \sqrt{-3} & -1 \end{pmatrix} = 1.$$

By the exercise 1.3, B is a free separable A-algebra.

2 Exercises for Section 2

2.2 Let $K \subset L$ be a Galois extension of fields, and I any directed set of subfields $E \subset L$ with $K \subset E$ Galois for which $\bigcup_{E \in I} E = L$. Prove that there is an isomorphism of profinite groups $\mathrm{Gal}(L/K) \cong \varprojlim_{E \in I} \mathrm{Gal}(E/K)$. (N.B.: the groups Gal(E/K) need not be finite here, they are merely profinite.)

The natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ is given by $\sigma \mapsto \sigma|_E$. This is well-defined since E is Galois over K. So we obtained a morphism

$$\theta : \mathrm{Gal}(L/K) \to \varprojlim_{E \in I} \mathrm{Gal}(E/K).$$

θ is injective, since if $\sigma|_E = \mathrm{id}_E$ for all such E, then $\sigma = \mathrm{id}_L$. For the surjectivity, let $(\sigma_E)_{E \in I} \in \varprojlim_{E \in I} \mathrm{Gal}(E/K)$. Construct an element $\epsilon \in \mathrm{Gal}(L/K)$ as follow: If $\alpha \in L$, then $\alpha \in E$ for some E since $L = \bigcup_{E \in I} E$. Then define $\epsilon(\alpha) := \sigma_E(\alpha)$. This is again well-defined by our assumption $(\sigma_E)_{E \in I} \in \varprojlim_{E \in I} \mathrm{Gal}(E/K)$. And $\epsilon \mapsto (\sigma_E)_{E \in I}$.

2.3 (a) Let $K \subset L$ be a Galois extension of fields, with Galois group G. View G as a subset of the set L^L of *all* functions $L \to L$. Let L be given the discrete topology and L^L the product topology. Prove that the topology of the profinite group G coincides with the relative topology inside L^L.

(b) Conversely, let L be any field and $G \subset \mathrm{Aut}(L)$ a subgroup that is compact when viewed as a subset of L^L (topologized as in (a)). Prove that $L^G \subset L$ is Galois with Galois group G.

(c) Prove that any profinite group is isomorphic to the Galois group of a suitably chosen Galois extension of fields.

For (a), if U is an open set in L^L, we may assume that $U = \prod_{l\in L} U_l$ with $U_k = \{s_k\}$ for finitely many $k \in L$ and $U_l = L$ for the remaining. The intersection $U \cap G$ is the set of all automorphisms σ such that $\sigma(k) = s_k$ for those k. Let $X \subset L$ be a finite Galois extension over K ontaining all such k. Let $\tau \in \mathrm{Gal}(X/K)$ with $\tau(k) = s_k$. Such τ exists provided that $U \cap G$ is non-empty.

Let I be the direct set given by finite Galois extensions with the usual inclusion maps. Define $V = \prod_{E\in I} V_E \subset \prod_{E\in I} \mathrm{Gal}(E/K)$ with $V_X = \{\tau\}$ and $V_E = \mathrm{Gal}(E/K)$ for $E \neq X$. V is open in $\prod_{E\in I} \mathrm{Gal}(E/K)$ and $V \cap G = U \cap G$.

So for any open set U in L^L, $G \cap U$ is open in G.

For the opposite direction, any open set in G is of the form $G \cap V$ with V open in $\prod_{E\in I} \mathrm{Gal}(E/K)$. We may assume $V = \prod_{E\in I} V_E$ with $V_E = \{\sigma_E\}$ for finitely many E and $V_F = \mathrm{Gal}(F/K)$ for the remaining. Since an automorphism is completely determined by its behavior on generators. Hence it is an intersection of G with some open set in L^L.

To prove (b), it suffices to show that L over L^G is algebraic. Take any $l \in L$. $G \cdot l$ is compact in L. Hence it is a finite set. Let $\{l_1, \cdots, l_N\}$ be the image. Then

$$f(x) := \prod_{i=1}^{N} (x - l_i) \in L^G[x].$$

So $L^G \subset L$ is an algebraic extension.

Finally, let G be any profinite group. $G = \varprojlim_{i\in I} G_i$ for some finite groups G_i. G_i can be embedded into S_{n_i} for some n_i. Let X_i be the set of n_i indeterminantes. S_{n_i} acts on X_i by permutation. This induces an action $G_i \times X_i \to X_i$. Let $X = \coprod_{i\in I} X_i$ and $L = \mathbb{C}(X)$. Then G acts on L. G is profinite $\Rightarrow$ G is compact, and hence by (a), the hypothesis of (b) holds. Therefore, L is a Galois extension of L^G with Galois group G.

2.6 Let $K \subset L$ be a Galois extension of fields, and $H' \subset H \subset \mathrm{Gal}(L/K)$ closed subgroups with $\mathrm{index}[H : H'] < \infty$. Prove that $L^H \subset L^{H'}$ is finite, and that $[L^{H'} : L^H] = \mathrm{index}[H : H']$. Which part of the conclusion is still true if H, H' are not necessarily closed?

Firstly, we prove that $[L^{H'} : L^H] \leq [H : H']$ and hence it is finite. Let $n = [H : H']$. Suppose the contrary that there exist $n+1$ elements which are linearly independent over

L^H, say $u_1, \cdots, u_{n+1}$. Let $\{\tau_i\}_{i=1}^n$ be a complete representative of left coset of H' in H. Let us consider the following linear equations.

$$\begin{aligned}
\tau_1(u_1)x_1 + \tau_1(u_2)x_2 + &\cdots + \tau_1(u_{n+1})x_{n+1} = 0 \\
\tau_2(u_1)x_1 + \tau_2(u_2)x_2 + &\cdots + \tau_2(u_{n+1})x_{n+1} = 0 \\
&\vdots \\
\tau_n(u_1)x_1 + \tau_n(u_2)x_2 + &\cdots + \tau_n(u_{n+1})x_{n+1} = 0.
\end{aligned}$$

There exists a non-zero solution to this system. Choose one, say $x_i = a_i$, so that the number of non-zero elements in the a_i's are minimum. Then I will try to construct another solution with more zeros in the a_i's.

Firstly, after multiplying by a non-zero constant and rearrange the variables, we may assume that $a_1 = 1$, $a_2 \neq 0$, $\cdots$, $a_k \neq 0$, and $a_{k+1} = \cdots a_{n+1} = 0$. Also, I may assume $\tau_1 = \mathrm{id}_{H'}$. The first equation reads

$$u_1 x_1 + \cdots + u_{n+1}x_{n+1} = 0.$$

Since u_i's are linearly independent over L^H, there exists at least one a_i, say a_2, such that $a_2 \in L^{H'} - L^H$. Choose an automorphism $\sigma \in H$ such that $\sigma(a_2) \neq a_2$. Now I consider the system equations

$$\begin{aligned}
\sigma\tau_1(u_1)x_1 + \sigma\tau_1(u_2)x_2 + &\cdots + \sigma\tau_1(u_{n+1})x_{n+1} = 0 \\
\sigma\tau_2(u_1)x_1 + \sigma\tau_2(u_2)x_2 + &\cdots + \sigma\tau_2(u_{n+1})x_{n+1} = 0 \\
&\vdots \\
\sigma\tau_n(u_1)x_1 + \sigma\tau_n(u_2)x_2 + &\cdots + \sigma\tau_n(u_{n+1})x_{n+1} = 0.
\end{aligned}$$

$\sigma(a_1) = \sigma(1) = 1$, $\sigma(a_2) \neq a_2, \cdots \sigma(a_{n+1})$ is a solution to this system. But since $\sigma\tau_i$ are a complete representatives of left cosets of H' in H, we have $\sigma\tau_i(u_s) = \tau_j(u_s)$ for some j, i.e., the new system is identically equal to the original one. Now $a_1 - \sigma(a_1) = 0$, $a_2 - \sigma(a_2) \neq 0$, $\cdots$, $a_{n+1} - \sigma(a_{n+1})$ is a non-zero solution to the system with more zeros than a_i's.

This proves $[L^{H'} : L^H] \leq [H : H']$.

Let $K \subset E \subset F \subset L$ be fields. I claim that $[E' : F'] \leq [F : E]$ if $[F : E] < \infty$, where E' means the automorphism groups of L fixing E.

Use induction on $n := [F : E]$. The case $n = 1$ is obvious. Suppose $n > 1$. Choose an element $u \in F - E$. Consider $E(u)$. If $[E(u) : E] < [F : E]$. Then by induction, we have $[E' : E(u)'] \leq [E(u) : E]$ and $[E(u)' : F'] \leq [F : E(u)]$. So the result follows.

We may assume $E(u) = F$. Let f be the minimal polynomial of u over E. We will construct an injection from the coset space E'/F' to the set of roots of f in L, say S.

Let $\tau F'$ be a coset. $\tau \in \mathrm{Aut}(L/E)$. Consider $\tau(u)$. This defines a map $T : E'/F' \to S$. It is not hard to check it is well-defined. Suppose $\tau(u) = \tau'(u)$. Then $\tau^{-1}\tau'(u) = u$. Hence $\tau^{-1}\tau'$ fixed F. So T is injective.

Now by Galois theory, since the groups are closed, $(L^H)' = H$ and $(L^{H'})' = H'$. So we have

$$[H : H'] \leq [L^{H'} : L^H] \leq [H : H'].$$

We remark that the closeness of H and H' are only used in the last step. Without assuming H, H' are closed, we still can show that

$$[L^{H'} : L^H] \leq [H : H'].$$

2.7 Let K, L, F be subfields of a field Ω, and suppose that $K \subset L$ is Galois and that $K \subset F$. Prove that $F \subset L \cdot F$ is Galois, and that $\mathrm{Gal}(L \cdot F/F) \cong \mathrm{Gal}(L/L \cap F)$ (as topological groups).

Define

$$I := \{K \subset E \subset L : [E : K] \text{ is finite and } E/K \text{ is Galois extension}\}.$$

Then L/K is Galois implies $L = \bigcup_{E \in I} E$. Also we have $L \cdot F = \bigcup_{E \in I} E \cdot F$ and

$$\mathrm{Gal}(E \cdot F/F) = \mathrm{Gal}(E/E \cap F) = \mathrm{Gal}(E \cdot (L \cap F)/L \cap F).$$

On the other hand, $E \cdot (L \cap F)$ is a Galois extension over $L \cap F$ and $L = \bigcup_{E \in I} E \cdot (L \cap F)$. Therefore, $L/L \cap F$ is a Galois extension. Moreover,

$$\mathrm{Gal}(L \cdot F/F) = \varprojlim_{E \in I} \mathrm{Gal}(E \cdot F/F) = \varprojlim_{E \in I} \mathrm{Gal}(E \cdot (L \cap F)/L \cap F) = \mathrm{Gal}(L/L \cap F).$$

2.8 Let K be a field. Prove that for every Galois extension $K \subset L$ the group $\mathrm{Gal}(L/K)$ is isomorphic to a quotient of the absolute Galois group of K.

Every Galois extension of K is a subfield of K_s containing K and corresponds to a closed normal subgroup of $\mathrm{Gal}(K_s/K)$. By (Thm2.3), done.

2.9 (a) Suppose that H is a *finite* subgroup of the absolute Galois group of a field K. Prove that $\#H \leq 2$ and $\#H = 1$ if $\mathrm{char}(K) > 0$. [*Hint:* [15, Theorem 56].]

(b) Let K be a field with separable closure K_s, and $\alpha \in K_s$, $\alpha \notin K$. Let E be a subfield of K_s, containing K that is maximal with respect to the property of not containing α. Prove that $\mathrm{Gal}(K_s/E) \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathrm{Gal}(K_s/K) \cong \mathbb{Z}_p$ for some prime number p.

(a) Let Σ be the set of all open normal subgroups of G with finite index. Because G is compact, elements of Σ are automatically closed subsets of G. Besides, $\bigcap_{N \in \Sigma} N = e$ (where e is identity element); therefore, e is closed in G. Let $g \in H$. Then the canonical translation map $g : G \to G$ is a homeomorphism implies that $g(e) = g$ is closed in G. Therefore, as a finite union of closed subsets, H is closed. Then by Main theorem of Galois theory, K_s/K_s^H is Galois with $\mathrm{Gal}(K_s/K_s^H) = H$. So K_s/K_s^H is a finite extension. Quote a theorem on this situation:

Theorem 56 (Fields and Rings, by Irving Kaplansky (1969; 2nd ed. 1972))

Theorem 1. *Let K be a field, not algebraically closed. If K has a finite extension L, which is algebraically closed. Then K is an ordered field and $L = K(i)$.*

If char$K = 0$, then $K_s = K_s^H(i)$, so $\#H = 2$. If char$K > 0$, then $H = \{e\}$; otherwise, K_s^H is an ordered field.

(b) There are two cases: K_s/E is a finite extension or not. By 2.9(a), if K_s/E is finite, then $\mathrm{Gal}(K_s/E) \cong \mathbb{Z}/2\mathbb{Z}$. In the following proof, assume K_s/E is infinite extension. The condition that E is maximal with respect to the property not containing α implies that for any proper extension H/E, $E(\alpha) \subset H$.

Step 1: $E(\alpha)/E$ is Galois extension of degree p, for prime number p.

Suppose $E(\alpha)/E$ is not Galois. Let $E(\alpha) \subset L$ be a Galois closure of E_α. Then $\mathrm{Gal}(L/E(\alpha))$ is not a normal subgroup in $\mathrm{Gal}(L/K)$. So there exists a distinct subgroup with same index as $\mathrm{Gal}(L/E(\alpha))$, but this implies L has a nontrivial subfield not containing $E(\alpha)$. Contradiction.

Also, $\mathrm{Gal}(E(\alpha)/E)$ has no proper subgroups. So $\mathrm{Gal}(E(\alpha)/E) = \mathbb{Z}/p\mathbb{Z}$.

Step 2: Any finite Galois extension H/E is of degree p^n for some positive integer n.

Suppose not. Let $\#\mathrm{Gal}(H/E) = p^n m$ where $(m,p) = 1$. Consider the p-Sylow subgroup Γ of $\mathrm{Gal}(H/E)$. Then $[H^\Gamma : E] = m$, which is impossible to contain $E(\alpha)$. Contradicition.

Step 3: For any positive integer n, there exists a unique finite Galois extension H/E such that $[H : E] = p^n$. ...

2.10 A *Steinitz number* or *supernatural number* is a formal expression $a = \prod_p p^{a(p)}$, where $a(p) \in \{0, 1, 2, \ldots, \infty\}$ for each prime number p. If $a = \prod_p p^{a(p)}$ is a Steinitz number, we denote $a\hat{\mathbb{Z}}$ the subgroup of $\hat{\mathbb{Z}}$ corresponding to $\prod_p p^{a(p)}\mathbb{Z}_p$ (with $p^\infty \mathbb{Z}_p = \{0\}$) under the isomorphism $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ (Exercise 1.14).

(a) Prove that the map $a \mapsto a\hat{\mathbb{Z}}$ from the set of Steinitz number to the set of closed subgroups of $\hat{\mathbb{Z}}$ is bijective. Prove also that $a\hat{\mathbb{Z}}$ is open if and only if a is *finite* (i.e., $\sum_p a(p) < \infty$).

(b) Let $\mathbb{F}_q$ be a finite field, with algebraic closure $\overline{\mathbb{F}}_q$. For a Steinitz number a, let $\mathbb{F}_{q^a}$ be the set of all $x \in \overline{\mathbb{F}}_q$ for which $[\mathbb{F}_q(x) : \mathbb{F}_q]$ divides a (in an obvious sense). Prove that the map $a \to \mathbb{F}_{q^a}$ is a bijection from the set of Steinitz numbers to the set of intermediate fields of $\mathbb{F}_q \subset \overline{\mathbb{F}}_q$. [Ernst Steinitz, German mathematician, 1871-1928.]

(a) Injectivity of such map is obvious. For subjectivity: Recall (ex1.11). A closed subgroup of $\prod_p \mathbb{Z}_p$ is of the form $\prod_p \pi_p$ where π_p is a closed subgroup of $\mathbb{Z}_p$, and closed subgroups of $\mathbb{Z}_p$ is of the form $p^{a(p)}\mathbb{Z}p$ for some $a(p) \in \mathbb{N}$. Recall that an subgroup is open if and only if it is closed with finite index. The index of $[\hat{\mathbb{Z}} : a\hat{\mathbb{Z}}] = [\prod_p \mathbb{Z}_p : \prod_p p^{a(p)}\mathbb{Z}_p] = \prod_p p^{a(p)}$. Therefore, $a\hat{\mathbb{Z}}$ is open if and only if a is finite.

(b) Discard the original notation.

Define ϕ : Steinitz numbers $\to$ collection of subsets of $\bar{\mathbb{F}}_q$ by

$$\phi(a) := \{x \in \bar{\mathbb{F}}_q \,|\, [\mathbb{F}_q(x) : \mathbb{F}_q] \text{ divides } a\}.$$

Step 1. For any Steinitz number a, $\phi(a)$ is a field containing $\mathbb{F}_q$.

Let $x \in \phi(a) \setminus \{0\}$. Then x^{-1} is in the subfield of $\mathbb{F}_q(x)/\mathbb{F}_q$. Therefore $[\mathbb{F}_q(x^{-1}) : \mathbb{F}_q]$ divides a. Let $y \in \phi(a)$. Because $\mathbb{F}_q$ is a finite field, there exists a unique extension of $\mathbb{F}_q$ with degree n, for any $n \in \mathbb{N}$, and every finite extension is Galois whose Galois group is cyclic. Therefore

$$[\mathbb{F}_q(x, y) : \mathbb{F}_q] = \text{l.c.m}([\mathbb{F}_q(x) : \mathbb{F}_q], [\mathbb{F}_q(y) : \mathbb{F}_q]),$$

which also divides a. Therefore, $\phi(a)$ is closed in addition and multiplication. So $\phi(a)$ is a field containing $\mathbb{F}_q$.

Step 2. If a is finite, set $a \in \mathbb{N}$, then $\phi(a) = \mathbb{F}_{q^a}$.

The reason is already stated in Step 1, it comes from the properties of a finite field.

Step 3. ϕ : Steinitz numbers → collection of intermediated fields of $\bar{\mathbb{F}}_q/\mathbb{F}_q$ is a bijective map. $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) = \hat{\mathbb{Z}}$. By 2.10(a), the closed subgroups has a 1-1 correspondence with Steinitz number. By Main theorem of Galois theory, there is a correspondence between intermediate field and closed subgroups; therefore, every intermediate field is of the form $\bar{\mathbb{F}}_q^{a\hat{\mathbb{Z}}}$. In the following, b is regarded to be a finite number dividing a.

$$\bar{\mathbb{F}}_q^{a\hat{\mathbb{Z}}} = \bar{\mathbb{F}}_q^{\bigcap_b b\hat{\mathbb{Z}}} = \bigcup_b \bar{\mathbb{F}}_q^{b\hat{\mathbb{Z}}} = \bigcup_b \mathbb{F}_{q^b} = \bigcup_b \phi(b) = \phi(a).$$

2.11 Let G be a profinite group. We call G *procyclic* if there exists $\sigma \in G$ such that the subgroup generated by σ is dense in G. Prove that the following assertions are equivalent:

(i) G is procyclic;

(ii) G is the projective limit of a projective system of finite cyclic groups;

(iii) $G \cong \hat{\mathbb{Z}}/a\hat{\mathbb{Z}}$ for some Steinitz number a (Exercise 2.10);

(iv) for any pair of open subgroups $H, H' \subset G$ with index$[G : H] =$ index$[G : H']$ we have $H = H'$.

Prove also that the Steinitz number a in (iii) is unique if exists.

(b)⇒(a) Given a direct system I with restriction maps $f_{ji} : G_j \to G_i$ where $j \geq i$ and G_i are cyclic. Let $G = \varprojlim G_i$. Without loss of generality, assume for every $j \geq i$, $f_{ji} : G_j \to G_i$ is surjective. Let S_i be the set of generators of G_i. Then S_i form a projective system because $f_{i,j}$ are surjective. Because S_i are finite and nonempty, their inverse limit is not empty. Now there exists an element $\sigma \in G$ given by $\sigma = \varprojlim_i \sigma_i$ where each σ_i is a generator of G_i. Now it is obvious to see that every open subset of G has non trivial intersection with $\langle \sigma \rangle$.

(a)⇒ (c) Consider the group homomorphism $\phi : \hat{\mathbb{Z}} \to G$ which sends 1 to *sigma*. It is obvious that ϕ is continuous. Because $\hat{\mathbb{Z}}$ is compact and G is Hausdorff, $\phi(\hat{\mathbb{Z}})$ is closed in G and containing $\langle \sigma \rangle$. Therefore, ϕ is surjective. Since $\ker \phi$ is closed in $\hat{\mathbb{Z}}$, $\ker \phi = a\hat{\mathbb{Z}}$ for some Steinitz number a. So $G \cong \hat{\mathbb{Z}}/a\hat{\mathbb{Z}}$.

(c)⇒ (d) From (c), $G \cong \prod_p \mathbb{Z}_p/p^{a(p)}\mathbb{Z}_p$. Then (d) is obvious.

(d)⇒(b) Step 1: Every subgroup of G with finite index is a normal subgroup.

Given a subgroup N, and any $g \in G$, gNg^{-1} is also subgroup having the same index with N. Therefore, $gNg^{-1} = N$ for every $g \in G$.

Step 2: Let N be a subgroup with finite index. Then G/N is cyclic. Let

$$n := \#G/N = \prod_{i=1}^{n} p_i^{s_i}.$$

If n is prime, then G/N is cyclic. Assume n is not prime. From condition (d), every cyclic subgroup of G/N is unique. So the collection of all cyclic subgroups of G/N can be endowed a partial order by the order of cyclic subgroups.

Suppose G/N is not cyclic. Then there does not exist an element with order n. But since G/N is a finite group, every element has a finite order. ...

2.12 Let K be a field with separable closure K_s. Prove that the absolute Galois group of K is procyclic (see Exercise 2.11) if and only if K has, for any positive integer n, at most one extension of degree n within K_s; and that it is isomorphic to $\hat{\mathbb{Z}}$ if and only if K has, for any positive integer n, exactly one extension of degree n within K_s.

The first statement is equivalent to (2.11 (d)). If $\mathrm{Gal}(K_s/K) = \hat{\mathbb{Z}}$, then $\mathrm{Gal}(K_s/K) = \hat{\mathbb{Z}}$ is pro-cyclic (2.11(c)).

Let

$$\Gamma = \{n \in \mathbb{N} | K \text{ has a finite extension with degree } n \text{ within } K_s\}.$$

Then $\mathrm{Gal}(K_s/K) = \varprojlim_{n\in\Gamma} \mathrm{Gal}(K_n/K) = \varprojlim_{n\in\Gamma} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$ implies $\Gamma = \mathbb{N}$. Conversely, if K has for any positive integer n, exactly one extension with degree n within K_s. Then $\mathrm{Gal}(K_s/K)$ satisfies (2.11(d)). So $\mathrm{Gal}(K_s/K) \cong \hat{\mathbb{Z}}/a\hat{\mathbb{Z}}$ for some Steinitz number a. Suppose $a \neq \prod_p p^\infty$, and let $a(p) < \infty$. Then K does not have a finite separable extension with degree $p^{a(p)+1}$, contradiction. So $\mathrm{Gal}(K_s/K) \cong \hat{\mathbb{Z}}$.

2.17 (**Kummer theory.**) Let K be a field with algebraic closure $\overline{K}$, and m a positive integer. Suppose that K contains a primitive m-th root of unity ζ_m, and let $E_m \subset K^*$ be the subgroup generated by ζ_m. Prove that there is a bijective correspondence between the collection of subfields $L \subset \overline{K}$ for which

$$L/K \text{ is Galois, } \mathrm{Gal}(L/K) \text{ is abelian, } \forall \sigma \in \mathrm{Gal}(L/K) : \sigma^m = \mathrm{id}_L$$

and the collection of subgroups $W \subset K^*$ for which $K^{*m} \subset W$; this correspondence maps L to $L^{*m} \cap K^*$ and W to $K(W^{1/m})$. Prove also that if L corresponds to W, there is an isomorphism of topological groups $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Hom}(W/K^{*m}, E_m)$ mapping σ to $(\alpha K^{*m} \mapsto \sigma(\alpha^{1/m})/\alpha^{1/m})$; here $\mathrm{Hom}(W/K^{*m}, E_m)$ has the relative topology in $(E_m)^{W/K^{*m}}$, where each E_m is discrete.

Let W be a subgroup of K^* containing K^{*m} and let $L = K(W^{1/m})$. Note that L/K is Galois because L is the splitting field of separable polynomials $X^m - \alpha$, $\alpha \in W$ (here we use assumptions that m primes to $\mathrm{char}(K)$ and K contains ζ_m).

First, we shall construct a bijection between $\mathrm{Hom}(W/K^{*m}, E_m)$ and the Galois group $G := \mathrm{Gal}(L/K)$. Define a pairing

$$G \times W \to E_m$$

by mapping (σ, α) to $\sigma(\alpha^{1/m})/\alpha^{1/m}$, denoted it by $\langle \sigma, \alpha \rangle$. Clearly, $\langle \sigma, \alpha \rangle$ is independent of the choice of an m-th root $\alpha^{1/m}$ of α, and the map is bilinear i.e.

$$\sigma((\alpha\beta)^{1/m})/(\alpha\beta)^{1/m} = (\sigma(\alpha^{1/m})/\alpha^{1/m})(\sigma(\beta^{1/m})/\beta^{1/m}).$$

Suppose that $\langle \sigma, \alpha \rangle = 1$ for all $\alpha \in W$. Then σ induces the identity on $W^{1/m}$ and thus on L. Hence the kernel on the left is 1. Let $\alpha \in W$ and suppose that $\langle \sigma, \alpha \rangle = 1$ for all $\sigma \in G$. If $\alpha^{1/m}$ is not in K, there is an automorphism of the subfield $K(\alpha^{1/m})$ over K which is not identity. Extend this automorphism to L, and call it σ. Then clearly $\langle \sigma, \alpha \rangle \neq 1$. Hence the kernel on the right is K^{*m}. Therefore the bilinear paring induces the bijection

$$G \xrightarrow{\sim} \mathrm{Hom}(W/K^{*m}, E_m)$$

which maps σ to $(\alpha K^{*m} \mapsto \sigma(\alpha^{1/m})/\alpha^{1/m})$. Note that the extension L/K is finite if and only if W/K^{*m} is finite and in particular we have the equality $[L : K] = [W : K^{*m}]$.

We shall prove that the correspondence between subfields $L \subset \overline{K}$ and subgroups $W \subset K^*$ is injective. Let W_1, W_2 be subgroups of K^* containing K^{*m}. If $W_1 \subseteq W_2$, then $K(W_1^{1/m}) \subseteq K(W_2^{1/m})$. Conversely, if $K(W_1^{1/m}) \subseteq K(W_2^{1/m})$ we wish to prove $W_1 \subseteq W_2$. For each $\alpha \in W_1$, we have

$$\alpha^{1/m} \in K(\alpha^{1/m}) \subseteq K(W_2^{1/m}).$$

Then $\alpha^{1/m}$ is contained in a finitely generated subextension of $K(W_2^{1/m})$ and thus we may assume that W_2/K^{*m} is finite. Let W_3 be the subgroup of K^* generated by W_2 and α. Then $K(W_2^{1/m}) = K(W_3^{1/m})$ and from what we saw above, we get the equality $[W_2 : K^{*m}] = [W_3 : K^{*m}]$ and thus $W_2 = W_3$. This proves that $W_1 \subseteq W_2$.

In order to prove the surjectivity, let L/K be an abelian (Galois) extension of exponent m. Any finite subextension is a composite of cyclic extensions of exponent m because any finite abelian group is a product of cyclic groups. Notice that m is a multiple of the degree of a finite cyclic extension. Since m is prime to $\mathrm{char}(K)$ and $\zeta_m \in K$, by a theorem of finite cyclic extension fields (cf. Hilbert 90), any finite cyclic extension of exponent dividing m equals $K(\alpha^{1/m})$ for some $\alpha \in K^*$. Hence L can be obtained by adjoining a collection of m-th roots $\{\alpha_\lambda^{1/m}\}_{\lambda \in \Lambda}$ with $\alpha_\lambda \in K^*$. Let W be the subgroup of K^* generated by K^{*m} and $\{\alpha_\lambda\}_{\lambda \in \Lambda}$. Hence $K(W^{1/m}) = K(\{\alpha_\lambda^{1/m}\}_{\lambda \in \Lambda}) = L$.

Finally, since each continuous bijection from a compact space to a Hausdorff space is a homeomorphism, the continuous bijection $G \xrightarrow{\sim} \mathrm{Hom}(W/K^{*m}, E_m)$ is an isomorphism of topological groups. We remark that this also can be proved by the following isomorphisms of profinite groups:

$$\begin{aligned} G &\simeq \varprojlim_{E\in I} \mathrm{Gal}(E/K) \\ &\simeq \varprojlim_{W'\in J} \mathrm{Hom}(W'/K^{*m}, E_m) \\ &\simeq \mathrm{Hom}(\varinjlim_{W'\in J} W'/K^{*m}, E_m) \simeq \mathrm{Hom}(W/K^{*m}, E_m), \end{aligned}$$

where I is the set of subfields E of L for which E/K is finite Galois and J is the set of subgroups W' of W for which $K^{*m} \subseteq W'$ and W'/K^{*m} is finite.

2.18 (**Artin-Schreier theory.**) Let K be a field with algebraic closure $\overline{K}$, let $p = \mathrm{char}(K) > 0$. Prove that there is a bijective correspondence between the collection of subfields $L \subseteq \overline{K}$ for which

$$K \subseteq L \text{ is Galois, } \forall \sigma \in \mathrm{Gal}(L/K) : \sigma^p = \mathrm{id}_L$$

and the collection of additive subgroups $W \subseteq K$ for which $\wp[K] \subseteq W$, where $\wp : \overline{K} \to \overline{K}$ is defined by $\wp(x) = x^p - x$; this correspondence maps L to $\wp[L] \cap K$ and W to $K(\wp^{-1}[W])$. Prove also that if L corresponds to W, there is an isomorphism of topological groups $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Hom}(W/\wp[K], \mathbb{F}_p)$ mapping σ to $(\alpha + \wp[K] \mapsto \sigma(\beta) - \beta$, where $\wp(\beta) = \alpha)$.

Let W be a subgroup of K containing $\wp[K]$ and let $L = K(\wp^{-1}[W])$. Note that L/K is Galois because L is the splitting field of separable polynomials $X^p - X - \alpha$, $\alpha \in W$.

First, we shall construct a bijection between $\mathrm{Hom}(W/\wp[K], \mathbb{F}_p)$ and the Galois group $G := \mathrm{Gal}(L/K)$. Define a pairing

$$G \times W \to \mathbb{F}_p$$

by mapping (σ, α) to $\sigma(\beta) - \beta$ where $\wp(\beta) = \alpha$, denoted it by $\langle \sigma, \alpha \rangle$. Clearly, $\langle \sigma, \alpha \rangle$ is independent of the choice of a β which satisfies $\wp(\beta) = \alpha$, and the map is bilinear since $\mathrm{char}(K) = p$.

Suppose that $\langle \sigma, \alpha \rangle = 0$ for all $\alpha \in W$. Then σ induces the identity on $\wp^{-1}(W)$ and thus on L. Hence the kernel on the left is 1. Let $\alpha \in W$ and suppose that $\langle \sigma, \alpha \rangle = 0$ for all $\sigma \in G$. If $\wp^{-1}\alpha$ is not contained in K, there is an automorphism of the subfield $K(\wp^{-1}\alpha)$ over K which is not identity. Extend this automorphism to L, and call it σ. Then clearly $\langle \sigma, \alpha \rangle \neq 0$. Hence the kernel on the right is $\wp[K]$. Therefore the bilinear paring induces the bijection

$$G \xrightarrow{\sim} \mathrm{Hom}(W/\wp[K], \mathbb{F}_p)$$

which maps σ to $(\alpha + \wp[K] \mapsto \sigma(\beta) - \beta)$, where $\wp(\beta) = \alpha$. Note that the extension L/K is finite if and only if $W/\wp[K]$ is finite and in particular we have the equality $[L : K] = [W : \wp[K]]$.

We shall prove that the correspondence between such subfields $L \subset \overline{K}$ and subgroups $\wp[K] \subseteq W \subseteq K$ is injective. Let W_1, W_2 be subgroups of K containing $\wp[K]$. If $W_1 \subseteq W_2$, then $K(\wp^{-1}[W_1]) \subseteq K(\wp^{-1}[W_2])$. Conversely, if $K(\wp^{-1}[W_1]) \subseteq K(\wp^{-1}[W_2])$ we wish to prove $W_1 \subseteq W_2$. For each $\alpha \in W_1$, we have

$$\wp^{-1}\alpha \subseteq K(\wp^{-1}\alpha) \subseteq K(\wp^{-1}[W_2]).$$

Then $\wp^{-1}\alpha$ is contained in a finitely generated subextension of $K(\wp^{-1}[W_2])$ and thus we may assume that $W_2/\wp[K]$ is finite. Let W_3 be the subgroup of K generated by W_2 and $\wp^{-1}\alpha$. Then $K(\wp^{-1}[W_2]) = K(\wp^{-1}[W_3])$ and from what we saw above, we get the equality $[W_2 : \wp[K]] = [W_3 : \wp[K]]$ and thus $W_2 = W_3$. This proves that $W_1 \subseteq W_2$.

In order to prove the surjectivity, let L/K be an abelian (Galois) extension of exponent p. Any finite subextension is a composite of cyclic extensions of exponent p because any finite abelian group is a product of cyclic groups. Notice that p is the degree of a finite cyclic extensions of exponent p. Since $\mathrm{char}(K) = p$, by a theorem of finite cyclic extension fields of degree p (cf. additive Hilbert 90), any finite cyclic extension of exponent p equals $K(\wp^{-1}\alpha)$ for some $\alpha \in K$. Hence L can be obtained by adjoining a collection of "$\wp$-th roots" $\{\wp^{-1}\alpha_\lambda\}_{\lambda\in\Lambda}$ with $\alpha_\lambda \in K$. Let W be the subgroup of K generated by $\wp[K]$ and $\{\alpha_\lambda\}_{\lambda\in\Lambda}$. Hence $K(\wp^{-1}W) = K(\cup_{\lambda\in\Lambda}\wp^{-1}\alpha_\lambda) = L$.

Finally, since each continuous bijection from a compact space to a Hausdorff space is a homeomorphism, the continuous bijection

$$G \xrightarrow{\sim} \mathrm{Hom}(W/\wp[K], \mathbb{F}_p)$$

is an isomorphism of topological groups. We remark that this also can be proved by the following isomorphisms of profinite groups:

$$\begin{aligned} G &\simeq \varprojlim_{E\in I} \mathrm{Gal}(E/K) \\ &\simeq \varprojlim_{W'\in J} \mathrm{Hom}(W'/\wp[K], \mathbb{F}_p) \\ &\simeq \mathrm{Hom}(\varinjlim_{W'\in J} W'/\wp[K], \mathbb{F}_p) \simeq \mathrm{Hom}(W/\wp[K], \mathbb{F}_p), \end{aligned}$$

where I is the set of subfields E of L for which E/K is finite Galois and J is the set of subgroups W' of W for which $\wp[K] \subseteq W'$ and $W'/\wp[K]$ is finite.

2.23 (a) Let A be a local ring and $x \in A$ such that $x^2 = x$. Prove that $x = 1$ or $x = 0$.

(b) Prove that any ring isomorphism $\prod_{i=1}^s A_i \xrightarrow{\sim} \prod_{i=1}^t B_j$, where the A_i and B_j are local rings and $s, t < \infty$, is induced by a bijection $\sigma : \{1, 2, \cdots, s\} \xrightarrow{\sim} \{1, 2, \cdots, t\}$ and isomorphisms $A_i \xrightarrow{\sim} B_{\sigma(i)}$, $1 \le i \le s$.

For (a), $x(1-x) = 0$. In a local ring, at least one of x and $1-x$ is a unit. Indeed, if $x \in \mathfrak{m}$ (resp. $1-x \in \mathfrak{m}$), the unique maximal ideal, then $1-x \notin \mathfrak{m}$ (resp. $x \notin \mathfrak{m}$). So $1-x$ (resp. x) is a unit. $\Rightarrow 1-x = 0$ or $x = 0$.

To prove (b), since A_i, B_j's are local, the number of maximal ideals of $A := \prod_{i=1}^s A_i$ (resp. $B := \prod_{j=1}^t B_j$) is exactly s (resp. t). $A \cong B$ implies $s = t$. Further, A_i is an ideal in A. So its image in B under the isomorphism $\phi : A \cong B$ is also an ideal of B. Hence it is isomorphic to a direct product of ideals in B_j, $1 \le j \le t$. Write $A_i \cong J_1 \times \cdots \times J_t$ for $J_k \lhd B_k$. Let $\phi_i : A_i \to A \to B$. $\phi_i(1)$ is a unit in B. It is of the form $(u_1, \cdots, u_t)$ with u_i's being units in B_i. So either $J_k = B_k$ or $J_k = 0$. It is impossible that there are more than one $J_k \neq 0$ since A_i contains no idempotent other than 0 and 1. Hence $A_i \cong B_j$ for some j. Induction on $s = t$ proves the result.

3 Exercises for Section 3

3.1 (**Left limits and right limits [12].**) A *directed graph* D consists of a set $V = V_D$ of *vertices*, a set $E = E_D$ of *edges*, a *source* map $s = s_D : E \to V$ and a *target* map $t = t_D : E \to V$; each $e \in E$ is to be thought of as an arrow from $s(e)$ to $t(e)$. Let D be a directed graph and $\mathbf{C}$ a category. A *D-diagram* in $\mathbf{C}$ is a map that assigns to each $v \in V$ an object X_v of $\mathbf{C}$ and to each $e \in E$ a morphism f_e from $X_{s(e)}$ to $X_{t(e)}$ in $\mathbf{C}$. A *morphism* from a D-diagram $((X_v)_{v\in V}, (f_e)_{e\in E})$ to a D-diagram $((Y_v)_{v\in V}, (g_e)_{e\in E})$ is a collection of morphisms $(h_v : X_v \to Y_v)_{v\in V}$ in $\mathbf{C}$ such that $h_{t(e)} f_e = g_e h_{s(e)}$ for all $e \in E$.

(a) Show that the D-diagrams in $\mathbf{C}$ form a category. We denote this category by $\mathbf{C}^D$.

(b) Show that there exists a functor $\Gamma : \mathbf{C} \to \mathbf{C}^D$ mapping an object X to the *constant D-diagram* with $X_v = X$ for all $v \in V$ and $f_e = \mathrm{id}_X$ for all $e \in E$, and mapping a morphism $h : X \to Y$ to the morphism $(h_v)_{v\in V}$ with all $h_v = h$.

(c) A *left limit* of a D-diagram A in $\mathbf{C}$ is an object $\varprojlim A$ of $\mathbf{C}$ such that

$$\mathrm{Hom}_{\mathbf{C}}(-, \varprojlim A) \cong \mathrm{Hom}_{\mathbf{C}^D}(\Gamma(-), A)$$

as functors on C. Prove that $\varprojlim A$ is unique up to isomorphism if it exists, and that the notion of a left limit generalizes that of a projective limit (see 1.7 and Exercise 1.8).

(d) Show that $\mathbf{C}$ admits left limits of all D-diagrams in $\mathbf{C}$ if and only if the functor $\Gamma : \mathbf{C} \to \mathbf{C}^D$ has a *right adjoint* $\varprojlim : C^D \to C$, i.e.,

$$\mathrm{Hom}_{\mathbf{C}}(-, \varprojlim(-)) \cong \mathrm{Hom}_{\mathbf{C}^D}(\Gamma(-), -).$$

If this right adjoint exists, we say that $\mathbf{C}$ *admits left limits over D*.

(e) A *right limit* of a D-diagram A in $\mathbf{C}$ is an object $\varinjlim A$ of $\mathbf{C}$ such that

$$\mathrm{Hom}_{\mathbf{C}}(\varinjlim A, -) \cong \mathrm{Hom}_{\mathbf{C}^D}(A, \Gamma(-))$$

Formulate and prove the analogues of the assertions in (c) and (d). If Γ has a left adjoint $\varinjlim : \mathbf{C}^D \to \mathbf{C}$ we say that C *admits right limits over D*.

(a) Let D-diagrams be class of objects, and class of morphisms be defined in the statement. We have to check three conditions:

(i) Composition of morphisms: Let a, b, c be objects and $f \in \mathrm{Hom}(a, b)$ $g \in \mathrm{Hom}(b, c)$, the canonical composition $g \circ f \in \mathrm{Hom}(a, c)$.

(ii) identity morphism $\mathrm{id}_X : X \to X$. Canonically, a collection of morphisms $(\mathrm{id}_v : X_v \to X_v)$. Associativity is obvious.

...

(b) This is a covariant functor.

(c) Let L_1, L_2 be two left limits for $A \in C^D$ and $f_i : \Gamma(L_i) \to A$ be the canonical morphisms, $i = 1, 2$. ...

Let $(I, \leq)$ be a directed poset and G_i be objects in the set category and restriction maps $f_{i,j} : G_j \to G_i$ with $j \geq i$ satisfying

(1) $f_{ii} = \mathrm{id}_{G_i}$

(2) $f_{ik} = f_{ij} \circ f_{jk}$ for all $k \geq j \geq i$.

Then $(I, \leq)$ can be thought of as a directed graph D and the projective system as a D-diagram. Then the universal property of $\varprojlim_{i \in I} G_i$ is the definition of the left limit of the D-diagram.

(d) This follows directly from the definition of left limits.

(e) Prove that $\varinjlim A$ is unique up to isomorphism if exists, and that the notion of a right limit generalizes that of a injective limit.

Let R_1, R_2 be two right limits for $A \in C^D$, and $g_i : A \to \Gamma(R_i)$ be the canonical morphisms, $i = 1, 2$. ...

3.2 (**Left limits in axiom G1.**) Let $\mathbf{C}$ be a category.

(a) Prove that $\mathbf{C}$ admits left limits over the empty directed graph (with $V = E = \emptyset$) if and only if $\mathbf{C}$ has a terminal object.

(b) Prove that $\mathbf{C}$ admits left limits over the directed graph $\cdot \longrightarrow \cdot \longleftarrow \cdot$ if and only if the fibres product of any two objects over a third one exists in $\mathbf{C}$.

(a) Suppose C^D has a left limit over empty graph A. For every $K \in \mathrm{Ob}(C)$, The set $\mathrm{Hom}_{C^D}(\Gamma(K), A) = \{\emptyset\}$ has a unique element. Then $\mathrm{Hom}_C(K, \varprojlim A)$ also has an unique element, which implies $\varprojlim A$ is the terminal object of C. Conversely, let T be the terminal object of C. Both $\mathrm{Hom}_{C^D}(\Gamma(K), A)$ and $\mathrm{Hom}_C(K, T)$ has unique element for every $K \in \mathrm{Ob}(C)$.

Therefore, $\mathrm{Hom}_C(K, T) \cong \mathrm{Hom}_{C^D}(\Gamma(K), A)$, so T is the left limit over empty graph.

(b) The universal property of the product of any two objects over a third one coincides with that of the left limit of $. \longrightarrow . \longleftarrow .$

3.3 (**Equalizers and finite left limits.**) Let $\mathbf{C}$ be a category. An *equalizer* of two morphisms $f, g : X \to Y$ in $\mathbf{C}$ is a left limit of the D-diagram $f, g : X \rightrightarrows Y$ with $D = \bullet \rightrightarrows \bullet$. We say that $\mathbf{C}$ has *equalizers* if it admits left limits over $D = \bullet \rightrightarrows \bullet$. We say that $\mathbf{C}$ has *finite products* if it admits left limits over any D with V finite and $E = \emptyset$. We say that $\mathbf{C}$ has *finite left limits* if it admits left limits over any finite D (i.e., with both V and E finite).

(a) Suppose $\mathbf{C}$ satisfies G1 (see 3.1), and let $f, g : X \to Y$ be morphisms in $\mathbf{C}$. Let $X \times_Y X$ be formed with respect to f and g. Prove that there exists a natural morphism $X \times_Y X \to X \times X$ and a diagonal morphism $X \to X \times X$ such that $X \times_{X \times X} (X \times_Y X)$ is an equalizer of f, g.

(b) Prove that **C** satisfies G1 if and only if it has equalizers and finite products, and if and only if it has finite left limits.

3.4 (**Right limits in axiom G2.**) Let **C** be a category.

(a) Prove that **C** admits right limits over the empty directed graph if and only if **C** has an initial object.

(b) Prove that the following three assertions are equivalent.

(i) finite sums exists in **C**;

(ii) any two objects X, Y of **C** have a sum $X \amalg Y$ in **C**, and **C** has an initial object;

(iii) **C** admits right limits over any directed graph D with V finite and E empty.

(c) Show how the quotient X/G of an object X by a finite subgroup $G \subset \mathrm{Aut}(X)$ can be interpreted as a right objects.

(a) Similar to (3.2(a)).

(b)

(i)⇒(ii) Uses (a).

(ii)⇒(iii) Do this by induction. Assume C has right limits over any directed graph D with $\#V(D) = n$ and $E(D) = \emptyset$. Let $X_1 \cdots X_{n+1}$ be objects of C. Let B be the right limits over $X_1, \cdots, X_n$. Let us verify that $A := B \sqcup X_{n+1}$ with morphisms $v_i : X_i \to A$ is the right limit of $X_1, \cdots, X_{n+1}$.
Given an object K with morphisms $k_i : X_i \to K, i = 1, \ldots, n$. k_i induce a morphism $b_1 : B \to K$, which further induces $b_2 : A \to K$ such that $b_2 \circ v_i = k_i$ for any i. So A with morphisms v_i implies that $\mathrm{Hom}_C(A, \cdot) \cong \mathrm{Hom}_{C^D}(D, \Gamma(\cdot))$. So A is the right limit over $X_1, \cdots, X_{n+1}$.

(iii)⇒(i) Definition of finite sums.

(c) Let G be a finite subgroups of $\mathrm{Aut}(X)$, and G=$\{\mathrm{id}_X, \sigma_1 \cdots \sigma_n\}$. Let A be the right limit of the graph

$$\begin{tikzcd}
X \arrow[dr, "\mathrm{id}_X"] & \cdots & X \arrow[dl, "\sigma_n"] \\
& X &
\end{tikzcd}$$

and let $p : X \to A$ be the canonical morphism such that $p = p \circ \sigma_i$, and let Y with morphism $f : X \to Y$ satisfying $f = f \circ \sigma_i$ where $i = 1 \cdots n$.

$$\begin{tikzcd}
X \arrow[dr, "\mathrm{id}_X"] & \cdots & X \arrow[dl, "\sigma_n"] \\
& X \arrow[d, "p"] \arrow[dr, "f"] & \\
& A \arrow[r, dotted, "g"] & Y
\end{tikzcd}$$

Then f induces a morphism $g : X/G \to Y$ such that $f = g \circ p$. So A satisfies the definition of the quotient X/G.

3.5 Let $f : X \to Y$ be a morphism in a category $\mathbf{C}$. Prove that f is an epimorphism if and only if Y, together with $\mathrm{id}_Y : Y \to Y$ and $f : X \to Y$, is a right limit of the diagram $Y \longleftarrow X \longrightarrow Y$ in which both arrows equal f.

Assume Y, together with id_Y and $f : X \to Y$ is the right limit of $Y \xleftarrow{f} X \xrightarrow{f} Y$. Then given an object Z with morphisms $g : Y \to Z$ and $h : Y \to Z$ such that $g \circ f = h \circ f$. Then it induces a morphism $p : Y \to Z$ such that $g = p \circ \mathrm{id}_Y = h$.

$$\begin{tikzcd}
Z & & & \\
& Y \arrow[ul, dotted, "p"] & & \\
& & X \arrow[ul, "f"] \arrow[r, "f"] \arrow[d, "f"] & Y \arrow[ull, bend right, "\mathrm{id}_Y"'] \arrow[uulll, bend right, "h"'] \\
& & Y \arrow[uul, bend left, "\mathrm{id}_Y"] \arrow[uuull, bend left, "g"] &
\end{tikzcd}$$

Therefore, f is epimorphism. Now reverse the argument and assume f is epimorphism. Then it can be easily seen that Y, together with id_Y and $f : X \to Y$ is the right limit of $Y \xleftarrow{f} X \xrightarrow{f} Y$.

3.6 Let $\mathbf{C}$ be a category satisfying G1, and F a covariant functor from $\mathbf{C}$ to the category of sets

(a) Prove that F satisfies G4 if and only if it commutes with equalizers and with finite products, and if and only if it commutes with arbitrary finite left limits.

(b) Suppose that F satisfies G4 and G6, and let $f, g : X \to Y$ be morphisms in $\mathbf{C}$ with $F(f) = F(g)$. Prove that $f = g$.

(a) Restatement of (ex3.3(b)).

(b) Let A with morphism $u : A \to X$ be the equalizer over $X \underset{g}{\overset{f}{\rightrightarrows}} Y$. Since $F(f) = F(g)$ and F commutes with finite left limits, $F(A) \simeq^{F(u)} F(X)$. So u is an isomorphism. So u is epimorphism. Then $f \circ u = g \circ u$ implies $f = g$.

3.7 Let $\mathbf{C}$ be a category and F a covariant functor from $\mathbf{C}$ to the category of sets. Suppose that F commutes with finite right limits. Prove that F satisfies G4. [*Hint:* Exercises 3.4 and 3.5.]

This is just the restatement of (ex3.4, ex3.5)

3.18 (**Injective limits.**) An *injective system* of sets consists of a directed partially ordered set I, a collection of sets $(S_i)_{i \in I}$ and a collection of maps $(f_{ij} : S_i \to S_j)_{i.j \in I, i \leq j}$ satisfying the conditions

$$f_{ii} = (\text{identity on } S_i) \quad \text{for each } I \in I,$$

$$f_{ik} = f_{jk} \circ f_{ij} \quad \text{for all } i, j, k \in I \text{ with } i \leq j \leq k.$$

Call $x \in S_i$ *equivalent* to $y \in S_j$ if there exists $k \in I$ with $k \geq i, k \geq j$ and $f_{ik}(x) = f_{jk}(y)$ in S_k

(a) Prove that this is an equivalence relation on disjoint union of the sets S_i. The set of equivalence classes is called the *injective limit* of the system, notation: $\varinjlim S_i$ or $\varinjlim_{i \in I} S_i$.

(b) Prove that injective limit can be expressed as a right limit (Exercise 3.1).

(c) Suppose $I \neq \emptyset$, that all S_i are groups and that all f_{ij} are group homomorphisms. Show that $\varinjlim S_i$ has a natural group structure.

(d) Let I be the set of positive integers, ordered by divisibility. For $n, m \in I$, n dividing m, let $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the group homomorphism by mapping ($1 \mod n$) to ($m/n \mod m$). Prove that $\varinjlim \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z}$.

(a) $f_{ii} = \mathrm{id}$ is clear, so $x \sim x$. $x \sim y$ implies $y \sim x$ is trivial. For $x \sim y$ and $y \sim z$, we have $f_{ik}(x) = f_{jk}(y)$ and $f_{jl}(y) = f_{hl}(z)$ for some $k, l \in I$. Choose $t \geq k, l$. Then

$$f_{it}(x) = f_{kt} f_{ik}(x) = f_{kt} f_{jk}(y) = f_{jt}(y) = f_{lt} f_{jl}(y) = f_{lt} f_{hl}(z) = f_{ht}(z).$$

So $x \sim z$.

(b) We have a commutative

$$\begin{tikzcd}
S_i \arrow[rr, "f_{ij}"] \arrow[dr, "\phi_i"'] & & S_j \arrow[dl, "\phi_j"] \\
& \varinjlim S_i &
\end{tikzcd}$$

for all i, j. Denote $S = \varinjlim S_i$. Then S satisfies the universal property: Let T be an object such that

$$\begin{tikzcd}
S_i \arrow[rr, "f_{ij}"] \arrow[dr, "\psi_i"'] & & S_j \arrow[dl, "\psi_j"] \\
& T &
\end{tikzcd}$$

for all i, j. Then there exist an unique $u : S \to T$ such that $u \circ \phi_i = \psi_i$ for all i, i.e., if $[x \in S_i] \in S$, then $u([x]) := \psi_i(x_i)$. Conversely, given an $u : S \to T$, let $u \circ \phi_i = \psi_i$, we recover the morphisms above. So we have a bijection $\mathrm{Hom}_{(SET)}(S, T) = \mathrm{Hom}_{(SET)^D}((S_i, I, f_{ij}), \Gamma(T))$. This map is functorial, so $\varinjlim S_i$ is a right limit.

(c) Define an operation "+" on $S = \varinjlim S_i$: Let $[x], [y] \in S$, so $x \in S_i$, $y \in S_j$ for some i, j. Pick $k \geq i, j$. Then we define $[x] + [y] \equiv [f_{ik}(x) + f_{jk}(y)] \in S$. This is well defined. Since if $[x] = [x']$, i.e., $x' \in S_{i'}$. So $\exists i'' \geq i, i'$ such that $f_{ii''}(x) = f_{i'i''}(x')$. We have two kinds result of $[x] + [y]$:

$$[f_{ik}(x) + f_{jk}(y)], [f_{i'k'}(x') + f_{jk'}(y)],$$

for $k \geq i, j$ and $k' \geq i', j$. Choose $l \geq k, k'$. Then

$$\begin{aligned}
[x] + [y] = [f_{ik}(x) + f_{jk}(y)] &= [f_{kl} f_{ik}(x) + f_{kl} f_{jk}(y)] \\
&= [f_{il}(x) + f_{jl}(y)] \\
&= [f_{il}(x)] + [f_{f_{jl}(y)}] \\
&= [f_{i''j} f_{ii''}(x)] + [f_{k'l} f_{jk'}(y)] \\
&= [f_{i''l} f_{i'i''}(x')] + [f_{k'l} f_{jk'}(y)] \\
&= [f_{i'l}(x')] + [f_{jl}(y)] \\
&= [x'] + [y]
\end{aligned}$$

so this is independent of choice of x, similar argument holds to y. The identity element is $[e_{S_i}]$, and the inverse element of $[x]$ is $[-x]$.

(d) We have a diagram

$$\begin{tikzcd}
\mathbb{Z}/n\mathbb{Z} \arrow[rr, "n|m"] \arrow[dr, "\psi_n"'] & & \mathbb{Z}/m\mathbb{Z} \arrow[dl, "\psi_m"] \\
& \mathbb{Q}/\mathbb{Z} &
\end{tikzcd}$$

where $\psi_n(1) := \frac{1}{n} = \frac{1}{m}\frac{m}{n} = \psi_m(\frac{m}{n})$, so the diagram commutes. This induces an unique map $\varinjlim \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ by $[a \in \mathbb{Z}/m\mathbb{Z}] \mapsto [a/m]$. The map is 1-1 since $[a/m] = 0$ in $\mathbb{Q}/\mathbb{Z}$ implies $a \equiv 0 \pmod{\mathrm{m}}$. The map is onto since for all $\frac{n}{m}$ is mapped from $n \in \mathbb{Z}/m\mathbb{Z}$.

4 Exercises for Section 4

4.6 Let K be a field and G a finite abelian group of order not divisible by char(K). Prove that $K[G]$ is isomorphic to the product of a finite number of fields, and deduce that every $K[G]$-module is projective.

Use Thm(2.6). There is a ring isomorphism $K[G] \cong \prod_{i=1}^{m} B_i$. Here B_i's are K-algebra that are local with nilpotent maximal ideals. It suffices to show that $K[G]$ is reduced. Then by theorem (2.7), B_i's are finite separable field extension of K. Let $G = \{g_1, \cdots, g_n\}$. Since $g_i^n = 1$, g_i are diagonalizable over some algebraical closure of K, say $\overline{K}$, as a linear map $\overline{K}[G] \to \overline{K}[G]$. Since g_i's commute to each other, they can be diagonalized simultaneously. So are g for all elements in $\overline{K}[G]$. Now $\forall g \in K[G]$, we may assume g is diagonal. $g^n = 0$ implies $g = 0$. Hence $K[G]$ is reduced. Hence each B_i is a field.

For the second statement, if R is a finite direct product of fields, then any R module M is projective. Indeed, the localization of R at any prime ideal must be a field. So the localization of M is free, and hence projective. The result follows from the fact that projectivity is a local property.

4.7 Let A be a ring and G a finite abelian group for which $\#G \cdot 1 \in A^*$.

(a) Suppose that $f : M \to N$ is a homomorphism of $A[G]$-modules, and $g : N \to M$ an A-linear map with $fg = \mathrm{id}_N$. Define $g' : N \to M$ by $g'(x) := (\#G \cdot 1)^{-1} \cdot \sum_{\sigma \in G} \sigma \cdot g(\sigma^{-1} \cdot x)$. Prove that g' is a homomorphism of $A[G]$-modules and that $fg' = \mathrm{id}_N$.

(b) Let P be an $A[G]$-module. Prove that P is projective as an $A[G]$-module if and only if P is projective when considered as an A-module. (See the following exercise for a converse.)

For (a), let $\tau \in G$.

$$g'(\tau x) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot g(\sigma^{-1} \tau x) = \frac{1}{|G|} \sum_{h \in G} \tau h \cdot g(hx) = \tau g'(x). \tag{1}$$

And note that f is already an $A[G]$-linear map. f commutes with G-actions. So

$$fg'(x) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot fg(\sigma^{-1} x) = \frac{1}{|G|} \cdot |G| x = x.$$

For (b), note $A[G]$ is a free A-module. So if P is a projective $A[G]$-module, it is a direct summand of a free $A[G]$-module. Therefore, it is a direct summand of a free A-module, i.e., P is projective A-module.

Suppose P is a projective A-module. Assume P can be fitted into a split exact sequence of $A[G]$-modules

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] & F \arrow[r, "f"] & P \arrow[r] & 0, \end{tikzcd}$$

with F a free $A[G]$-module. Now regard this sequence as an A-module exact sequence. Then there exists a A-linear splitting $g : P \to F$. (a) says we can modify g into an $A[G]$-linear map g' with $fg' = \mathrm{id}_P$. We obtain a $A[G]$ splitting, i.e., P is a projective $A[G]$-module.

4.8 Let A be a ring and G a finite abelian group. Consider A as an $A[G]$-module by letting every $\sigma \in G$ act as the identity on A. Prove that A is projective as an $A[G]$-module if and only if $\#G \cdot 1 \in A^*$.

If $|G| \cdot 1 \in A^*$, consider $A[G] \to A$ by

$$(a_\sigma)_{\sigma \in G} \mapsto \sum_{\sigma \in G} a_\sigma \in A.$$

The map has a splitting $A \to A[G]$ by $a \mapsto (a/|G|)_{\sigma \in G}$. Note that these maps are $A[G]$-linear. Hence A is a direct summand of a free $A[G]$-module. So A is a projective $A[G]$-module.

Conversely, assume that A is a projective $A[G]$-module. Define $f : A[G] \to A$ by

$$\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g.$$

It is surjective and $A[G]$-linear. By projectivity, there exists a splitting $g : A \to A[G]$ so that $fg = \mathrm{id}_A$. Then splitting must be of the form

$$g(x) = \sum_{k \in G} h(x)k$$

by $A[G]$-linearity. $fg = \mathrm{id}_A \Rightarrow 1 = |G|h(1)$. Therefore, $|G| \in A^*$.

4.12 Let A be a Dedekind domain and $(I_n)_{n=0}^{\infty}$ a sequence of fractional A-ideals. Prove that $\oplus_{n=0}^{\infty} I_n \cong \oplus_{n=0}^{\infty} A$ as A-modules, and deduce that every projective A-module that is not finitely generated is free.

Let $\{x_1, x_2, ...\}$ be a countable set of generators of $\oplus_{n=0}^{\infty} I_n$ (Generators may have relations, but the construction below still work). Try to build a sequences of submodules $\{K_j\}_{j=1}^{\infty}$ of $\oplus_{n=0}^{\infty} I_n$ such that

(i) $K_1 \subset K_2 \subset ...$

(ii) K_j is free for all j

(iii) K_{j+1} is the direct sum of K_j and a free module

(iv) $\oplus_{n=0}^{\infty} I_n$ is the direct sum of K_j and a module L_j which is an infinite direct sum of finitely generated module of rank one

(v) $\cup_{n=1}^{\infty} K_n = \oplus_{n=0}^{\infty} I_n$

(i)∼(v) implies that $\oplus_{n=0}^{\infty} I_n$ is free.

Take $K_1 = (0)$, and suppose K_r has been constructed. Let y denote the first of the x_i's which is not in K_r, and z is the L_r component of y with respect to $K_r \oplus L_r = \oplus_{n=0}^{\infty} I_n$. By assumption, $L_r \simeq \oplus_{t=0}^{\infty} P_t$, where $P_t \triangleleft A$ is an invertible ideal. Suppose $z \in P_1 \oplus ... \oplus P_s$ and write $I := P_1 P_2 ... P_s$.

By A is Dedekind,

$$P_{s+1} \oplus P_{s+2} \simeq A \oplus P_{s+1}P_{s+2} \simeq I^{-1} \oplus IP_{s+1}P_{s+2} =: G \oplus H,$$

where $G := I^{-1}$ and $H := IP_{s+1}P_{s+2}$, respectively. Then the module $P_1 \oplus ... \oplus P_s \oplus G \simeq P_1 \oplus ... \oplus P_s \oplus P_1^{-1} ... P_s^{-1} \simeq A \oplus ... \oplus A$ is a free A-module, and we set $K_{r+1} := P_1 \oplus ... \oplus P_s \oplus G \oplus K_r$, and $L_{r+1} := H \oplus P_{s+3} \oplus ....$ Hence K_{r+1} and L_{r+1} satisfying $(i) \sim (iv)$, the final (v) is trivial, hence we are done.

(The construction can be found in I.Kaplansky's paper: "Modules over Dedekind Rings and Valuation Rings".)

Let P be a projective module over a Dedekind ring A which is not finitely generated. Then $P \oplus Q = F$ for some module Q and free module F. By A is Dedekind, A is hereditary, so $P \simeq \oplus_{k=0}^{\infty} I_k$ for I_k be ideals in A (ex.4.9(a)). So P is free by above argument.

4.13 Let A be a domain with field of fractions K and $I \subset K$ an A-module.

(a) Prove that I is projective if and only if it is invertible, and that it is free if and only if it is principal. [*Hint:* map a free module onto I.]

(b) Prove that invertible ideals are finitely generated.

(c) Prove that A is a Dedekind domain if and only if all ideals of A are projective.

For (a), suppose I is invertible, $I^{-1}I = A$, $1 = \sum_{i=1}^m c_i b_i$ for some $c_i \in I^{-1} := \{x \in Q(A) | xI \subset A\}$ and $b_i \in I$. Define maps $f_i : a \in I \mapsto ac_i \in A$, so $f_i \in \mathrm{Hom}_A(I, A)$. Hence for all $a \in A$, $a = \sum_i (ac_i)b_i = \sum_i f_i(a)b_i$, so by dual basis lemma, I is projective. (Recall the dual basis lemma: A module M is projective if and only if $\exists\{x_\alpha\}_{\alpha\in I} \subset M$ and $\{x^*_\alpha\}_{\alpha\in I} \subset M^*$ such that $\forall x \in M$, $x^*_\alpha(x) = 0$ for all but finitely many α and $x = \sum_\alpha x^*_\alpha(x)x_\alpha$.)

Conversely, suppose $I \lhd A$ is projective, the dual basis lemma asserts that $\exists\{b_\alpha\}_{\alpha\in\Lambda}$ generators of I, $\exists\{f_\alpha\}_{\alpha\in\Lambda} \subset \mathrm{Hom}_A(I, A)$, such that for each $a \in I$, $f_\alpha(a) = 0$ for all but finitely many α and $a = \sum_\alpha f_\alpha(a)b_\alpha$. Note that if $f \in \mathrm{Hom}_A(I, A)$ and $I \lhd A$ be fractional, then $f : a \mapsto b^{-1}f(b)a$ for all $b \in I \setminus \{0\}$. Fix $b \in I \setminus \{0\}$, since $f_\alpha(b) = 0$ for almost all α except some $\alpha = 1, 2, ..., m$ and $a = \sum_{\alpha\in\Lambda} f_\alpha(a)b_\alpha = \sum_{\alpha=1}^m b^{-1}f_\alpha(b)ab_\alpha$, so $1 = \sum_{\alpha=1}^m b^{-1}f_\alpha(b)b_\alpha$. Since $b^{-1}f_\alpha(b)a \in A$ for all $a \in I$, so define $c_\alpha := b^{-1}f_\alpha(b) \in I^{-1}$. Hence $1 = \sum_{\alpha=1}^m c_\alpha b_\alpha$, $c_\alpha \in I^{-1}$ and $b_\alpha \in I$, so I is invertible.

If the fractional ideal is principle, then it is clearly free. Conversely, if $I \subset K = Q(A)$ is free, choose $x_\alpha = \frac{a_\alpha}{b_\alpha}$ and $x_\beta = \frac{a_\beta}{b_\beta}$ be A-linearly independent for some a_α, a_β, b_α, and b_β in $A \setminus \{0\}$. Then

$$(-a_\beta b_\alpha)x_\alpha + (a_\alpha b_\beta)x_\beta = (-a_\beta b_\alpha)\frac{a_\alpha}{b_\alpha} + (a_\alpha b_\beta)\frac{a_\beta}{b_\beta} = 0.$$

So by A-linearly independence, $-a_\beta b_\alpha = a_\alpha b_\beta = 0$, means A has zero divisors, a contradiction. So I has at most one (free) generator.

(b) Let $I^{-1}I = A$, so $\exists c_i \in I^{-1}$ and $b_i \in I$ such that $\sum_{i=1}^n c_i b_i = 1$. So for all $b \in I$,

$$b = b \cdot 1 = b\sum_{i=1}^n c_i b_i = \sum_{i=1}^n (bc_i)b_i \in I$$

where $bc_i \in A$ since $c_i \in I^{-1}$.

(c) The definition of A to be Dedekind is that every fractional ideals in $Q(A)$ is invertible. So by (a), all ideals in A are projective.

4.14 Let A be a local ring with residue field k.

(a) Suppose $a_1, a_2, \ldots, a_n \in A$ are such that none of the a_i belongs to the ideal generated by the others, and let $a = (a_i)_{i=1}^n \in A^n$. Let $f : A^n \to A^n$ be an A-linear map with $f(a) = a$. Prove that $f \otimes \mathrm{id}_k$ is the identity mapping on k^n, and f is invertible.

(b) Let F be a free A-module, P a direct summand of F, and $a \in P$. Prove that there exists a free direct summand of P containing a. [*Hint:* Choose a basis of F on which a has the smallest possible number of non-zero coordinates, say $a_1, a_2, \ldots, a_n$, and apply (a) to a suitable map $A^n \to P \to A^n$.]

(c) Prove that countably generated projective A-module is free.

(a) Let $\{e_1, ..., e_n\}$ be standard basis of A^n and $f(e_i) = \sum_{j=1}^n b_{ij}e_j$ for all $i = 1, ..., n$. I need to show that (b_{ij}) is invertible. By $f(a) = a$, $\sum_{i=1}^n a_i e_i = \sum_{i=1}^n a_i \sum_{j=1}^n b_{ij}e_j = \sum_{j=1}^n (\sum_{i=1}^n a_i b_{ij})e_j$. So I get $a_j = \sum_{i=1}^n a_i b_{ij}$ for all j, hence

$$(1 - b_{jj})a_j = a_1 b_{1j} + ... + a_j \hat{b}_{jj} + ... + a_n b_{nj}$$

for all $j = 1, ..., n$. By a_j not lies in $(a_1, ..., a_{j-1}, a_{j+1}, ..., a_n)$, $(1-b_{jj})$ and b_{ij} are nonunits. $(1 - b_{jj})$ is nonunit means that it lies in the Jacobson radical of A, so $b_{jj} = 1 - (1 - b_{jj})$ is an unit in A. So the determinant of (b_{ij}) is $\det(b_{ij}) = \prod_{j=1}^n b_{jj} + (\mathit{nonunits})$ is an unit in A. Hence (b_{ij}) is invertible.

$f \otimes \mathrm{id}_k = \mathrm{id}$. ...

(b) Let $\mathbf{B} = \{e_i\}_{i \in I}$ be a free base of F such that $a = \sum_{i=1}^n a_i e_i$ and the number n is the smallest. This implies that a_i not lies in the ideal $(a_1, ..., a_{i-1}, a_{i+1}, ..., a_n)$, for if $a_j = \sum_{i \neq j}^n a_i b_i$ for some $b_i \in A$, then replace e_i by $e_i + b_j e_j, i = 1, ..., n, i \neq j$, and other e_i (i not in $\{1, ..., n\} \setminus \{j\}$) unchanged. Then we get a new base with shorter expression in a.

Let $e_i = y_i + z_i$, $y_i \in P$ and $z_i \in Q, i = 1, ..., n$. Then I get $a = \sum_{i=1}^n a_i y_i + \sum_{i=1}^n a_i z_i \in P$, so $\sum_{i=1}^n a_i z_i = 0 \in P \cap Q = \{0\}$. Define $N := \mathrm{span}_A(y_1, ..., y_n) \subseteq P$. Then $a = \sum_{i=1}^n a_i y_i \in N$.

I show that N is free, the strategy is to show $\{y_1, ..., y_n\} \cup (\mathbf{B} \setminus \{e_1, ..., e_n\})$ is a free base. Write $y_i = \sum_{j=1}^n h_{ij}e_j + t_i$, $i = 1, ..., n$, where t_i are combinations of $\{e_j\}_{j \geq n+1}$. Plug y_i into $a = \sum_{j=1}^n a_j e_j = \sum_{i=1}^n a_i y_i = a$, so

$$\sum_{j=1}^n a_j e_j = \sum_{i=1}^n a_i (\sum_{j=1}^n h_{ij}e_j + t_i) = \sum_{i,j=1}^n a_i h_{ij} e_j + \sum_{i=1}^n a_i t_i.$$

By $\{e_j\}$ are free basis, we get $a_j = \sum_{i=1}^n a_i h_{ij}$. From our choice of a_j's and similar arguments in (a), (h_{ij}) is invertible, so the map $F \to F$ via $e_i \mapsto y_i$ for $i = 1, ..., n$, and $e_i \mapsto e_i$ for $i \geq n + 1$ is invertible, ...

(c) Let P be countably generated and projective. Then $P \oplus Q = F$ for some A-module Q and free A-module F. Let $\{x_i\}_{i=1}^\infty$ be generators (not free) of P. I construct a sequence of free submodules of P_i (which are all free and $\oplus_{i=1}^\infty P_i \simeq P$) as follows: By (b), let P_1 be a free direct summand of P contains x_1, so we furnish P_1. Suppose we have constructed $P_1, \cdots, P_s$ such that $\oplus_{i=1}^s P_i$ contains $x_1, \cdots, x_s$ and $\oplus_{i=1}^s P_i$ is free, by (b), let P_{s+1} be a free direct summand of $P / \oplus_{i=1}^s P_i$ such that P_{s+1} contains the element $\pi_s(x_{s+1})$, where $\pi_s : P \to P / \oplus_{i=1}^s P_i$ is the canonical projection. So we construct all P_i's by induction.

By our construction, $\oplus_{i=1}^\infty P_i$ is free and it contains $\{x_i\}_{i=1}^\infty$, so $P = \oplus_{i=1}^\infty P_i$.

4.16 Deduce from 4.14 and 4.15 that any projective module over a local ring is free.

Let P be projective, so $P \oplus Q = F$ for some free F and Q. By F is free, we can write $F = \oplus_{\lambda \in \Lambda} F_\lambda$ where F_λ is countably generated for all λ. Then by ex.4.15(c), $P = \oplus_\lambda P_\lambda$ where P_λ is countably generated for all λ (and P_λ is also projective). So by ex.4.14(c), P_λ is free for all λ. So P is free.

4.17 Let an ideal $\mathfrak{a}$ of a ring A called *almost nilpotent* if for every sequence $(a_i)_{i=0}^\infty$ of elements of $\mathfrak{a}$ there exists n with $\prod_{i=0}^n a_i = 0$.

(a) Prove that a nilpotent ideal is almost nilpotent.

(b) Prove that a finitely generated almost nilpotent ideal is nilpotent.

(c) Let $K[X_1, X_2, \dots]$ be the polynomial ring in countably many variables over a field K, and I be the ideal generated by $\{X_k \cdot \prod_{i=1}^{n} X_i^{a(i)} : k, n \geq 1, a(i) \geq 0\,(0 \leq i \leq n), \sum_{i=1}^{n} a(i) \geq k\}$. Prove that $K[X_1, X_2, \dots]/I$ is a local ring whose maximal ideal is almost nilpotent but not nilpotent.

(a) If $\mathfrak{a}$ is nilpotent, then there exists $n \in \mathbb{N}$ such that $\mathfrak{a}^n = 0$. Done.

(b) If $\mathfrak{a}$ is almost nilpotent and finitely generated. Let $a_1, \dots, a_n$ generates $\mathfrak{a}$. Then it suffices to prove that every a_i is nilpotent. Consider sequences $a_i, a_i, a_i \cdots$. Then a_i is nilpotent.

(c) To prove that $K[X_1, X_2, \dots]/I$ is a local ring, it suffices to prove that for any element $r \in K[X_1, X_2, \dots]/I$ whether r or $1-r$ is unit. Furthermore, it suffices to prove that $1 + g(X_1, \dots X_n)$ is a unit where $g(X_1, \dots, X_n)$ is any polynomial without constant term and n any positive integer. Let $g(X_1, \dots, X_n) = \sum_{i_1,\dots i_n}^{n+1} k_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n}$. $g^n = 0$, so $1 + g$ is unit. $K[X_1, X_2, \dots]/I$ is a local ring with the maximal ideals $\mathfrak{m} := \{f \in K[X_1, X_2, \dots]/I | f \text{ has no constant term}\}$. Given a sequence $\{f_i\}_{i=1}^{\infty}$, $f_i \in \mathfrak{m}$, let $f_1 = f_1(X_1, \dots, X_n) = \sum_{i_1,\dots i_n}^{n+1} k_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n}$. Then $\prod_{i=1}^{n+1} f_i = 0$ because each term of $\prod_{i=1}^{n+1}(f_i)$ has degree larger than $n+1$. So $\mathfrak{m}$ is almost nilpotent.

Suppose $\mathfrak{m}$ is nilpotent. Let $\mathfrak{m}^N = 0$. But $x_{N+1}^N \in \mathfrak{m}$ is nonzero. Contradiction.

4.18 Let A be a local ring whose maximal ideal $\mathfrak{m}$ is almost nilpotent.

(a) Prove that any A-module M with $\mathfrak{m}M = M$ is zero.

(b) Let F be a free A-module. Prove that a subset of F is an A-basis if and only if it yields an $A/\mathfrak{m}$-basis for $F \otimes_A A/\mathfrak{m}$. Prove also that any generating set for F contains a basis.

(a) Suppose $\mathfrak{m}M = M \neq 0$. Let $J := Ann_A(M)$. Then $\mathfrak{m} \setminus J \neq 0$ because $M \neq 0$. Choose any $a_1 \in \mathfrak{m} \setminus J$. Then $a_1 M = a_1 \mathfrak{m} M \neq 0$. So $a_1 \mathfrak{m} \setminus J \neq \emptyset$.

Then there exist $a_2 \in \mathfrak{m} \setminus J$ such that $a_1 a_2 \in \mathfrak{m} \setminus J$. By induction, we can form an infinite sequence in $\mathfrak{m}$, but there exists finite integer n such that $\prod_{i=1}^{n} a_i = 0 \in J$, contradiction.

(b) Let Ξ be a basis of F. Then obviously $\Xi \otimes_A 1$ generates $F \otimes_A A/\mathfrak{m}$. Given $\{m_1 \dots m_n\} \subset F$ and $\{a_1 \dots a_n\} \subset A/\mathfrak{m}$ such that $\sum_{i=1}^{n} a_i m_i \otimes_A 1 = 0$. Then $\sum_{i=1}^{n} a_i m_i \subset \mathfrak{m}F$, which implies $a_i \equiv 0 \bmod \mathfrak{m}$.

Conversely, if $\Xi \otimes_A 1$ is a basis of $F \otimes_A A/\mathfrak{m}$, ...

Let Ω be a generating set of F. Then $\Omega \otimes_A 1$ contains a basis for $F \otimes_A A/\mathfrak{m}$, because every generating set of a vector space contains a basis. By previous argument, such subset of Ω is actually a basis of F.

4.19 Let A be a local ring whose maximal ideal $\mathfrak{m}$ is *not* almost nilpotent.

(a) Construct a countably generated nonzero A-module M with $M = \mathfrak{m}M$. [*Hint:* Consider a suitable injective limit $A \to A \to A \to \dots$.]

(b) Let $f : F \to M$ be A-linear, with F free and M as in (a). Prove that $\ker(f) \cup \mathfrak{m}F$ generates F but does not contain a basis.

(a) There exists a sequence $(a_i)_{i=1}^{\infty}$, $a_i \in \mathfrak{m}$ such that $\prod_{i=1}^{n} a_i \neq 0$ for any integer n. Consider the injective system $A \xrightarrow{a_1} A \xrightarrow{a_2} \cdots$ Let $M := \varinjlim A = \oplus_{i=1}^{\infty} A/(\sim)$ be the injective limit with respect to above system where $(\sim)$ is the submodule of $\oplus_{i=1}^{\infty} A$ generated by canonical relations. Then M is countably generated. Let $u_i : A \to M$ be the canonical homomorphism into the i-th component. Suppose $M = 0$. Then $u_1(1) = 0$ implies $\prod_{i=1}^{n} a_i = 0$ for some integer n. Contradiction.

Let $m \in M$. Then $m = u_i(m_i)$ for some integer i. So $m = a_{i+1}u_{i+1}(m_i) \in \mathfrak{m}M$. So $\mathfrak{m}M = M$.

(b) $M = \mathfrak{m}M$ implies that $\text{coker}f = \mathfrak{m}\text{coker}f$. ...

4.20 Let M, N be modules over a ring A, with M finitely presented, and let $S \subset A$ be a multiplicative subset. Prove that the obvious map $S^{-1}\operatorname{Hom}_A(M,N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$ is an $S^{-1}A$-module isomorphism.

Since M is finitely presented, there exists an exact sequence

$$\begin{tikzcd} A^m \arrow[r] & A^n \arrow[r] & M \arrow[r] & 0. \end{tikzcd}$$

Because $\operatorname{Hom}_A(\cdot, N)$ functor is right-exact, applying $\operatorname{Hom}_A(\cdot, N)$ to above sequence, we have

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}_A(M,N) \arrow[r] & \operatorname{Hom}_A(A^n,N) \arrow[r] & \operatorname{Hom}_A(A^m,N) \end{tikzcd}$$

and recognise $\operatorname{Hom}_A(A^n, N) = N^n$. Furthermore, S^{-1} localisation is an exact functor, apply to above sequence, we have:

$$\begin{tikzcd} 0 \arrow[r] & S^{-1}\operatorname{Hom}_A(M,N) \arrow[r] & S^{-1}N^n \arrow[r] & S^{-1}N^m. \end{tikzcd}$$

On the other side, back to the original sequence, and apply S^{-1} functor first then $\operatorname{Hom}_{S^{-1}A(\cdot, S^{-1}N)}$

$$\begin{tikzcd} S^{-1}A^m \arrow[r] & S^{-1}A^n \arrow[r] & S^{-1}M \arrow[r] & 0, \end{tikzcd}$$

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)) \arrow[r] & S^{-1}N^n \arrow[r] & S^{-1}N^m. \end{tikzcd}$$

Putting identity maps in vertical maps between the last two and check the commutativity

$$\begin{tikzcd} 0 \arrow[r] & S^{-1}\operatorname{Hom}_A(M,N) \arrow[r] \arrow[d, "\pi"] & S^{-1}N^n \arrow[r] \arrow[d, equal] & S^{-1}N^m \arrow[d, equal] \\ 0 \arrow[r] & \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)) \arrow[r] & S^{-1}N^n \arrow[r] & S^{-1}N^m \end{tikzcd}$$

where $\pi : S^{-1}\operatorname{Hom}_A(M,N) \to \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N))$ is the canonical map. We conclude that π is isomorphism by five lemma.

4.21 Let A be a ring, $(f_i)_{i\in I}$ a collection of elements of A with $\sum_{i\in I} f_i A = A$, and M an A-module.

(a) Suppose that $M_{f_i} = 0$ for all $i \in I$. Prove that $M = 0$.

(b) Suppose that M_{f_i} is a finitely generated A_{f_i}-module for each $i \in I$. Prove that M is finitely generated.

(a) Let $f_1 \dots f_n \in I$ such that $\sum_{i=1}^n a_i f_i = 1$ for some $a_1 \dots a_n \in A$. Given $m \in M$. Since $M_{f_i} = 0$, there exists integers n_i such that $f_i^{n_i} m = 0$. Then $m = (\sum_{i=1}^n a_i f_i) m = (\sum_{i=1}^n a_i f_i)^{\sum_{i=1}^n n_i} m = 0$.

(b) Same notation as above $\sum_{i=1}^n a_i f_i = 1$. Let $\{\frac{m_{i,1}}{f_i^{s_1}} \dots, \frac{m_{i,i_m}}{f_i^{s_m}}\}$ be a generating set of M_{f_i}. Then $\{\frac{m_{i,1}}{1}, \dots, \frac{m_{i,i_m}}{1}\}$ also generates M_{f_i}. Then there exists integer N_i such that

$$f_i^{N_i} m \in A[m_{i_1} \dots m_{i,i_m}]$$

(where $A[m_{i_1} \dots m_{i,i_m}]$ is a A-module generated by $\{m_{i1} \dots m_{i,i_m}\}$). Then choose an integer N large enough, we have $m = (\sum_{i=1}^n a_i f_i)^N m \in A[m_{11} \dots m_{1,1_m} \dots m_{n,n_m}]$.

4.22 Let $M = \{q \in \mathbb{Q} : q \text{ has a squarefree denominator}\}$, considered as a module over $A = \mathbb{Z}$. Prove that $M_{\mathfrak{p}}$ is $A_{\mathfrak{p}}$-free module of rank 1 for every prime ideal $\mathfrak{p}$ of A, but that M is not projective over A.

If $p > 0$, observe that $M_p = \frac{1}{p} A_p$. If $p = 0$, then $M_p = \mathbb{Q}$. Then M_p is a free A_p module of rank 1 for every prime ideal p. Since $\mathbb{Z}$ is PID, a module over $\mathbb{Z}$ is projective if and only if it is free. Let us prove that M is not a free $\mathbb{Z}$ module.

Suppose $E \subset M$ is a basis of M, and E only contains one element, say $\frac{q}{p}$ generates M. But prime numbers are infinitely many, so there exists prime g such that $\frac{1}{g} \notin \mathbb{Z} -$ module generated by $\frac{q}{p}$.

So E contains more than one element. Let $\frac{a}{p}, \frac{b}{q} \in E$. But $pb\frac{a}{p} - qa\frac{b}{q} = 0$. Contradiction. Therefore, M is not projective.

4.23 Let V be an infinite set and $A = \mathbb{F}_2^V$ be a ring.

(a) Prove that A has a maximal ideal $\mathfrak{n}$ that is not principal.

(b) Let $M = A/\mathfrak{n}$, with $\mathfrak{n}$ as in (a). Prove that M is finitely generated, that $M_{\mathfrak{m}}$ is $A_{\mathfrak{m}}$-free of rank ≤ 1 for all maximal ideal $\mathfrak{m}$ of A, but that M is not projective.

(a) Let $\mathbf{n} := \oplus_{v\in V} \mathbb{F}_2 \triangleleft A \simeq \prod_{v\in V} \mathbb{F}_2$ be an ideal; it is not principle. This $\mathbf{n}$ is maximal since every non-zero element $f + \mathbf{n}$ in $A/\mathbf{n}$ is of the form $f + \mathbf{n} = I + (f - I) + \mathbf{n}$, where $f(x) = 1$ for all but finitely many $x \in V$ and I denotes the function "$x \mapsto 1$ for all $x \in V$". By definition, $(f - I) \in \mathbf{n}$, so $A/\mathbf{n}$ has only two elements: $0 + \mathbf{n}$ and $I + \mathbf{n}$. So it is isomorphic to a field $\mathbb{F}_2$. So $\mathbf{n}$ is maximal.

(b) Let $\mathbf{n}$ as in (a). Then the A-module $A/\mathbf{n}$ is finitely generated (in fact, it has only two elements). By A is a Boolean ring, localization of $A/\mathbf{n}$ at any maximal ideal $m \triangleleft A$ gives an $\mathbb{F}_2$-module, hence a vector space (of dimension ≤ 1), hence free. . . .

Suppose $M := A/\mathbf{n}$ is projective. The the exact sequence $0 \to \mathbf{n} \to A \to A/\mathbf{n}$ splits, so we get $A \simeq A/\mathbf{n} \oplus \mathbf{n}$ as A-module. . . .

4.24 Let A be a ring and P a finitely generated projective A-module. Prove that A can be written as the product of finitely many rings, $A = A_1 \times \cdots \times A_n$, such that $P = P_1 \times \cdots \times P_n$ where each P_j is a finite generated projective A_j-module of constant rank.

(Reference: http://www.maths.ed.ac.uk/∼aar/papers/kbook.pdf)

Let A be a ring and P a finitely generated projective A-module. The map $r = \operatorname{rank}_A(P) : \operatorname{Spec} A \longrightarrow \mathbb{Z}$ is locally constant and hence continuous. Since $\operatorname{Spec}\mathbb{Z}$ is quasi-compact, the image of r is also quasi-compact, and so r takes on only finitely many values, namely $m_1, \cdots, m_n$. Now each $V_j := r^{-1}(m_j)$ is closed and open due to the discrete topology on $\mathbb{Z}$. It follows that

$$\operatorname{Spec} A = V_1 \sqcup \cdots \sqcup V_n.$$

We want to write each V_j as $\operatorname{Spec} A_j$ such that $A = A_1 \times \cdots \times A_n$.

To do this we may assume that the ring A is reduced. In fact, if N is the nilradical (the ideal of all nilpotent elements in A), then A/N is reduced. Also, we have $\operatorname{Spec} A/N = \operatorname{Spec} A$; and by *idempotent lifting* we know there is an equivalence between the category of finitely generated projective A-modules and the category of finitely generated projective A/N-modules.

Now, let $I_j = \bigcap_{\mathfrak{p}\in V_j} \mathfrak{p}$ be the ideal of V_j and write $A_j = A/I_j$. Then for any i, j with $i \neq j$, we have $V(I_i + I_j) = V(I_i) \cap V(I_j) = \emptyset$. It follows that $I_i + I_j = A$, and $I_1 \cdots I_n = \bigcap_j I_j = 0$. By the Chinese remainder theorem, we have

$$A \simeq A_1 \times \cdots \times A_n$$

Pick $P_j := P \otimes_A A_j$. Then we obtain the desired decomposition.

4.25 Let A be a ring and P a finitely generated projective A-module. Prove that the following four properties are equivalent:

(i) P is faithfully projective;

(ii) the map $A \to \operatorname{End}_{\mathbb{Z}}(P)$ giving the A-module structure is injective;

(iii) P is *faithful*, i.e., an A-module M is zero if and only if $M \otimes P = 0$;

(iv) P is *faithfully flat*, i.e., a sequence $M_0 \to M_1 \to M_2$ of A-modules is exact if and only if the induced sequence $M_0 \otimes P \to M_1 \otimes P \to M_2 \otimes P$ is exact.

(iv)⇒(iii) $0 \to M \to 0$ is exact $\Leftrightarrow$ $0 \to M \otimes P \to 0$ is exact.

(iii)⇒(ii) The map $A \to \operatorname{End}_{\mathbb{Z}}(P)$ is clearly defined by $a \mapsto \left[P \xrightarrow{a} P \right]$. Let $x \in A$ such that $xP = 0$. Consider Ax as A-module. Then, $Ax \otimes P = 0$ implies $Ax = 0$ and $1 \in A$ gives $x = 0$.

(ii)⇒(i) If not, $\exists \mathfrak{p} \in \operatorname{Spec} A$ such that $P_{\mathfrak{p}} = 0$. Since P is finitely generated, let $\{p_i\}_1^n$ be generators. Then, $\frac{p_i}{1} = 0$ implies $\exists x_i \in A - \mathfrak{p}$ such that $x_i p_i = 0$. Thus, $xP = 0$ for $x = \prod_1^n x_i \in A - \mathfrak{p}$ ($\Rightarrow x \neq 0$), contradiction.

(i)⇒(iv) Using the facts that localization is an exact functor (and $\forall \mathfrak{p}$ localization of the sequence is exact implies exact) and it commutes with tensor product and also $P_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module, we obtain:

$$\begin{aligned}
&M_0 \otimes P \longrightarrow M_1 \otimes P \longrightarrow M_2 \otimes P \text{ is exact}\\
\Leftrightarrow\ &(M_0)_{\mathfrak{p}} \otimes (A_{\mathfrak{p}})^n \longrightarrow (M_1)_{\mathfrak{p}} \otimes (A_{\mathfrak{p}})^n \longrightarrow (M_2)_{\mathfrak{p}} \otimes (A_{\mathfrak{p}})^n \text{ is exact } \forall \mathfrak{p}\\
\Leftrightarrow\ &(M_0)_{\mathfrak{p}}^n \longrightarrow (M_1)_{\mathfrak{p}}^n \longrightarrow (M_2)_{\mathfrak{p}}^n \text{ is exact } \forall \mathfrak{p}\\
\Leftrightarrow\ &(M_0)_{\mathfrak{p}} \longrightarrow (M_1)_{\mathfrak{p}} \longrightarrow (M_2)_{\mathfrak{p}} \text{ is exact } \forall \mathfrak{p}\\
\Leftrightarrow\ &M_0 \longrightarrow M_1 \longrightarrow M_2 \text{ is exact}
\end{aligned}$$

4.26 Let P and P' be finitely generated projective modules over a ring A, and $k \in \mathbb{Z}$, $k \geq 0$. Prove that the A-modules $P \oplus P'$, $P \otimes P', \mathrm{Hom}_A(P, P')$, $P^* = \mathrm{Hom}_A(P, A)$, $\bigwedge^k P$, $P^{\otimes k}$ are finitely generated projective, and the ranks of these modules are given by

$$\begin{aligned}
&\mathrm{rank}(P \oplus P') = \mathrm{rank}(P) + \mathrm{rank}(P'),\\
&\mathrm{rank}(P \otimes P') = \mathrm{rank}(P) \cdot \mathrm{rank}(P'),\\
&\mathrm{rank}(\mathrm{Hom}_A(P, P')) = \mathrm{rank}(P) \cdot \mathrm{rank}(P'),\\
&\mathrm{rank}(P^*) = \mathrm{rank}(P),\\
&\mathrm{rank}(\bigwedge^k P) = \binom{\mathrm{rank}(P)}{k},\\
&\mathrm{rank}(P^{\otimes k}) = \mathrm{rank}(P)^k
\end{aligned}$$

as functions on $\mathrm{Spec} A$.

Note that the ranks can be easily computed once we prove that they are finitely generated projective modules, since they are free $A_{\mathfrak{p}}$-modules for every prime $\mathfrak{p}$. We only need to prove for $P \oplus P', P \otimes P', P^*, \wedge^k P$, since $\mathrm{Hom}_A(P, P') \cong P^* \otimes P'$.

To prove a module P is finitely generated projective, one only needs to find a module Q such that $P \oplus Q$ is free of finite rank (converse is also true). Now suppose P and P' are finitely generated projective modules. Then there exists Q and Q' such that $P \oplus Q$ and $P' \oplus Q'$ are free of finite ranks. Then $(P \oplus P') \oplus (Q \oplus Q')$ is free of finite rank.

$(P \oplus Q) \otimes (P' \oplus Q') = (P \otimes P') \oplus [(Q \otimes P') \oplus (P' \otimes Q) \oplus (Q \otimes Q')]$ is free of finite rank.

$(P \oplus Q)^* = P^* \oplus Q^*$ is free of finite rank.

$\bigwedge^k (P \oplus Q) = \bigwedge^k P \oplus [\oplus_{1 \leq l \leq k} (\bigwedge^{k-l} P \otimes \bigwedge^l Q)]$ is free of fintie rank.

4.27 Let P be a fintiely generated A-module such that for each $\mathfrak{p} \in \mathrm{Spec}\, A$ the $A_{\mathfrak{p}}$-module $P_{\mathfrak{p}}$ is free of finte rank $r(\mathfrak{p})$, where $r : \mathrm{Spec}\, A \to \mathbb{Z}$ is continuous. Prove that P is finitely generated projective.

We first try to prove the following statement: $\forall$ maximal ideal $\mathfrak{m}$ of A, $\exists\ f \in A - \mathfrak{m}$ such that P_f is a free A_f-module of finite rank. If this is true, consider the ideal I

generated by all such f. Then, $I \not\subseteq \mathfrak{m}$, $\forall\, \mathfrak{m}$ implies $I = A$ and therefore exists $f_i \in I$ and $a_i \in A$ such that $\sum_{i=1}^{n} a_i f_i = 1$. By 4.6 (iii), we obtain the desired result.

To show this statement, consider a maximal ideal $\mathfrak{m}$ of A. Suppose $r(\mathfrak{m}) = n$ and let $\{y_i\}_{i=1}^{n}$ be the basis of $P_{\mathfrak{m}}$. We can then find $\{x_i\}_{i=1}^{n} \subset P$ such that $x_i = b_i y_i$ for some invertible element b_i in $A_{\mathfrak{m}}$. Let $\{e_i\}$ be the standard basis of A^n and $\eta : A^n \to P$ such that $\eta(e_i) = x_i$. Because P is finitely generated, so is $Q = \operatorname{cok}(\eta)$. Then, by $Q_{\mathfrak{m}} = 0$ and Q is finitely generated, we are able to find $f \in A - \mathfrak{m}$ such that $fQ = 0 \Rightarrow Q_f = 0$. In other words, $\exists\, f$ makes the induced map η_f surjective. We conclude that η_{fg} is also surjective for all $g \in A - \mathfrak{m}$ and by hypothesis, $\exists\, g \in A - \mathfrak{m}$ such that $r(A_{\mathfrak{p}'}) = n$, $\forall\, \mathfrak{p}' \in D(fg)$. Now, replace f by fg, we obtain $(\eta_f)_{\mathfrak{p}'} : (A_f^n)_{\mathfrak{p}'} \to (P_f)_{\mathfrak{p}'}$ is a surjective homomorphism and $(A_f^n)_{\mathfrak{p}'}$, $(P_f)_{\mathfrak{p}'}$ are free modules of the same rank n for all $\mathfrak{p}'$ in A_f. We then conclude $(\eta_f)_{\mathfrak{p}'}$ is a bijective homomorphism for all $\mathfrak{p}'$ and hence so is η_f.

4.28 Let P be a fintiely generated module over a ring A. Prove that P is projective of rank 1 if and only if P is *invertible*, i.e., if and only if $P \otimes Q \cong A$ for some A-module Q. [*Hint* for the "only if" part: take $Q = P^*$.]

Suppose that P is finitely generated projective module of rank 1. Define $f : P \otimes P^* \to A$ by $(x \otimes f \mapsto f(x))$, where $x \in P, f \in P^*$. By Exercise 4.26, P^* is also a finitely generated projective module of rank 1, so both $P_{\mathfrak{p}}$ and $P^*_{\mathfrak{p}}$ are free $A_{\mathfrak{p}}$-module of rank 1 for any $\mathfrak{p} \in \operatorname{Spec} A$, and thus $f_{\mathfrak{p}}$ is an isomorphism, which proves that P is invertible.

Conversely, suppose that $P \otimes Q \cong A$ for some A-module Q. Localizing this isomorphism to each prime ideals, then passing to the residue fields, we can see that $P_{\mathfrak{p}}/\mathfrak{p}P_{\mathfrak{p}}$ is a 1-dimensional $k(\mathfrak{p})$-vector space for any $\mathfrak{p} \in \operatorname{Spec} A$. By Nakayama lemma, $P_{\mathfrak{p}}$ can be generated by a single element. This element is not a torsion since we have $P_{\mathfrak{p}} \otimes Q_{\mathfrak{p}} \cong A_{\mathfrak{p}}$. Hence $P_{\mathfrak{p}}$ is free of rank 1. And by Exercise 4.27, P is projective.

4.29 For a ring A, let $\operatorname{Pic}(A)$ be the set of isomorphism classes of finitely generated projective A-modules of rank 1. Prove that $\operatorname{Pic}(A)$ is an *abelian group* with operation $\otimes_A$, the *Picard group* of A. Express the function $\operatorname{Hom}_A(-,-) : \operatorname{Pic}(A) \times \operatorname{Pic}(A) \to \operatorname{Pic}(A)$ in terms of the group operation.

For any two finitely generated projective A-modules P, Q of rank 1, $P \otimes Q$ is also finitely generated projective of rank 1 by Exercise 4.26. The identity element in $\operatorname{Pic}(A)$ is A. The existence of an inverse element is followed by Exercise 4.28. And $\operatorname{Hom}_A(P, Q) = P^{-1} \otimes Q$ clearly.

4.30 Let A be a ring. The group $K_0 A$ is defined by generators and relations. There is one generator $[P]$ for each finitely generated projective A-module P (up to isomorphism), and one relation $[P \oplus P'] = [P] + [P']$ for each pair P, P' of such modules.

(a) Prove that $[P] = [P']$ if and only if P and P' are *stably isomorphic*, i.e., if and only if $P \oplus A^n \cong P' \oplus A^n$ for some $n \geq 0$.

(b) Prove that $\otimes_A$ induces a multiplication on $K_0 A$ that makes $K_0 A$ into a commutative *ring* with unit element $[A]$.

(c) Show that there are group homomorphisms $\phi : \mathrm{Pic}(A) \to (K_0A)^*$ and $\psi : K_0A \to \mathrm{Pic}(A)$ (the latter from an additive group to a multiplicative group) with $\psi\phi = \mathrm{id}_{\mathrm{Pic}(A)}$. [*Hint:* put $\psi([P]) = [\bigwedge^{\mathrm{rank}(P)} P]$, to be defined in a suitable way if $\mathrm{rank}(P)$ is non-constant.]

(a) If $[P] = [P']$, then there exists finitely generated projective A-modules $Q_1, \dots, Q_m$, such that $P \oplus Q_1 \oplus \cdots \oplus Q_m \cong P' \oplus Q_1 \oplus \cdots \oplus Q_m$. And there exists a finitely generated projective A-module Q such that $Q \oplus Q_1 \oplus \cdots \oplus Q_m \cong A^n$ for some $n \geq 0$, which proves that P and P' are stably isomorphic. The converse is obvious.

(b) Define $[P] \cdot [Q] := [P \otimes Q]$. Firstly, we need to check that if $[P] = [P']$, then $[P \otimes Q] = [P' \otimes Q]$. By (a), $P \oplus A^n \cong P' \oplus A^n$ for some $n \geq 0$. Hence

$$[P \otimes Q] = [(P \oplus A^n) \otimes Q] - [A^n \otimes Q] = [(P' \oplus A^n) \otimes Q] - [A^n \otimes Q] = [P' \otimes Q],$$

so the map is well-defined. The fact that $\otimes_A$ gives a commutative ring structure with unit element $[A]$ is easy to see.

(c) The map ϕ is defined to be the obvious one. Note that ϕ is in fact injective, i.e., stably isomorphic implies isomorphic in rank 1 case. This is a special case of a statement that will be proved later.

To define ψ, given a finitely generated projective module P, consider its rank function $\mathrm{Spec}\, A \to \mathbb{Z}$. $\mathrm{Spec}\, A$ will decompose into finitely many components, where the rank function is constant on each components. Every component is closed in $\mathrm{Spec}\, A$, so we may write down the decomposition as $\mathrm{Spec}\, A = \mathrm{Spec}(A/I_1) \amalg \cdots \amalg \mathrm{Spec}(A/I_n)$. Suppose that P has constant rank k_j on the component $\mathrm{Spec}(A/I_j)$. Then we define $\psi(P) := \bigwedge^{k_1}(P/I_1P) \times \cdots \times \bigwedge^{k_n}(P/I_nP)$. (If $k_j = 0$ for some j, put A/I_j at the j-th place.) Then $\psi(P)$ is finitely generated, and for any prime ideal $\mathfrak{p}$ of A, suppose that $\mathfrak{p}$ is in $\mathrm{Spec}(A/I_j)$. Then $\psi(p)_{\mathfrak{p}} = \bigwedge^{k_j}(P/I_jP)_{\mathfrak{p}}$ is a free $(A/I_j)_{\mathfrak{p}} = A_{\mathfrak{p}}-$module of rank 1 (since $\bigwedge^{k_i}(P/I_iP)_{\mathfrak{p}} = 0 = (A/I_i)_{\mathfrak{p}}$ for $i \neq j$). Hence $\psi(P) \in \mathrm{Pic}(A)$.

Firstly, we show that this definition is independent of the decomposition of $\mathrm{Spec}\, A$, i.e., if P has constant rank k on $\mathrm{Spec}\, A$, and we also have $A = (A/I_1) \times \cdots \times (A/I_n)$, then we show that $\bigwedge^k(P/I_1P) \times \cdots \times \bigwedge^k(P/I_nP) \cong \bigwedge^k P$.

Expand the right hand side, $\bigwedge^k P = \bigwedge^k(P/I_1P \times \cdots \times P/I_nP)$, so we have to show that the "mixed terms" like $\bigwedge^{k-1}(P/I_1P) \otimes \bigwedge^1(P/I_2P)$ are all zero. This follows from a simple observation: $I_1 + I_2 = A$. Suppose that this is false. Then $I_1 + I_2$ is contained in some maximal ideal, which contradict to $\mathrm{Spec}\, A/I_1$ and $\mathrm{Spec}\, A/I_2$ are disjoint.

Now we show that ψ is well-defined on K_0A, i.e., if $P \oplus A^n \cong P' \oplus A^n$, then $\psi(P) = \psi(P')$. Note that P and P' have the same rank, so it is suffices to check on each component. This reduces to the case that, if P and P' are of constant rank k and $P \oplus A^n \cong P' \oplus A^n$, we claim that $\bigwedge^k P \cong \bigwedge^k P'$. Take the determinant line bundle, $\bigwedge^{k+n}(P \oplus A^n) \cong \bigwedge^k P \otimes \bigwedge^n A^n \cong \bigwedge^k P$, which proves the claim.

Finally, we claim that ψ is a group homomorphism, i.e., $\psi(P \oplus Q) \cong \psi(P) \otimes \psi(Q)$. We can find $I_1, \dots, I_n$ such that both P and Q are of constant rank on each $\mathrm{Spec}\, A/I_j$, say the ranks are k_j and l_j. We have to prove that

$$\bigwedge^{k_1+l_1} ((P \oplus Q)/I_1(P \oplus Q)) \times \cdots \times \bigwedge^{k_n+l_n} ((P \oplus Q)/I_n(P \oplus Q))$$

is isomorphic to

$$\left(\bigwedge^{k_1}(P/I_1P)\times\cdots\times\bigwedge^{k_n}(P/I_nP)\right)\otimes\left(\bigwedge^{l_1}(Q/I_1Q)\times\cdots\times\bigwedge^{l_n}(Q/I_nQ)\right).$$

Observe that $\bigwedge^{k_1+l_1}((P\oplus Q)/I_1(P\oplus Q))\cong\bigwedge^{k_1}(P/I_1P)\otimes\bigwedge^{l_1}(Q/I_1Q)$, and the "mixed terms" $\bigwedge^{k_1}(P/I_1P)\otimes\bigwedge^{l_2}(Q/I_2Q)=0$ by $I_1+I_2=A$.

Note that $\psi\phi=\mathrm{id}_{\mathrm{Pic}(A)}$ by our construction.

4.31 Let A be a ring, and H_0A the ring of continuous functions $\operatorname{Spec}A\to\mathbb{Z}$.

(a) Prove the rank: $K_0A\to H_0A$ is a ring homomorphism.

(b) Construct a ring homomorphism $\lambda: H_0A\to K_0A$ such that $\operatorname{rank}\circ\lambda=\mathrm{id}_{H_0A}$.

(c) Let $\tilde{K}_0A=\ker\lambda$.[1] Prove that $K_0A\cong H_0A\oplus\tilde{K}_0A$. *Remark.* It can be proved that $\tilde{K}_0A$ is the nilradical of K_0A; see [4, Proposition IX.4.6].

(a) This is a direct result followed by Exercise 4.26.

(b) Since $\operatorname{Spec}A$ is quasicompact for any commutative ring A, it has only finite connected components U_i. Because every element in H_0A is a continuous function, each U_i corresponds to an integer d_i. Follow by Exercise 4.24, we know A has decomposition as $\prod_{i=1}^n A/I_i$ by Chinese Remainder Theorem, such that $U_i\cong\operatorname{Spec}(A/I_i)$. Now, consider λ defined by $[U_i\mapsto d_i]\mapsto\prod_{i=1}^n(A/I_i)^{d_i}$. Then, clearly, $\operatorname{rank}\circ\lambda=\mathrm{id}_{H_0A}$.

(c) Since the exact sequence

$$0\to\tilde{K}_0A\to K_0A\to H_0A\to 0$$

splits by (b), the claim holds.

4.32 (a) Prove that $\tilde{K}_0A=0$ if A is a field, or a local ring, or a principal ideal domain, or a semilocal ring (i.e., a ring with only finitely many maximal ideals).

(b) Prove that $\tilde{K}_0A\cong\mathrm{Pic}(A)\cong\mathrm{Cl}(A)$, the ideal class group of A, if A is a Dedekind domain.

Note that a general element in $\tilde{K}_0A$ can be written as $[P]-[Q]$, where P and Q are finitely generated projective modules with the same rank function.

(a) If A is a field, then the statement is obviously true since P and Q are simply vector spaces with the same finite dimension. If A is a local ring, then P and Q are free modules with the same finite rank, so we still have $\tilde{K}_0A=0$. If A is a PID, we have the structure theorem for finitely generated modules. Projectivity of the module implies that it does not have torsion part, so finitely generated projective modules over PID are free modules of finite rank, hence $\tilde{K}_0A=0$.

Let A be a semilocal ring, with maximal ideals $\mathfrak{m}_1,\dots,\mathfrak{m}_k$. Then A can not be written as a direct product of more than k nonzero rings, so we may write $A=A_1\times\cdots\times A_r$,

[1] $\tilde{K}_0A=\ker(\text{rank})$.

where each A_j is an indecomposable ring (i.e., with only trivial idempotents). Then each A_j is still semilocal. We may write $P = P_1 \times \cdots \times P_r$, where P_j is a finitely generated projective A_j-module of constant rank, and $A_i \cdot P_j = 0$ for $i \neq j$ (c.f. the proof of Exercise 4.30).

Claim: Let A be a semilocal ring, P a finitely generated projective A-module of constant rank n. Then $P \cong A^n$.

Note that if this claim is true, then the isomorphic class of $P = P_1 \times \cdots \times P_r$ only depends on the rank, which proves that $\tilde{K}_0 A = 0$ in the semilocal case. Now back to the claim. For any $\mathfrak{m}_i$, pick $x_{i1}, \ldots, x_{in} \in P$ such that they form a free basis of $P_{\mathfrak{m}_i}$. Then by Chinese Remainder Theorem, we can find $x_1, \ldots, x_n$, such that $x_j \equiv x_{ij} \pmod{\mathfrak{m}_i P}$. Hence $x_1, \ldots, x_n$ form a basis of $P_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. Now we define $A^n \to P$ which sends the basis e_i to x_i. This map is an isomorphism on every maximal ideal, hence an isomorphism.

(b) By the structure theorem for finitely generated modules over Dedekind domains, P decomposes into torsion part and torsion-free part. The torsion part vanishes due to the projectivity, and the torsion-free part is precisely controlled by the class group, i.e., a finitely generated torsion-free module of rank n is isomorphic to $A^{n-1} \oplus I$, where I is a rank one projective module. (c.f. 4.4 Example (d)) The map $\tilde{K}_0 A \to \mathrm{Pic}(A)$ ...

4.33 Let A be a ring, B an A-algebra and P a projective A-module. Prove that $P \otimes_A B$ is a projective B-module, and that the diagram

$$\begin{tikzcd}
\operatorname{Spec} B \arrow[rr] \arrow[dr, "\mathrm{rank}_B(P \otimes_A B)"'] & & \operatorname{Spec} A \arrow[dl, "\mathrm{rank}_A(P)"] \\
& \mathbb{Z} &
\end{tikzcd}$$

commutes if P is finitely generated.

P is a projective A-module $\Rightarrow \exists\, Q$ an A-module such that $P \oplus Q$ is a free A-module $\Rightarrow (P \oplus Q) \otimes_A B = (P \otimes_A B) \oplus (Q \otimes_A B)$ is a free B-module $\Rightarrow P \otimes_A B$ is a projective B-module. If P is finitely generated as an A-module, so is $P \otimes_A B$ as a B-module. Consider $\mathfrak{p}$ is a prime ideal of B. We would like to prove that $(P \otimes_A B)_{\mathfrak{p}}$ is a free $B_{\mathfrak{p}}$-module of the same finite rank as the free $A_{\mathfrak{q}}$-module $P_{\mathfrak{q}}$, where $\mathfrak{q}$ is the inverse of $\mathfrak{p}$. As in the proof of Exercise 4.27, we are able to find the basis $\{x_i\}_{i=1}^n \subset P$ for the $A_{\mathfrak{q}}$-module $P_{\mathfrak{q}}$. It is then natural to claim that $\{x_i \otimes 1\}_{i=1}^n$ is the basis for $(P \otimes_A B)_{\mathfrak{p}} \cong P_{\mathfrak{q}} \otimes_{A_{\mathfrak{q}}} B_{\mathfrak{p}}$. However, this is certainly true because every element of $P_{\mathfrak{q}} \otimes_{A_{\mathfrak{q}}} B_{\mathfrak{p}}$ has an *unique* representation in the form $\sum_{i=1}^n x_i \otimes b_i$. (This can be obtained by some elementary argument. See [Keith].)

4.34 Prove that any ring homomorphism $f : A \to B$ induces a ring homomorphism $K_0 A \to K_0 B$ via $- \otimes_A B$, and that K_0 is a functor.

Let P be a finitely generated projective A-module. First we claim that $P \otimes_A B$ is a finitely generated projective B-module. Note that there exists an A-module Q such that $P \oplus Q$ is a free A-module of finite rank. Hence $(P \otimes_A B) \oplus (Q \otimes_A B)$ is a free B-module of finite rank, which proves our claim. Since $- \otimes_A B$ commutes with direct sum, it gives a well-defined map $K_0A \to K_0B$. We have $(P \otimes_A P') \otimes_A B \cong (P \otimes_A B) \otimes_B (P' \otimes_A B)$, hence the map is a ring homomorphism. Also, given another ring homomophism $g : B \to C$, we have $K_0(g \circ f) = K_0(g) \circ K_0(f)$, since $(P \otimes_A B) \otimes_B C \cong P \otimes_A C$. Hence K_0 is a functor.

4.35 Let P be a free A-module with basis $w_1, w_2, ..., w_n$, and define $w_i^* \in P^* = \mathrm{Hom}_A(P, A)$ by $w_i^*(w_j) = 1$ if $i = j$ and $w_i^*(w_j) = 0$ if $i \neq j$.

(a) Prove that P^* is a free A-module with basis $w_1^*, w_2^*, ..., w_n^*$.

(b) Let $f : P \to P$ be A-linear, $f(w_i) = \sum_{j=1}^n a_{ij} w_j$ with $a_{ij} \in A$. Prove that $\phi^{-1}(f) = \sum_{i,j} a_{ij} w_i^* \otimes w_j$, where $\phi : P^* \otimes_A P \to \mathrm{Hom}_A(P, P)$ is as in 4.8.

(c) Prove that the traces defined in 1.1 and 4.8 coincide.

(a) Consider any $T \in P^*$ such that $T(w_i) = a_i$. Then, it is clear that $T = \sum_{i=1}^n a_i w_i^*$. If $\sum_{i=1}^n b_i w_i^* = 0$ for some $b_i \in A$, we have $0 = 0(w_j) = \sum_{i=1}^n b_i w_i^*(w_j) = b_j$ showing the linear independence.

(b) Since ϕ is an isomorphism, it suffices to show $\phi(\sum_{i,j} a_{ij} w_i^* \otimes w_j) = f$, which is clearly true by definition.

(c) Followed by 4.8, $\mathrm{Tr}(f) = \sum_{i,j} a_{ij} w_i^*(w_j) = \sum_{i=1}^n a_{ii}$.

4.36 Let A be a ring, B an A-algebra and P a finitely generated projective A-module. Prove that the diagram of natural maps

$$\begin{tikzcd}
\mathrm{End}_A(P) \arrow[r, "\otimes \mathrm{id}_B"] \arrow[d, "\mathrm{Tr}_{P/A}"'] & \mathrm{End}_B(P \otimes_A B) \arrow[d, "\mathrm{Tr}_{P \otimes_A B/B}"] \\
A \arrow[r] & B
\end{tikzcd}$$

is commutative.

Note that $\mathrm{End}_A(P) = P^* \otimes P$. Given $f \in P^*, p \in P$,

$$\begin{tikzcd}
f \otimes p \arrow[r, mapsto] \arrow[d, mapsto] & (f \otimes 1) \otimes (p \otimes 1) \arrow[d, mapsto] \\
f(p) \arrow[r, mapsto] & \phi(f(p)) = f(p) \otimes 1
\end{tikzcd}$$

4.37 Let A be a ring and P a finitely generated projective A-module.

(a) Suppose that P has constant rank n. Prove that $\mathrm{Tr}_{P/A}(\mathrm{id}_P) = n \cdot 1 \in A$.

(b) In the general case, prove that $\mathrm{Tr}_{P/A}(\mathrm{id}_P)$ is the image of $\mathrm{rank}(P)$ under the natural map $H_0A \to \Gamma(\mathrm{Spec}\, A, \mathcal{O}) \cong A$; here H_0A is as in Exercise 4.31, the sheaf $\mathcal{O}$ is the natural sheaf of rings on Spec A (see [10, Chapter II, Section 2]), the map $H_0A \to \Gamma(\mathrm{Spec}\, A, \mathcal{O})$ is induced by the ring homomorphisms $\mathbb{Z} \to A_{\mathfrak{p}}$, and $\Gamma(\mathrm{Spec}\, A, \mathcal{O}) \cong A$ is the isomorphism from [10, Chapter II, Proposition 2.2].

For (a), if P has constant rank n, then for any prime ideal $\mathfrak{p}$, we have $\operatorname{rank}(P_{\mathfrak{p}}) = n$. Note that now $P_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of rank n. Using the previous exercise (Exercise 4.33) with $B = A_{\mathfrak{p}}$, we have that $\operatorname{Tr}_{P/A}(\mathrm{id}_P)$ equals to n in every localization $A_{\mathfrak{p}}$. So $\operatorname{Tr}_{P/A}(\mathrm{id}_P) = n \in A$.

Let $\Phi : H_0 A \to \Gamma(\operatorname{Spec} A, \mathcal{O})$. Note that $\operatorname{Tr}_{P/A}(\mathrm{id}_P)$ and $\Phi(\operatorname{rank}(P))$ are elements in A. To prove they are equal, it suffices to show that they are equal under every localization $A_{\mathfrak{p}}$. Suppose P has constant rank. Then (b) follows from (a). If P does not have constant rank, then use Exercise 4.24. This completes the proof.

4.38 Let A be a ring, $0 \to P_0 \to P_1 \to P_2 \to 0$ an exact sequence of A-modules in which P_1 and P_2 are finitely generated projective, and $g : P_1 \to P_1$ an A-linear map with $g[P_0] \subset P_0$. Denote by h the induced map $P_2 \to P_2$. Prove that P_0 is finitely generated projective and $\operatorname{Tr}_{P_1/A}(g) = \operatorname{Tr}_{P_0/A}(g \mid P_0) + \operatorname{Tr}_{P_2/A}(h)$.

Since P_2 is projective, the exact sequence splits. Hence there exists an exact sequence

$$0 \to P_2 \to P_1 \to P_0 \to 0.$$

So P_0 is finitely generated. It is projective since it is a direct summand of a projective module. For the trace formula, we firstly localized at $\mathfrak{p}$. We may assume P_i's are free. Thus, the assertion follows from the standard fact from linear algebra.

4.39 Let P and Q be two finitely generated projective A-modules, and $f : P \to Q$, $g : Q \to P$ two A-linear maps. Prove that $\operatorname{Tr}_{Q/A}(f \circ g) = \operatorname{Tr}_{P/A}(g \circ f)$.

Since the trace map commutes with localization, we may prove this equality under localization at arbitrary prime ideal $\mathfrak{p}$. We may assume A is local. But then $P \cong A^m$ and $Q \cong A^n$. Now this is a consequence in linear algebra.

4.40 (a) Let P be a finitely generated projective A-module. Prove that the map $\psi : \operatorname{End}_A(P) \to \operatorname{End}_A(P^*)$ defined by $\psi(f)(g) = g \circ f$ is an anti-isomorphism of not necessarily commutative rings, and that $\operatorname{Tr}_{P^*/A}(\psi(f)) = \operatorname{Tr}_{P/A}(f)$.

(b) Let $f : P \to P$ and $g : Q \to Q$ be endomorphisms of finitely generated projective A-modules P and Q. Prove that $\operatorname{Tr}_{P\otimes Q/A}(f \otimes g) = \operatorname{Tr}_{P/A}(f) \cdot \operatorname{Tr}_{Q/A}(g)$.

As in the previous exercise, we may assume A is local, so P and P^* are free A-modules. Let $e_1, \cdots e_n$ be a basis of P and $e_1^*, \cdots, e_n^*$ be the dual basis of P^*. So under the matrix representation, f corresponds to a matrix M and $\psi(f) = M^t$. Now the result follows from a direct computation. This proves (a).

For the statement (b), let $e_1, \cdots, e_n$ be a basis of P and $d_1, \cdots, d_m$ be the one of Q. Under these bases, f has a matrix representation M and g has a matrix representation N. Then $f \otimes g$ has a matrix representation $M \otimes N$. Now the theorem follows from a basic fact from linear algebra.

4.41 Let $B_1, B_2, \ldots, B_n$ be algebras over a ring A. Prove that $\prod_{i=1}^n B_i$ is a finite projective A-algebra if and only if each B_i is a finite projective A-algebra.

It is clear that $\prod_{i=1}^n B_i$ is a finite A-algebra if and only if each B_i is. It remains to show that, when regarded as A-modules, $\prod_{i=1}^n B_i$ is projective if and only if so is each B_i.

Let $B_1, \cdots, B_n$ be projective. For any A-epimorphism $f : M \longrightarrow N$ and any A-linear map $g : \prod_{i=1}^n B_i \longrightarrow N$, consider the map $g|_{B_i} : B_i \longrightarrow N$ which is A-linear. By the projectiveness of B_i there is an A-linear map $h_i : B_i \longrightarrow M$ such that $g|_{B_i} = f \circ h_i$. Setting $h = \prod_{i=1}^n h_i$, we have $g = f \circ h$. Hence $\prod_{i=1}^n B_i$ is projective.

Now we suppose that $\prod_{i=1}^n B_i$ is projective. Let $f : M \longrightarrow N$ be an A-epimorphism and $g_j : B_j \longrightarrow N$ an A-linear map. Define $g^j : \prod_{i=1}^n B_i \longrightarrow N$ as $g^j = g_j \circ p_j$, where $p_j : \prod_{i=1}^n B_i \longrightarrow B_j$ is the natural projection. Since $\prod_{i=1}^n B_i$ is projective, there exists an A-linear map $h^j : \prod_{i=1}^n B_i \longrightarrow M$ such that $g^j = f \circ h^j$. Note that in the category of A-modules, finite products coincide with finite sums. Let $\iota_j : B_j \longrightarrow \prod_{i=1}^n B_i$ be the inclusion. Choose $h_j = \iota_j \circ h^j$. Then we have $g_j = f \circ h_j$. This shows each B_j is projective.

4.42 Let A be a ring, B a finite projective A-algebra, and P a finitely generated projective B-module. Prove that P, when considered as an A-module, is finitely generated and projective. Prove also that the map $\mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(P, B) \to \mathrm{Hom}_A(P, A)$ sending $f \otimes g$ to $f \circ g$ is *surjective.*

Since P is a finitely generated projective B-module, by Exercise 4.3, there exists a finitely generated B-module Q such that $P \oplus Q \simeq B^{\oplus n}$ for some finite n. And since B is a finite projective A-algebra, there is a finitely generated A-module C such that $B \oplus C \simeq A^{\oplus m}$ for some finite m, when B is considered as an A-module. Then,

$$P \oplus Q \oplus C^{\oplus n} \simeq B^{\oplus n} \oplus C^{\oplus n} \simeq (A^{\oplus m})^{\oplus n} = A^{\oplus mn},$$

where $Q \oplus C^{\oplus n}$ is a finitely generated A-module. Again by 4.3 we know P can be regarded as a finitely generated projective A-module.

For the second part, let

$$\theta : \mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(P, B) \longrightarrow \mathrm{Hom}_B(P, \mathrm{Hom}_A(B, A))$$

be the map given by

$$\theta(f \otimes g)(p)(b) = f(g(bp)),$$

where $f \in \mathrm{Hom}_A(B, A)$, $g \in \mathrm{Hom}_B(P, B)$, $p \in P$ and $b \in B$. One can easily check that it is a well-defined B-linear map. We claim that θ is an isomorphism. Indeed, if $P = B$, then both sides of θ are isomorphic to $\mathrm{Hom}_A(B, A)$, and θ is clearly induced from the identity map. It can be generalized to the case in which $P = B^{\oplus n}$ for some finite n since finite direct sums commute with both tensor products and Hom functors. It follows that θ is an isomorphism for any finitely generated projective B-module P since P is a direct summand for some $B^{\oplus n}$ of finite rank.

Now we define

$$\phi : \mathrm{Hom}_B(P, \mathrm{Hom}_A(B, A)) \longrightarrow \mathrm{Hom}_A(P, A)$$

to be the map given by

$$\phi(k)(p) = k(p)(1_B),$$

where $k \in \mathrm{Hom}_B(P, \mathrm{Hom}_A(B, A))$ and $p \in P$. Then $\psi = \phi \circ \theta$. Moreover, ϕ is a surjection since each $h \in \mathrm{Hom}_A(P, A)$ is the image of the B-linear map $k : P \longrightarrow \mathrm{Hom}_A(B, A)$ defined by $k(p)(b) = h(bp)$. Hence ψ is surjective.

4.45 Let $B_1, B_2, \ldots, B_n$ be algebras over a ring A. Prove that $\prod_{i=1}^n B_i$ is a projective separable A-algebra if and only if each B_i is a projective separable A-algebra.

In Exercise 4.41, we have seen that $\prod_{i=1}^n B_i$ is a finite projective A-algebra if and only if each B_i is a finite projective A-algebra. It remains to show that the map

$$\phi : \prod_{i=1}^n B_i \longrightarrow \mathrm{Hom}_A\left(\prod_{i=1}^n B_i, A\right)$$

given by $\phi((b_i)_{1\le i\le n})((b'_i)_{1\le i\le n}) = \mathrm{Tr}_{\prod B_i/A}((b_i b'_i)_{1\le i\le n})$ is an isomorphism if and only if each

$$\phi_i : B_i \longrightarrow \mathrm{Hom}_A(B_i, A)$$

given by $\phi_i(b_i)(b'_i) = \mathrm{Tr}_{B_i/A}(b_i b'_i)$ is an isomorphism.

Considering each B_i as an A-module, we have the natural isomorphism $\prod_{i=1}^n B_i = \coprod_{i=1}^n B_i$, and hence the canonical

$$\mathrm{Hom}_A\left(\prod_{i=1}^n B_i, A\right) \simeq \prod_{i=1}^n \mathrm{Hom}_A(B_i, A).$$

So it suffices to check that

$$\mathrm{Tr}_{\prod_{i=1}^n B_i/A}((b_i b'_i)_{1\le i\le n}) = \sum_{i=1}^n \mathrm{Tr}_{B_i/A}(b_i b'_i).$$

In fact, for $n = 2$, it is just the result of Exercise 4.38; by using an induction argument we can show that the identity holds for a general n.

4.46 Let A be a ring, B a projective separable A-algebra and C a projective separable B-algebra. Prove that C is a projective separable A-algebra. [*Hint:* use Exercises 4.42 and 4.44. In 5.12 we shall give a different proof.]

Since B and C are projective separable algebra over A and over B, respectively, we know they are finite over their base rings; and the maps

$$\phi_{B/A} : B \longrightarrow \mathrm{Hom}_A(B, A) \quad \text{and} \quad \phi_{C/B} : C \longrightarrow \mathrm{Hom}_B(C, B)$$

defined by $\phi_{B/A}(b)(b') = \mathrm{Tr}_{B/A}(bb')$ and $\phi_{C/B}(c)(c') = \mathrm{Tr}_{C/B}(cc')$ are isomorphisms over A and over B, respectively. By Exercise 4.43, C is then a finite projective A-algebra. It remains to show that the map

$$\phi_{C/A} : C \longrightarrow \mathrm{Hom}_A(C, A)$$

given by $\phi_{C/A}(c)(c') = \mathrm{Tr}_{C/A}(cc')$ is an A-linear isomorphism.

Note that $\phi_{C/A}$ can be factorized as the chain

$$C = B \otimes_B C \xrightarrow{\phi_{B/A} \otimes \phi_{C/B}} \mathrm{Hom}_A(B, A) \otimes_B \mathrm{Hom}_B(C, B) \xrightarrow{\psi} \mathrm{Hom}_A(C, A),$$

where ψ is map $f \otimes g \mapsto f \circ g$. In fact, for any $c, c' \in C$, we have

$$\psi(\phi_{B/A} \otimes \phi_{C/B}(1 \otimes c))(c') = \mathrm{Tr}_{B/A}(\mathrm{Tr}_{C/B}(cc')) = \mathrm{Tr}_{C/A}(cc') = \phi_{C/A}(c)(c')$$

by applying the result in Exercise 4.44. Also, we know that $\phi_{B/A} \otimes \phi_{C/B}$ is an isomorphism, and that ψ is a surjection from Exercise 4.42. It now suffices to show that $\phi_{C/A}$ is injective. Suppose that $\phi_{C/A}(c) = 0$, or that $\mathrm{Tr}_{C/A}(cc') = 0$ for all $c' \in C$. ...

4.47 Let A be a ring, B a projective separable A-algebra and C any A-algebra. Prove that $B \otimes_A C$ is a projective separable C-algebra.

It follows from the given condition that $B \otimes_A C$ is a finite projective C-algebra by Exercise 4.33. So now it suffices to check that the map

$$\bar{\phi} : B \otimes_A C \longrightarrow \mathrm{Hom}_C(B \otimes_A C, C)$$

given by $\bar{\phi}(b \otimes c)(b' \otimes c') = \mathrm{Tr}_{B \otimes_A C/C}(bb' \otimes cc')$ is an isomorphism. Let

$$\phi : B \longrightarrow \mathrm{Hom}_A(B, A)$$

be the isomorphism given by the separability of B over A so that $\phi(b)(b') = \mathrm{Tr}_{B/A}(bb')$. Suppose

$$\theta : \mathrm{Hom}_A(B, A) \otimes_A C \longrightarrow \mathrm{Hom}_C(B \otimes_A C, C)$$

is the C-linear map such that $\theta(f \otimes c)(b \otimes c') = f(b)cc'$. We claim that the following diagram commutes:

$$\begin{tikzcd}
B \otimes_A C \arrow[r, "\phi \otimes \mathrm{id}_C"] \arrow[dr, "\bar{\phi}"'] & \mathrm{Hom}_A(B, A) \otimes_A C \arrow[d, "\theta"] \\
 & \mathrm{Hom}_C(B \otimes_A C, C)
\end{tikzcd}$$

and that θ is an isomorphism. Indeed, we have

$$\begin{aligned}
\theta((\phi \otimes \mathrm{id}_C)(b \otimes c))(b' \otimes c') &= \theta(\phi(b) \otimes c)(b' \otimes c') \\
&= \mathrm{Tr}_{B/A}(bb')cc' \\
&= \mathrm{Tr}_{B \otimes_A C/C}(bb' \otimes cc'),
\end{aligned}$$

where the third equality follows from Exercise 4.36. This proved the commutativity of the diagram. ...

5 Exercises for Section 5

5.1 Let X be a scheme and $d : X \to \mathbb{Z}$ any continuous function that assumes only non-negative values. Prove that there exists a finite and locally free morphism $Y \to X$ such that $d = [Y : X]$.

Decompose X into disjoint connected components $X = \amalg X_i$. Then the continuous function d is constant on each X_i, say d_i. We simply define $Y = \amalg(\amalg_{1 \le k \le d_i} X_i^{(k)})$, where $X_i^{(k)}$ is a copy of X_i, and $Y \to X$ maps each $X_i^{(k)}$ to X_i.

5.2 Let $Y \to X$ be a finite and locally free morphism. Prove that the underlying map $\mathrm{sp}(Y) \to \mathrm{sp}(X)$ is open and closed.

It is suffice to check locally since $Y \to X$ is finite. Let B be a finitely generated projective A-algebra via $\phi : A \to B$, we want to show that $f : \operatorname{Spec} B \to \operatorname{Spec} A$ is open and closed. We may assume that $\operatorname{Spec} A$ is connected, so B has constant rank on A, and assume that $B \neq 0$. Hence $\phi : A \to B$ is injective.

To show that f is closed, let I be an ideal in B, we claim that $f(V(I)) = V(\phi(I))$. So, if $\phi^{-1} I \subset \mathfrak{p} \in \operatorname{Spec} A$, we want to show that there exists $I \subset \mathfrak{q} \in \operatorname{Spec} B$ such that $\phi^{-1}\mathfrak{q} = \mathfrak{p}$. Since B over A is finite, ϕ is in fact an integral extension. Hence $\bar{\phi} : A/\phi^{-1}I \to B/I$ is also an integral extension, and the closedness of f follows from the going-up property.

To show that f is open, we are going to use several facts.

Fact: A subset of $\operatorname{Spec} A$ is open if and only if it is constructible and stable under generalization.

Fact: (Chevalley's theorem) If $\phi : A \to B$ is finitely presented, then the image of a constructible subset of $\operatorname{Spec} B$ is a constructible subset of $\operatorname{Spec} A$.

Fact: Finitely generated projective implies finitely presented. (Theorem 4.6)

Combining these facts, in order show that f is open, it is suffice to show that for any distinguished open subset $D(g)$ of $\operatorname{Spec} B$, $f(D(g))$ is stable under generalization, i.e., if $\mathfrak{p} \in f(D(g))$ and $\mathfrak{p} \in \overline{\{\mathfrak{p}'\}}$ (equivalently, $\mathfrak{p}' \subset \mathfrak{p}$), then $\mathfrak{p}' \in f(D(g))$. So there exists $g \notin \mathfrak{q} \in \operatorname{Spec} B$ such that $\mathfrak{p} = \phi^{-1}(\mathfrak{q})$. Since $\phi : A \to B$ is a finite projective extension, it is in particular a flat extension. Hence $A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ is also a flat extension. By going down, there exists $\mathfrak{q}' \subset \mathfrak{q}$ such that $\mathfrak{p}' = \phi^{-1}(\mathfrak{q}')$. Since $g \notin \mathfrak{q}'$, this proves the openness.

5.3 Let $f_i : Y_i \to X$ be a morphism of schemes, for $1 \le i \le n$, and $f : Y = Y_1 \amalg \cdots \amalg Y_n \to X$ the induced morphism. Prove that $Y \to X$ is finite and locally free if and only if each $Y_i \to X$ is finite and locally free. Prove also that $[Y : X] = \sum_{i=1}^{n} [Y_i : X]$ if $Y \to X$ is finite and locally free.

Note that if U is an open affine subset of $Y = Y_1 \amalg \cdots \amalg Y_n$, then $U \cap Y_i$ is a closed subset of U for all i, hence is also affine. So by Prop. 5.2, the first statement is equivalent to: B_i is a finite projective A-algebra for all $1 \le i \le n$ if and only if $B_1 \times \cdots \times B_n$ is a finite projective A-algebra, which is precisely Exercise 4.41.

For the second statement, suppose that $\operatorname{Spec} A$ is an connected open affine subset of X. Then its preimage is $\operatorname{Spec} B_1 \amalg \cdots \amalg \operatorname{Spec} B_n$, where B_i is a finite projective A-algebra of constant rank for all $1 \le i \le n$, and the rank of $B_1 \times \cdots \times B_n$ is simply the sum of the ranks of all B_i.

5.4 Let $(X_i)_{i\in I}$ be a collection of schemes, and $Y_i \to X_i$ a finite and locally free morphism, for each $i \in I$. Prove that the induced morphism $\amalg_{i\in I} Y_i \to \amalg_{i\in I} X_i$ is finite and locally free, and that each finite and locally free morphism $Y \to \amalg_{i\in I} X_i$ is obtained in this way. Prove also that $[\amalg_{i\in I} Y_i : \amalg_{i\in I} X_i]$ equals $[Y_j : X_j]$ when restricted to $\mathrm{sp}(X_j)$, for each $j \in I$.

Only the statement "each finite and locally free morphism $Y \to \amalg_{i\in I} X_i$ is obtained in this way" is less obvious. Decompose Y into $\amalg Y_i$ according to its image, we want to show that each $Y_i \to X_i$ is finite and locally free. By Prop. 5.2, it is suffices to show that for any affine open subset $\operatorname{Spec} A$ of X_i, its preimage is also affine, say $\operatorname{Spec} B$, and B is a finite projective A-algebra. But this follows from $Y \to \amalg X_i$ is finite and locally free.

5.5 Let $f : Y \to X$ be a finite and locally free morphism of schemes, and let $W \to X$ be any morphism of schemes.

(a) Prove that $p : Y \times_X W \to W$ is finite and locally free.

(b) Prove the diagram

$$\begin{tikzcd}
\mathrm{sp}(W) \arrow[rr] \arrow[dr, "{[Y\times_X W:W]}"'] & & \mathrm{sp}(X) \arrow[dl, "{[Y:X]}"] \\
& \mathbb{Z} &
\end{tikzcd}$$

is commutative.

(c) Suppose that $Y \to X$ is surjective. Prove that $Y \times_X W \to W$ is surjective.

(a) There exists an open affine cover $\{U_i = \operatorname{Spec} A_i\}$ of X such that $f^{-1}(U_i) = \operatorname{Spec} B_i$ is affine and B_i is a free A_i-module of finite rank. And there is an affine open cover $\{V_j = \operatorname{Spec} C_j\}$ of W such that every $f(\operatorname{Spec} C_j)$ is contained in some $\operatorname{Spec} A_i$. So $p^{-1}(\operatorname{Spec} C_j) = \operatorname{Spec}(B_i \otimes_{A_i} C_j)$ is affine and $B_i \otimes_{A_i} C_j$ is a free C_j-module of finite rank, which is the rank of B_i over A_i.

(b) follows from the proof of (a).

(c) Surjectivity is stable under base change in general case. It is suffice to prove the following claim:

Claim: Given fiber product

$$\begin{tikzcd}
Y \times_X W \arrow[r, "p"] \arrow[d, "q"'] & W \arrow[d, "g"] \\
Y \arrow[r, "f"'] & X,
\end{tikzcd}$$

we have $g^{-1}(f(Z)) = p(q^{-1}(Z))$ for any $Z \subset Y$.

By definition, $x \in g^{-1}(f(Z))$ if and only if there exists $y \in Z$ such that $g(x) = f(y)$. So it is suffice to prove the following claim:

Claim: If $x \in W, y \in Y$ satisfies $g(x) = f(y) = s$, then there exists $u \in Y \times_X W$ such that $p(u) = x, p(u) = y$.

We have the following diagram:

$$\begin{tikzcd}
\mathrm{Spec}(k(x) \otimes_{k(s)} k(y)/\mathfrak{m}) \arrow[r] \arrow[d] & \mathrm{Spec}(k(x)) \arrow[r] \arrow[d] & W \arrow[dd] \\
\mathrm{Spec}(k(y)) \arrow[r] \arrow[d] & \mathrm{Spec}(k(s)) \arrow[dr] & \\
Y \arrow[rr] & & X
\end{tikzcd}$$

where $\mathfrak{m}$ is any maximal ideal of $k(x) \otimes_{k(s)} k(y)$.

So this induces a morphism from $\mathrm{Spec}(k(x) \otimes_{k(s)} k(y)/\mathfrak{m})$ to the fiber product $Y \times_X W$, and the image of this morphism gives the desired $u \in Y \times_X W$.

5.7 Let $Y \to X$ and $Z \to X$ be finite and locally free morphisms of schemes.

(a) Prove that $Y \times_X Z \to X$ is finite and locally free.

(b) Prove that $[Y \times_X Z : X] = [Y : X] \cdot [Z : X]$.

(c) Prove that $Y \times_X Z \to X$ is surjective if $Y \to X$ and $Z \to X$ are surjective.

(a) follows from Exercises 5.5(a) and 5.6.

(b) $[Y \times_X Z : X] = [Y \times_X Z : Z] \cdot [Z : X] = [Y : X] \cdot [Z : X]$ by Exercises 5.5(b) and 5.6.

(c) follows from Exercise 5.5(c).

5.8 Do Exercise 5.1-5.7 with everywhere “finite and locally free” replaced by“finite étale”.

The construction of 5.1 is still valid. 5.2 is still true. In 5.3, we should replace the usage of Prop. 5.2 by Prop. 5.8. Then it is suffices to show that B_i is a projective separable A-algebra for all $1 \leq i \leq n$ if and only if $B_1 \times \cdots \times B_n$ is a projective separable A-algebra, which is precisely Exercise 4.45. The argument of 5.4 is still valid, after replacing Prop. 5.2 by Prop. 5.8. For 5.5(a), we need to show that if B is a projective separable A-algebra, then $B \otimes_A C$ is a projective separable C-algebra, which is Exercise 4.47. And 5.5(b)(c) are still true. For 5.6, we have to show that if B is a projective separable A-algebra and C a projective separable B-algebra, then C is a projective separable A-algebra, which is Exercise 4.46. Finally, the argument of 5.7 is still valid.

6 Exercises for Section 6

6.1 A module M over a domain A is called *torsionfree* if for every non-zero $a \in A$ and every non-zero $x \in M$ one has $ax \neq 0$.

(a) Prove that a flat module over a domain is torsionfree.

(b) Let A be a Dedekind domain. Prove that any torsionfree A-module can be written as an injective limit of finitely generated projective A-modules, and that an A-module is flat if and only if it is torsionfree.

(a). Let M be flat, so the functor $M\otimes_A$ is exact. Let $a \neq 0$, $a \in A$, consider the module homomorphism $A \to A$ via $r \mapsto ar$. This is injective by A is a domain. Tensoring the functor, by M is flat, we have again an injection:

$$M \otimes_A A \to M \otimes_A A$$

via $m \mapsto am$. So M is torsion free.

For (b), let A be Dedekind. We have to prove if M is a torsion free A-module, then M is flat. Since any element $x \in M$ is contained in a finitely generated submodule of M (e.g. $Ax \leq M$), and $\{M_i \subseteq M |\ M_i \text{ a finite generated submodule }\}_{i\in I}$ with respect to inclusion form an injective system, hence $M = \varinjlim_i M_i$. Now by A is Dedekind and M_i is finitely generated torsionfree for all $i \in I$. Hence M_i are projective, hence flat. By taking direct limit is an exact functor in module theory, we get M is flat.

6.2 Prove Proposition 6.3: Let $f : Y \to X$ be a morphism of schemes. Then the following four assertions are equivalent:

(i) f is flat;

(ii) for any pair of open affine subsets $V = \operatorname{Spec} B \subset Y$, $U = \operatorname{Spec} A \subset X$ with $f[V] \subset U$ the induced ring homomorphism $A \to B$ is flat;

(iii) there is a covering of Y by open affine subsets $V_i = \operatorname{Spec} B_i$ such that for each i there is an open affine subset $U_i = \operatorname{Spec} A_i \subset X$ with $f[V_i] \subset U_i$ for which the induced ring homomorphism $A_i \to B_i$ is flat;

(iv) for every closed point $y \in Y$ the induced ring homomorphism $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is flat.

(i) $\Rightarrow$ (ii) $\mathcal{O}_Y|_V \cong B$ and $\mathcal{O}_X|_U \cong A$. Then, the statement is equivalent to Proposition 6.2 (iii) $\Rightarrow$ (i).

(ii) $\Rightarrow$ (iii) X is a scheme covered by open affine subsets $U_i = \operatorname{Spec} A_i$. Consider the open subset $f^{-1}(U_i)$, which can be also covered by affine subsets V_{ij}. Since the collection of $f^{-1}(U_i)$ covers Y, all V_{ij} form an affine open covering of Y satisfying the condition $f[V_{ij}] \subset U_i$. Then, by (ii), the statement that the induced ring homomorphism is flat immediately follows.

(iii) $\Rightarrow$ (iv) $\Rightarrow$ (i) Equivalent to Proposition 6.2 (i) $\Rightarrow$ (iv) $\Rightarrow$ (ii).

6.3 Let $f : Y \to X$ be a morphism of schemes. Prove that f is finitely presented (as in 6.4) if and only if for every open affine subset $U = \operatorname{Spec} A \subset X$ the open subscheme $f^{-1}[U] \subset Y$ is affine, $f^{-1}[U] = \operatorname{Spec} B$, where B is an A-algebra that is finitely presented as an A-module.

The "if" part follows from definition. Now suppose that there exists a covering of X by open affine subsets $U_i = \operatorname{Spec} A_i$, such that for each i the open subscheme $f^{-1}(U_i) = \operatorname{Spec} B_i$, where B_i is an A_i-algebra that is finitely presented as an A_i-module.

Let $U = \operatorname{Spec} A \subset X$ be an affine open subset of X. For each U_i, $U \cap U_i$ can be covered by distinguished open sets $\{\operatorname{Spec}(A_i)_{f_j} | j \in J\}$ for some $f_j \in A_i$ and index set J. Observe that $f^{-1}(\operatorname{Spec}(A_i)_{f_j}) = \operatorname{Spec}(B_i)_{\phi(f_j)}$, where ϕ is the map from A_i to B_i induced by f. Also observe that $(B_i)_{\phi(f_j)}$ is finitely presented $(A_i)_{f_j}$-module. So we have reduce to proving the statement for X is affine, say $X = \operatorname{Spec} A$.

$U_i = \operatorname{Spec} A_i$ can be covered by distinguished open subsets $\operatorname{Spec} A_f$, observe that if $\phi : A \to A_i$ is the map induced by the inclusion $U_i \to X$, then $A_f \cong (A_i)_{\phi(f)}$. Using the fact that the underlying topology of an affine scheme is quasi-compact, we have reduce to proving the following statement: Let $X = \operatorname{Spec} A$, $X = \cup_{1 \leq i \leq n} U_i$, where $U_i = \operatorname{Spec} A_{f_i}$ (so $f_1, \cdots, f_n$ generates A), $f^{-1}(U_i) = \operatorname{Spec} B_i$, and B_i is a finitely presented A_{f_i}-module. Aim to show that Y is affine(say $\operatorname{Spec} B$), and B is a finitely presented A-module.

To show that Y is affine, we use the affineness criterion in [Hartshorne, Algebraic Geometry]: Let $B = \Gamma(Y, \mathcal{O}_Y)$. Then Y is affine if and only if there exists $g_1, \cdots, g_m \in B$ such that $Y_{g_i} := \{y \in Y | (g_i)_y \notin m_y\}$ are affine for all $1 \leq i \leq m$, and $g_1, \cdots, g_m$ generates B.

Let $\phi : A \to B$ be the map induced by $f : Y \to X$, we define $g_i = \phi(f_i)$.

Claim: $Y_{g_i} = \operatorname{Spec} B_i$.

$y \in \operatorname{Spec} B_i$ if and only if $f(y) \in \operatorname{Spec} A_{f_i}$ if and only if $f_i \notin f(y)$ if and only if $(f_i)_{f(y)} \notin m_{f(y)}$ if and only if $(g_i)_y \notin m_y$. The last "if and only if" is because the induced map between local rings is local homomorphism.

These $g_1, \cdots, g_n$ generates B since $f_1, \cdots, f_n$ generates A. Hence the affineness criterion is checked, so $Y = \operatorname{Spec} B$. Finally, we reduce to proving the following algebraic problem: Let $f_1, \ldots, f_n$ genereates A, M a A-module. If M_{f_i} is finitely presented for every i, then so is M.

Claim: If M_{f_i} are finitely generated, then so is M.

Let $x_{i_1}, \ldots, x_{i_{k_i}} \in M$ generates M_{f_i}, we claim that these x_{i_j} generates M. Given any $y \in M$, there exists N large enough such that $f_i^N y$ are generated by x_{i_j} for all i. Observe that $f_1^N, \ldots, f_n^N$ also generates A, which proves the claim.

By simple diagram chasing, one can show that if N is finitely presented A-module, then for any $A^{\oplus n} \to N \to 0$, the kernel is finitely generated. Apply to our case, we already know that M is finitely generated, write $K \to A^{\oplus l} \to M \to 0$, we want to show that K is finitely generated. Localize to each f_i, by the diagram-chasing-fact that just mentioned, K_{f_i} is finitely generated, hence by our claim again, K is finitely generated. Hence M is finitely presented.

6.8 Let $A = \prod_{i \in I} k_i$ be the product of an infinite collection $(k_i)_{i \in I}$ of fields, and $\mathfrak{a} = \{(x_i)_{i \in I} \in A : x_i = 0 \text{ for almost all } i \in I\}$. Prove that the morphism $\operatorname{Spec} A/\mathfrak{a} \to \operatorname{Spec} A$ is finite and étale, but not finite étale.

Certainly, $A/\mathfrak{a}$ is a finitely generated A-module generated by $1 + \mathfrak{a}$. However, the kernel $\mathfrak{a}$ has infinitely many independent generators e_j with $x_i = \delta_i^j$, so there is no possibility for $\mathfrak{a}$ to be finitely generated. Hence, $A/\mathfrak{a}$ is NOT finitely presented and the morphism is NOT finite étale. It remains to show the morphism is flat and unramified. $(A/\mathfrak{a})_{\mathfrak{p}/\mathfrak{a}} \cong (A - \mathfrak{p})^{-1}(A/\mathfrak{a}) \cong A/\mathfrak{a} \otimes_A A_{\mathfrak{p}} \cong A_{\mathfrak{p}}/\mathfrak{a}A_{\mathfrak{p}}$, $\forall\, \mathfrak{p} \in \operatorname{Spec} A \Rightarrow$

$$A_{\mathfrak{p}}/\mathfrak{p} \cong (A_{\mathfrak{p}}/\mathfrak{a}A_{\mathfrak{p}})/(\mathfrak{p}(A_{\mathfrak{p}}/\mathfrak{a}A_{\mathfrak{p}}))$$

So, the morphism is certainly unramified. To show flatness, we need the following lemma from [Stack]: (Equational criterion for flatness) A module M over A is flat if and only if every relation in M is trivial.

Given $\sum_{i=1}^{n} a_i(b_i + \mathfrak{a}) = \mathfrak{a}$, where $a_i, b_i \in A$. We have $\sum_{i=1}^{n} a_i b_i = \sum_{j=1}^{m} s_j e_j \in \mathfrak{a}$, where $s_j \in k_j$ and e_j as defined before. Let the j-th component of b_i be $(b_i)_j \in k_j$. Assume $b_i' = b_i - \sum_{j=1}^{m} (b_i)_j e_j \in A$. Then, $b_i + \mathfrak{a} = b_i'(e + \mathfrak{a})$, where e is the identity. And $\sum_{i=1}^{n} a_i b_i' = 0$. Therefore, the relation is trivial.

6.9 Let A be a ring, M and N two finitely generated free A-module, and $f : M \to N$ an A-linear map. Prove that f is an isomorphism if and only if for each $\mathfrak{p} \in \operatorname{Spec} A$ the induced map $M \otimes_A k(\mathfrak{p}) \to N \otimes_A k(\mathfrak{p})$ is an isomorphism.

Since isomorphism between modules is a local property, it is suffice to show the following statement: Let $(A, \mathfrak{m})$ be a local ring, M and N two finitely generated free A-modules. Then $f : M \to N$ is an isomorphism if and only if $\bar{f} : M/\mathfrak{m}M \to N/\mathfrak{m}N$ is an isomorphism.

The "only if" part is obvious since a free basis of M(resp. N) over A gives a basis of $M/\mathfrak{m}M$ (resp. $N/\mathfrak{m}N$) over $A/\mathfrak{m}$. For the "if" part, we choose a free basis of M, by using $\bar{f}$ is isomorphism and Nakayama lemma, the image of this basis under f generates N, i.e., f is surjective.

Note that $\bar{f}$ is an isomorphism implies M and N have the same ranks, hence we can compose f with an isomorphism from N to M. So it is suffice to show that if an A-linear map $g : M \to M$ is surjective, then it is an isomorphism.

We can view M as a finitely generated $A[X]$-module by setting $X \cdot m = g(m)$ for $m \in M$. Then $XM = M$ since g is surjective. By Nakayama lemma, there exists $Y \in A[X]$ such that $(1 + XY)M = 0$. Now if $u \in ker(g)$, then $0 = (1 + XY)u = u + Yf(u) = u$. Hence g is an isomorphism.

6.11 Let A be a ring, B a separable A-algebra (see 6.10), and C an A-algebra. Prove that $B \otimes_A C$ is a separable C-algebra.

B a separable A-algebra $\Rightarrow$ B is a projective $B \otimes_A B$-module. Given $(B \otimes_A B) \otimes_A C$-modules M, N with surjective homomorphism $M \twoheadrightarrow N$. M, N can be seen as $B \otimes_A B$-modules by the natural map $B \otimes_A B \to (B \otimes_A B) \otimes_A C$. Hence, we have

$$\begin{tikzcd}
& B \arrow[d] \arrow[dl, dotted, "\exists"'] \\
M \arrow[r, two heads] & N
\end{tikzcd}$$

Similarly, C is a projective C-module and M, N can be viewed as C-modules. We obtain the following diagram by the universal property.

$$\begin{tikzcd}
& C \arrow[d] \arrow[dl, dotted, "\exists"'] & & & B \otimes_A C \arrow[d] \arrow[dl, dotted, "\exists"'] \\
M \arrow[r, two heads] & N & \Longrightarrow & M \arrow[r, two heads] & N
\end{tikzcd}$$

Therefore, $B \otimes_A C$ is a projective $(B \otimes_A B) \otimes_A C \cong (B \otimes_A B) \otimes_A (C \otimes_C C) \cong B \otimes_A (B \otimes_A C) \otimes_C C \cong B \otimes_A C \otimes_C (B \otimes_A C)$-module $\Rightarrow$ $B \otimes_A C$ is a separable C-algebra.

6.12 Let A be a ring and $B_1, B_2, ..., B_n$ algebras over A. Prove that $\prod_{i=1}^{n} B_i$ is a separable A-algebra if and only if each B_i is a separable A-algebra.

First prove the if part. Since B_i is projective $B_i \otimes_A B_i$-module for all i, we view any $(\oplus B_i) \otimes_A (\oplus B_i)$-module diagram

$$\begin{tikzcd}
 & \oplus B_i \arrow[d] \arrow[dl, dotted, "?"'] \\
M \arrow[r, two heads] & N
\end{tikzcd}$$

as $B_i \otimes_A B_i$-module diagram. Then, for each i we have

$$\begin{tikzcd}
 & B_i \arrow[d] \arrow[ddl, dotted, "\exists f_i"'] \\
 & \oplus B_i \arrow[d] \arrow[dl, dotted, "?"'] \\
M \arrow[r, two heads] & N
\end{tikzcd}$$

We can really find a map from $\oplus B_i$ to M by summing up f_i, which is a $(\oplus B_i) \otimes_A (\oplus B_i)$-module homomorphism. On the other hand, if $\oplus B_i$ is a separable A-algebra, we consider any $B_i \otimes_A B_i$-module diagram

$$\begin{tikzcd}
 & \oplus B_i \arrow[d] \arrow[ddl, dotted, "\exists f"'] \\
 & B_i \arrow[d] \arrow[dl, dotted, "?"'] \\
M \arrow[r, two heads] & N
\end{tikzcd}$$

as a $(\oplus B_i) \otimes_A (\oplus B_i)$-module by the natural map

$$(\oplus B_i) \otimes_A (\oplus B_i) \to B_i \otimes_A B_i$$

Then, we can choose the map from B_i to M be $f|_{B_i}$ to make the diagram commute. So, B_i is a separable A-algebra.

6.13 Let K be an algebraically closed field and B a finite dimensional K-algebra that is a local ring. Prove that the residue class field of B is K, and that $B \otimes_K B$ is a local ring.

Assume B has the unique maximal ideal $\mathfrak{m}$. Then, $B/\mathfrak{m}$ is a B-module and thus a K-module, which is necessarily a finite dimensional K-algebra. However, $B/\mathfrak{m}$ is a field K' and hence finite extension of K. By $K = \bar{K}$, $K' = K$. Now consider $B \otimes_K B$. Follow by 2.6, we know $\mathfrak{m}$ is the unique prime ideal and hence equal to nil(B). So, $\mathfrak{m} \otimes_K B$ and $B \otimes_K \mathfrak{m}$ are also nil ideals. And thus they are lie in radical. To show $B \otimes_K B$ is local, it then suffices to show $B \otimes_K B/(\mathfrak{m} \otimes_K B + B \otimes_K \mathfrak{m})$ is local. However, the latter one is isomorphic to $K \otimes_K K \cong K$.

A more general discussion about whether tensor products of local rings are local or not can be referred to [Sweedler] and [Lawrence].

6.14 Let X be a topological space that can be written as the union of open irreducible subsets. Prove that X can be written as the *disjoint* union of open irreducible subsets.

We first claim $X_1 \cup X_2$ is open and irreducible if so are X_1 and X_2 and they are not disjoint. Open is clear. To show it is irreducible, we consider any two open subsets and assert they cannot have nonempty intersection. If U, V are two open subsets in $X_1 \cup X_2$, then by irreducibility, $U \cap (X_1 \cap X_2)$ and $V \cap (X_1 \cap X_2)$ are nonempty. So, again by irreducibility, $U \cap V \cap (X_1 \cap X_2) \neq \emptyset \Rightarrow U \cap V \neq \emptyset$.

Now, consider X is the union of open irreducible subsets U_α, $\alpha \in \Lambda$. Consider

$$P = \{V \mid V = \bigcup_{\beta \in \Xi \subset \Lambda} U_\beta, V \text{ is connected and irreducible}\}.$$

Then, P is a nonempty poset and every chain $\{V_\gamma\}_{\gamma \in \Gamma}$ in P has an upper bound, that is, $W = \bigcup_{\gamma \in \Gamma} V_\gamma$ will also be irreducible and connected: If X_1, X_2 are open subsets of W, then there exists γ_i with $X_i \cap V_{\gamma_i} \neq \emptyset$. If, without lost of generality, say $V_{\gamma_2} \subset V_{\gamma_1}$, then $X_1 \cap X_2 \cap V_{\gamma_1} \neq \emptyset$ by the claim. So, W is also irreducible. Similar argument works for connectedness. Hence, by Zorn's lemma, $\forall\, U_\alpha$, it is contained in some $W_\alpha = \bigcup_{\beta \in \Xi \subset \Lambda} U_\beta$, which is connected, irreducible and *maximal.* That is, $\forall\, U_{\alpha'}, \alpha' \notin \Xi$, $W_\alpha \cup U_{\alpha'}$ cannot be connected or irreducible. However, if it is connected, it needs to be irreducible by claim again. So, every two W_α are either disjoint or the same and $X = \amalg\, W_\alpha$.

6.15 Let A be noetherian ring for which $\operatorname{Spec} A$ is connected, and suppose that $A_\mathfrak{p}$ is a domain for all $p \in \operatorname{Spec} A$. Prove that A is a domain. [*Hint:* if $\mathfrak{a}\mathfrak{b} = 0$ for all non-zero ideals $\mathfrak{a}, \mathfrak{b}$ of A, choose $\mathfrak{a}, \mathfrak{b}$ as large as possible and prove that $\mathfrak{a} + \mathfrak{b} = A$.]

Since A is noetherian, $\operatorname{Spec} A$ is a noetherian topological space. There are only finitely many irreducible components, say $X_1, ..., X_n$. Then, $X_1 \cap X_j \neq \emptyset$ for some j because $\operatorname{Spec} A$ is connected. Consider $x \in X_1 \cap X_j$. Since irreducible components correspond to the unique generic points, which are minimal prime ideals, say $\mathfrak{p}_1$ and $\mathfrak{p}_j$, satisfying $x \supset \mathfrak{p}_1$ and $x \supset \mathfrak{p}_j$. Then, consider the corresponding prime ideals in A_x and denote them by $\mathfrak{p}'_1$ and $\mathfrak{p}'_j$, still minimal. The nilradical of A_x is contained in $\mathfrak{p}'_1 \cap \mathfrak{p}'_j$, which is not a prime ideal unless $\mathfrak{p}'_1 \subset \mathfrak{p}'_j$ or $\mathfrak{p}'_1 \supset \mathfrak{p}'_j$. In other words, $\mathfrak{p}_1 \subset \mathfrak{p}_j$ or $\mathfrak{p}_1 \supset \mathfrak{p}_j$, implying X_1 and X_j cannot be distinct irreducible components. So, nilradical of A_x is necessarily not prime, which contradicts the assumption A_x is a domain. On the other hand, reduceness is a local property. So, $\operatorname{Spec} A$ is irreducible and reduced, and thus integral ([Hartshorne, Proposition II.3.1]).

6.16 Let X be a locally noetherian scheme all of whose local rings are domains. Prove that X is the disjoint union of a collection of integral schemes. [*Hint:* use Exercises 6.14 and 6.15.]

Let X_i be connected components of X. Consider $X = \cup \operatorname{Spec} A_\alpha$ with A_α noetherian. Since $\operatorname{Spec}(A_\alpha)_{f_{\alpha\beta}}$ form the base of X and X_i is open, X_i is the union of some affine open subset, called $\operatorname{Spec} A_{i_j}$, where A_{i_j} is noetherian since localization of a noetherian ring is still noetherian. Then, by Exercise 6.15, A_{i_j} is a domain, hence a reduced ring. Finally, any two open subsets $D(f)$, $D(g)$ of $\operatorname{Spec} A_{i_j}$ has intersection $D(fg)$ and this intersection is not empty unless $fg \in \operatorname{nil}(A_{i_j}) = \{0\} \Rightarrow f = 0$ or $g = 0 \Rightarrow D(f) = \emptyset$ or $D(g) = \emptyset$. So, every open subset is dense and $\operatorname{Spec} A_{i_j}$ is necessarily irreducible. By Exercise 6.14, we obtain what we want.

6.18 Let K be a field, L a finite extension field of K, and $x \in L$. Let $\sum_{i=0}^{n} a_i X^i$ be the irreducible polynomial of x over K, with $a_n = 1$. Prove that $\operatorname{Tr}_{L/K}(x) = -[L : K(x)] \cdot a_{n-1}$.

Let $\{v_1, \cdots, v_k\}$ be a basis of field extension L over $K(x)$. Then $\{x^j v_i | 0 \leq j \leq n-1, 1 \leq i \leq k\}$ is a basis of L over K. For any $1 \leq i \leq k$, $< v_i, xv_i, \cdots, x^{n-1}v_i >$ is invariant under multiplying x, and its trace is given by $-a_{n-1}$ by direct computations. Hence $\operatorname{Tr}_{L/K}(x) = -k \cdot a_{n-1} = -[L : K(x)] \cdot a_{n-1}$.

6.19 Let K be a finite field and C the K-algebra $K^{\#K+1}$. Prove that there does not exist $\gamma \in C$ with $C = K[\gamma]$.

Suppose that $C = K^{|K|+1} = K[\gamma]$ for some $\gamma \in C$. Since K is a finite field, we have $\gamma^{|K|} = \gamma$. Hence $\dim_K K[\gamma] \leq |K| < |K| + 1 = \dim_K K^{|K|+1}$, contradiction.

6.20 Let A be a domain with field of fractions K, and L an algebraic field extension of K. Prove that for every $x \in L$, there exists $a \in A, a \neq 0$ such that ax is integral over A.

By x is algebraic over K, $x^n + \frac{a_{n-1}}{b_{n-1}} x^{n-1} + \cdots + \frac{a_0}{b_0} = 0$ for some coefficients $a_i, b_i \in A$. Let $a := (b_{n-1} b_{n-2} \cdots b_0)^n$. Then $a\frac{a_i}{b_i} \in A$ and hence the element ax satisfying a monic polynomial with coefficient in A, so ax is integral over A.

6.21 Let $f : Y \to X$ be a continuous surjective map from a topological space Y to a connected topological space X, and assume that every $x \in X$ has an open neighborhood U for which $f^{-1}(U)$ is connected. Prove that Y is connected.

Suppose that Y is not connected, write $Y = Y_1 \amalg Y_2$, where Y_1 and Y_2 are disjoint nonempty open subsets of Y.

Claim: $f(Y_1)$ and $f(Y_2)$ are both disjoint.

If not, say $x \in f(Y_1) \cap f(Y_2)$. For any open neighborhood U of x, $f^{-1}(U)$ is not connected since it has nonempty intersections with both Y_1 and Y_2, this proves the claim. So we have $X = f(Y_1) \amalg f(Y_2)$ since f is surjective.

Claim: $f(Y_1)$ and $f(Y_2)$ are both open.

Suppose that $f(Y_1)$ is not open. Then there exists $x \in f(Y_1)$ such that for any open neighborhood U of x, U has nonempty intersection with $f(Y_2)$, but this implies that $f^{-1}(U)$ is not connected, which proves the claim.

So X can be written as a disjoint union of two nonempty open subsets, contradiction.

6.23 Let A be a ring and B a finitely generated A-algebra that is integral over A. Prove that B is a finitely generated as an A-module.

By assumption, we may assume $B = A[u_1, ..., u_m]$, u_i's may have relations. For each i, by integral assumption, there exists $n_i \in \mathbb{N}$ such that $u_i^{n_i} \in A + Au_i + ... + Au_i^{n_i-1} \subseteq B$.

So for any element $u \in B$, u is an A-linear combination of the monomials $\prod_{i=1}^{m} u_i^{t_i}$ and $0 \leq t_i \leq n_i - 1$, these monomials form a finite collection, say $\{w_1, ..., w_k\}$. So $B = \sum_{j=1}^{k} Aw_j$.

6.26 Let X be a connected scheme. Prove the following properties are equivalent:

(a) X is locally noetherian, and every local ring of X is a discrete valuation ring or a field;

(b) there is a covering of X by open affine subsets $U_i = \operatorname{Spec} A_i$ where each A_i is a Dedekind domain or a field;

(c) for each open affine subset $U = \emptyset$ of X we have $U = \operatorname{Spec} A$, where A is a Dedekind domain or a field.

(c) implies (b) is clear. (b) implies (a) follows from the fact that the localization of a Dedekind domain at a prime is either a discrete valuation ring (localize at maximal ideals) or a field(localize at zero ideal). So it remains to prove (a) implies (c). Let $U = \operatorname{Spec} A$ be an open affine subset of X. By the conditions of (a), A is noetherian and $A_{\mathfrak{p}}$ is a DVR or a field for every prime $\mathfrak{p}$.

Observe that $U = \operatorname{Spec} A$ is connected, since X is connected. Assume that A is not a field, otherwise we are done. Suppose that A is an integral domain. Then A is a Dedekind domain if and only if the localization $A_{\mathfrak{m}}$ at every maximal ideal is DVR, which follows from the conditions of (a), since $A_{\mathfrak{m}}$ is not a field. So it remains to prove the following statement: Let A be a noetherian ring, such that $A_{\mathfrak{p}}$ is integral domain for every prime $\mathfrak{p}$, and $\operatorname{Spec} A$ is connected. Show that A is an integral domain.

Suppose that there exists $a, b \in A$ such that $ab = 0, a \neq 0, b \neq 0$. Since $A_{\mathfrak{p}}$ is integral domain, $a_{\mathfrak{p}}$ or $b_{\mathfrak{p}}$ must be zero. Hence $Ann(a) + Ann(b) = A$ since the left hand side does not contained in any prime ideals. So there exists $u \in Ann(a)$ and $a_1 \in Ann(b)$ such that $u + a_1 = 1$. Hence $a = a(u + a_1) = aa_1$. So we get an element $a_1 \in A$ such that $a_1 b = 0, a_1 \neq 0, b \neq 0$, with equation $a = aa_1$. We can use this process to produce the next a_2, a_3, and so on.

So we have $(a) \subset (a_1) \subset (a_2) \subset \cdots$. Since A is noetherian, there exists $(a_{n-1}) = (a_n)$, write $a_n = a_{n-1}c$ for some $c \in A$. Then $a_n^2 = a_n a_{n-1} c = a_{n-1} c = a_n$, i.e., a_n is an idempotent element, which is not $0, 1$. This contradicts to $\operatorname{Spec} A$ is connected, which proves that A is an integral domain.

6.32 Let B be a ring and $I \subset B$ a nilpotent ideal. Prove that the set of idempotents of B maps bijectively to the set of idempotents of B/I, under the natural map $B \to B/I$.

Let $e \in B$ be an idempotent. $(e + I)^2 = e^2 + I = e + I$ is also an idempotent. $e + I = e' + I \Rightarrow e - e' \in I \Rightarrow (e - e')^n = 0$, $\forall n \geq N$ for some $N \in \mathbb{N}$. Pick $2 \nmid n$. Then, by $e^2 = e$, $e'^2 = e'$ and the binomial theorem, $0 = (e - e')^n = e^n - (e')^n = e - e'$. Finally, if $x + I$ is an idempotent, $x^2 - x \in I$. Let $x_1 = x$, $x_{i+1} = 3x_i^2 - 2x_i^3$. Then

$$x_{i+1}^2 - x_{i+1} = (x_i^2 - x_i)^2(3 - 2x_i)(2x_i + 1) \in I^{2^i} \subset I,$$

which will be zero for sufficiently big i. Moreover, let $y_i = x_i^2 - x_i \in I$. Then

$$x_{i+1} - x_i = 3(x_i + y_i) - 2(x_i y_i + x_i + y_i) - x_i = y_i - 2x_i y_i \in I.$$

Thus, $x_i + I = x + I$ for all i.

6.33 Let p be a prime number and $n \in \mathbb{Z}$, $n > 0$. Prove that the ring homomorphism $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ induces an isomorphism $\pi(\operatorname{Spec} \mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\sim} \pi(\operatorname{Spec} \mathbb{Z}_p)$.

Spec$(\mathbb{Z}/p^n\mathbb{Z})$ contains one element thus must be connected. By 6.24, consider $\mathbb{F}_p$ be its residue class field, we have $\pi(\operatorname{Spec} \mathbb{F}_p) \xrightarrow{\sim} \pi(\operatorname{Spec} \mathbb{Z}/p^n\mathbb{Z})$ induced by natural ring homomorphism $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{F}_p$. Finite extensions of $\mathbb{F}_p$ are $\mathbb{F}_{p^n}$ and indeed they are all separable. By 6.18 (or [E. Weiss, *Algebraic Number Theory*, Section 3-2]), the ring homomorphism $\mathbb{Z}_p \to \mathbb{F}_p$, which is the composition of $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{F}_p$, is exactly the residue class map and induces the equivalence of category $\mathbf{FEt}_{\operatorname{Spec} \mathbb{F}_p} \to \mathbf{FEt}_{\operatorname{Spec} \mathbb{Z}_p}$ and thus induces the isomorphism $\pi(\operatorname{Spec} \mathbb{F}_p) \xrightarrow{\sim} \pi(\operatorname{Spec} \mathbb{Z}_p)$. Thus, the ring homomorphism $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ induces an isomorphism $\pi(\operatorname{Spec} \mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\sim} \pi(\operatorname{Spec} \mathbb{Z}_p)$.

6.35 Prove that $\pi(\operatorname{Spec} \mathbb{Z}[i])$ and $\pi(\operatorname{Spec} \mathbb{Z}[(1 + \sqrt{-3})/2])$ are trivial.

Observe that $\mathbb{Z}[i]$ and $\mathbb{Z}[(1 + \sqrt{-3})/2]$ are rings of integers of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, respectively. By Corollary 6.17, it is suffices to show that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ have no unramified extensions, . . .